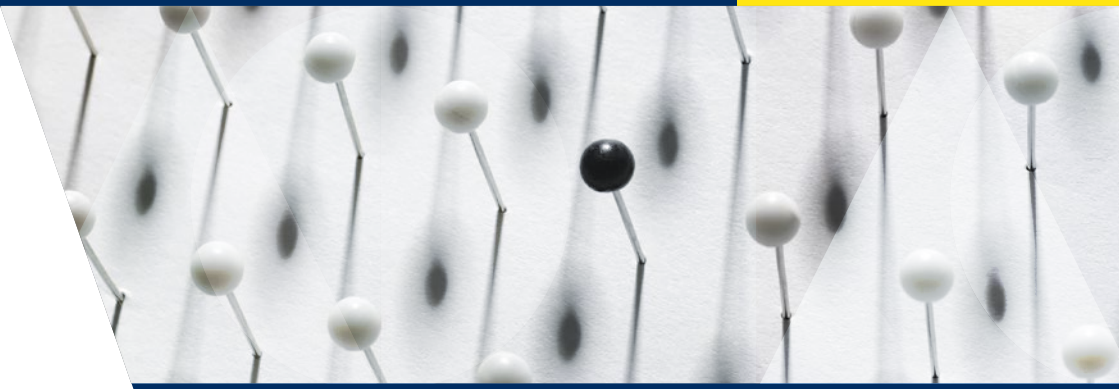
HÅNDBOG



Håndbog om europæisk databeskyttelseslovgivning

2018-udgave

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Manuskriptet til denne håndbog blev færdiggjort i april 2018.

Fremtidige opdateringer af håndbogen vil blive gjort tilgængelige på FRA's websted på fra.europa.eu, på Europarådets websted på coe.int/dataprotection, på Den Europæiske Menneskerettighedsdomstols websted under menuen »Case-Law« på echr.coe.int og på Den Europæiske Tilsynsførende for Databeskyttelses websted på edps.europa.eu.

Foto (omslag og inderside): © iStockphoto

Luxembourg: Den Europæiske Unions Publikationskontor, 2021

Europarådet:	ISBN 978-92-871-9810-5		
FRA – Print:	ISBN 978-92-9461-345-5	doi:10.2811/58	TK-05-17-225-DA-C
FRA – PDF:	ISBN 978-92-9461-344-8	doi:10.2811/834732	TK-05-17-225-DA-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Håndbog om europæisk databeskyttelseslovgivning

2018-udgave

Forord

Vores samfund bliver i stigende grad mere digitaliseret. Tempoet for den teknologiske udvikling og måden, hvorpå personoplysninger behandles, påvirker os alle hver dag og på alle mulige måder i lyset af disse ændringer. Retsgrundlaget for Den Europæiske Union (EU) og Europarådet, som sikrer beskyttelse af privatlivets fred og personoplysninger, blev revideret for nylig.

Europa er i spidsen inden for databeskyttelse på verdensplan. EU's databeskyttelsesstandarder er baseret på Europarådets konvention 108, EU-instrumenter — herunder databeskyttelsesforordningen og databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder — samt gældende retspraksis for Den Europæiske Menneskerettighedsdomstol og Den Europæiske Unions Domstol.

De databeskyttelsesreformer, som EU og Europarådet har gennemført, har været omfattende og til tider komplekse, og de har haft omfattende fordele for og indvirkninger på fysiske personer og virksomheder. Formålet med denne håndbog er at øge bevidstheden om og udbrede kendskabet til databeskyttelsesregler, især blandt ikke-specialiserede aktører inden for retsvæsenet, der er nødt til at håndtere spørgsmål vedrørende databeskyttelse i forbindelse med deres arbejde.

Denne håndbog er udarbejdet af Den Europæiske Unions Agentur for Grundlæggende Rettigheder (FRA), Europarådet (i samarbejde med Den Europæiske Menneskerettighedsdomstols justitskontor) og Den Europæiske Tilsynsførende for Databeskyttelse. Den ajourfører en udgave fra 2014, og er den del af en serie af juridiske håndbøger, der er udarbejdet i fællesskab af FRA og Europarådet.

Vi vil gerne takke databeskyttelsesmyndighederne i Belgien, Det Forenede Kongerige, Estland, Frankrig, Georgien, Irland, Italien, Monaco, Schweiz og Ungarn for deres nyttige feedback til håndbogens udkast. Vi vil også gerne takke Europa-Kommissionens Databeskyttelsesafdeling og dens afdeling for Internationale Datastrømme og Beskyttelse. Vi vil gerne takke Den Europæiske Unions Domstol for deres dokumentationsstøtte under det forberedende arbejde til denne håndbog. Endelig vil vi gerne udtrykke vores taknemmelighed over for Datatilsynet for dets støtte til revisionen af den danske version af denne håndbog.

Christos Giakoumopoulos	**Giovanni Buttarelli**	**Michael O'Flaherty**
Generaldirektør for Menneskerettigheder og Retsstaten, Europarådet	Den Europæiske Tilsynsførende for Databeskyttelse	Direktør for Den Europæiske Unions Agentur for Grundlæggende Rettigheder

Indholdsfortegnelse

Forkortelser og akronymer

CETS	Council of Europe Treaty Series (Europarådets traktatserie)
Charter	Den Europæiske Unions charter om grundlæggende rettigheder
CIS	Customs information system (toldinformationssystem)
CRM	Customer relations management (forvaltning af kunderelationer)
C-SIS	Det centrale Schengeninformationssystem
DPO	Data Protection Officer (databeskyttelsesrådgiver)
EDPB	Det Europæiske Databeskyttelsesråd
EDPS	Den Europæiske Tilsynsførende for Databeskyttelse
EFSA	Den Europæiske Fødevaresikkerhedsautoritet
EMD	Den Europæiske Menneskerettighedsdomstol
EMRK	Den europæiske menneskerettighedskonvention
ENU	Europol National Unit (national Europolenhed)
EØS	Det Europæiske Økonomiske Samarbejdsområde
EPPO	Den Europæiske Anklagemyndighed
ESMA	Den Europæiske Værdipapir- og Markedstilsynsmyndighed
eTEN	Transeuropæiske telenet
EU	Den Europæiske Union
EU-Domstolen	Den Europæiske Unions Domstol (De Europæiske Fællesskabers Domstol, ECJ, inden december 2009)
eu-LISA	Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed
Europarådet	Council of Europe (Europarådet)
EuroPriSe	European Privacy Seal (europæisk datasikkerhedsmærkning)
EUT	EU-Tidende
FN	De Forenede Nationer
FRA	Den Europæiske Unions Agentur for Grundlæggende Rettigheder
GDPR	Generel forordning om databeskyttelse

GPS	Globalt positioneringssystem
ICCPR	International Covenant on Civil and Political Rights (den internationale konvention om borgerlige og politiske rettigheder)
IKT	Informations- og kommunikationsteknologi
ISP	Internet service provider (internetudbyder)
JSB	Joint Supervisory Body (Den Fælles Kontrolinstans)
Konvention 108	Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (Europarådet). Ændringsprotokollen (CETS nr. 223) til konvention 108 (»den moderniserede konvention 108«) blev vedtaget af Europarådets Ministerkomité ved dets 128. samling i Helsingør, Danmark (17.-18. maj 2018). Henvisninger til »den moderniserede konvention 108« skal tolkes som henvisninger til konventionen som ændret ved protokollen, CETS nr. 223.
NGO	Ikke-statslig organisation
N-SIS	Det nationale Schengeninformationssystem
OECD	Organisationen for Økonomisk Samarbejde og Udvikling
PIN	Personligt identifikationsnummer
PNR	Passenger name record (passagerliste)
SEPA	Single Euro Payments Area (fælleseuropæisk betalingsområde)
SIS	Schengeninformationssystemet
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEU	Traktaten om Den Europæiske Union
TEUF	Traktaten om Den Europæiske Unions funktionsmåde
UDHR	Universal Declaration of Human Rights (verdenserklæringen om menneskerettighederne)
VIS	Visuminformationssystem

Sådan anvendes håndbogen

Denne håndbog giver en oversigt over retlige standarder vedrørende databeskyttelse, som er fastlagt af Den Europæiske Union (EU) og Europarådet. Håndbogen har til formål at bistå jurister, der ikke er specialiseret i databeskyttelse, herunder advokater, dommere og andre jurister, og fysiske personer, der arbejder for andre organer, såsom ikke-statslige organisationer (NGO'er), som kan støde på juridiske spørgsmål vedrørende databeskyttelse.

Håndbogen omhandler først og fremmest gældende EU-lovgivning, den europæiske menneskerettighedskonvention, Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108) og andre instrumenter fra Europarådet.

Hvert kapitel starter med en tabel med lovbestemmelser, som har relevans for kapitlets emner. Tabellerne omfatter både Europarådets lovgivning og EU-retten samt eksempler på retspraksis fra Den Europæiske Menneskerettighedsdomstol (EMD) og Den Europæiske Unions Domstol (EU-Domstolen). Derefter præsenteres de relevante love i disse to europæiske systemer efter hinanden i det omfang, de er relevante for de pågældende emner. Derved kan læseren se, hvor de to retsordener overlapper, og hvor de er forskellige. Det hjælper også læseren med at finde de informationer, som er mest relevante for deres situation, især hvis denne kun er underlagt Europarådets lovgivning. I nogle kapitler kan rækkefølgen for emnerne i tabellen afvige fra rækkefølgen i kapitlet, hvis det giver en mere kortfattet præsentation af indholdet. Håndbogen gennemgår også kort De Forenede Nationers retsgrundlag.

Jurister i tredjelande, som er medlem af Europarådet og part i Den europæiske menneskerettighedskonvention (EMRK) og konvention 108, kan få adgang til de oplysninger, som er relevante for deres eget land, ved at gå direkte til afsnittene om Europarådet. Jurister i tredjelande skal også være opmærksomme på, at EU's databeskyttelsesregler, efter vedtagelsen af EU's databeskyttelsesforordning, gælder for organisationer og andre enheder, som ikke er etableret i EU, hvis de behandler personoplysninger og udbyder varer eller tjenester til registrerede i Unionen eller overvåger sådanne registreredes opførsel.

Jurister i EU's medlemsstater skal anvende begge afsnit, da disse lande er bundet af begge retsordener. Det skal understreges, at reformerne og moderniseringen af databeskyttelsesregler i Europa, som både blev gennemført inden for retsgrundlaget for Europarådet (den moderniserede konvention 108, som ændret ved protokollen,

CETS nr. 223) og EU (vedtagelse af den generelle forordning om databeskyttelse og direktiv (EU) 2016/680), blev udført på samme tid. Kontrolorganer inden for begge retsordener har så vidt muligt sikret sammenhæng og forenelighed mellem de to retsgrundlag. Reformerne har derfor bidraget til en større harmonisering af Europarådets og EU's databeskyttelseslovgivning. Fysiske personer, som har brug for flere oplysninger om et bestemt spørgsmål, kan finde en liste over mere specialiseret materiale i afsnittet »Yderligere materiale«. Læsere, som er interesseret i oplysninger om bestemmelserne i konvention 108 og dens tillægsprotokol af 2001, der fortsat er gældende indtil ikrafttrædelsen af ændringsprotokollen, henvises til 2014-udgaven af håndbogen.

Europarådets lovgivning præsenteres via korte henvisninger til udvalgte EMD-sager. De er udvalgt ud fra alle de EMD-domme og -afgørelser, som omhandler spørgsmål vedrørende databeskyttelse.

Relevant EU-ret består af vedtagne retsakter, relevante bestemmelser i traktaterne og Den Europæiske Unions charter om grundlæggende rettigheder som fortolket ved EU-Domstolens retspraksis. Desuden indeholder håndbogen udtalelser og retningslinjer, som er vedtaget af Artikel 29-Gruppen, det rådgivende organ, som under databeskyttelsesdirektivet havde fået til opgave at forsyne EU's medlemsstater med ekspertrådgivning, og som blev afløst af Det Europæiske Databeskyttelsesråd (EDPB) den 25. maj 2018. Udtalelser fra Den Europæiske Tilsynsførende for Databeskyttelse giver også et vigtigt indblik i fortolkningen af EU-ret, og de er derfor inkluderet i denne håndbog.

De sager, der beskrives eller citeres i denne håndbog, giver eksempler på vigtig retspraksis ved både EMD og EU-Domstolen. Retningslinjerne sidst i håndbogen kan hjælpe læseren med at søge efter retspraksis på internettet. EU-Domstolens retspraksis, som præsenteres heri, omhandler det tidligere databeskyttelsesdirektiv. EU-Domstolens fortolkninger forbliver dog gældende i forhold til de tilsvarende rettigheder og forpligtelser, som fastlægges i den generelle forordning om databeskyttelse.

Derudover er praktiske illustrationer med hypotetiske scenarier anført i tekstbokse med en blå baggrund. Disse illustrerer den praktiske anvendelse af de europæiske databeskyttelsesregler, især i de tilfælde, hvor der ikke findes nogen særlig relevant retspraksis ved EMD eller EU-Domstolen. Andre tekstbokse — med en grå baggrund — indeholder eksempler fra andre kilder end retspraksis ved EMD og EU-Domstolen, såsom lovgivning og udtalelser udstedt af Artikel 29-Gruppen.

Håndbogen indledes med en kort beskrivelse af de to retsordeners rolle som fastlagt ved EMRK og EU-ret (kapitel 1). Kapitel 2-10 omhandler følgende emner:

- databeskyttelsesterminologi
- de centrale principper i den europæiske databeskyttelseslovgivning
- reglerne i den europæiske databeskyttelseslovgivning
- uafhængigt tilsyn
- de registreredes rettigheder og håndhævelsen heraf
- internationale dataoverførsler og udvekslinger af personoplysninger
- databeskyttelse i forbindelse med politi og strafferet
- specifikke datatyper og deres relevante databeskyttelsesregler
- nutidens udfordringer med beskyttelse af personoplysninger.

1

Kontekst og baggrund for den europæiske databeskyttelseslovgivning

EU	Omhandlede emner	Europarådet
Retten til databeskyttelse		
Traktat om Den Europæiske Unions funktionsmåde, artikel 16 Den Europæiske Unions charter om grundlæggende rettigheder (Chartret), artikel 8 (ret til beskyttelse af personoplysninger) Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesdirektivet), EFT L 281 af 23.11.1995 (gældende indtil maj 2018) Rådets rammeafgørelse 2008/977/RIA om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, EUT L 350 af 30.12.2008 (gældende indtil maj 2018) Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), EUT L 119 af 4.5.2016		EMRK, artikel 8 (ret til respekt for privatliv og familieliv, hjem og korrespondance) Den moderniserede konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (den moderniserede konvention 108)

EU	Omhandlede emner	Europarådet
Direktiv (EU) 2016/680 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (databeskyttelse for politi og strafferetlige myndigheder), EUT L 119 af 4.5.2016 Direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), EFT L 201 af 31.7.2002 Forordning (EF) nr. 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (forordning om databeskyttelse inden for EU-institutionerne), EFT L 8 af 12.1.2001		
Begrænsninger af retten til beskyttelse af personoplysninger		
Chartret, artikel 52, stk. 1 Generel forordning om databeskyttelse, artikel 23 EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 2010		EMRK, artikel 8, stk. 2 Den moderniserede konvention 108, artikel 11 EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 2008
Afvejning af rettigheder		
EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 2010	**Generelt**	
EU-Domstolen, C-73/07, *Tietosuojavaltuutettu mod Satakunnan Markkinapörssi Oy og Satamedia Oy* [GC], 2008 EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 2014	**Ytringsfrihed**	EMD, *Axel Springer AG mod Tyskland* [GC], nr. 39954/08, 2012 EMD, *Mosley mod Det Forenede Kongerige*, nr. 48009/08, 2011 EMD, *Bohlen mod Tyskland*, nr. 53495/09, 2015

EU	Omhandlede emner	Europarådet
EU-Domstolen, C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd* [GC], 2010 EU-Domstolen, C-615/13 P, *ClientEarth og Pesticide Action Network Europe (PAN Europe) mod Den Europæiske Fødevaresikkerhedsautoritet (EFSA) og Europa-Kommissionen*, 2015	**Aktindsigt**	EMD, *Magyar Helsinki Bizottság mod Ungarn* [GC], nr. 18030/11, 2016
Generel forordning om databeskyttelse, artikel 90	**Tavshedspligt**	EMD, *Pruteanu mod Rumænien*, nr. 30181/05, 2015
Generel forordning om databeskyttelse, artikel 91	**Religions- og trosfrihed**	
	Frihed for kunst og videnskab	EMD, *Vereinigung bildender Künstler mod Østrig*, nr. 68354/01, 2007
EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU* [GC], 2008	**Beskyttelse af ejendomsret**	
EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 2014 EU-Domstolen, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 2017	**Økonomiske rettigheder**	

1.1. Retten til beskyttelse af personoplysninger

Hovedpunkter

- Ifølge artikel 8 i EMRK er en persons ret til beskyttelse mod behandling af personoplysninger en del af retten til respekt for privatliv og familieliv, hjem og korrespondance.
- Europarådets konvention 108 er det første, og i skrivende stund det eneste, internationalt retligt bindende instrument, som omhandler databeskyttelse. Konventionen gennemgik en moderniseringsproces, der blev afsluttet med vedtagelsen af en ændringsprotokol, CETS nr. 223.
- I EU-retten er databeskyttelse blevet anerkendt som en selvstændig grundlæggende rettighed. Det bekræftes i artikel 16 i traktaten om Den Europæiske Unions funktionsmåde samt i artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder.
- I EU-retten blev databeskyttelse første gang reguleret ved databeskyttelsesdirektivet i 1995.
- Som følge af den hurtige teknologiske udvikling vedtog EU ny lovgivning i 2016 for at tilpasse databeskyttelsesreglerne til den digitale tidsalder. Den generelle forordning om databeskyttelse trådte i kraft i maj 2018 og ophævede databeskyttelsesdirektivet.
- Sammen med den generelle forordning om databeskyttelse vedtog EU lovgivning om statslige myndigheders behandling af personoplysninger i forbindelse med retshåndhævelse. Direktiv (EU) 2016/680 fastlægger databeskyttelsesregler og -principper for behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre og retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner.

1.1.1. Retten til respekt for privatlivet og retten til beskyttelse af personoplysninger: en kort introduktion

Retten til respekt for privatlivet og retten til beskyttelse af personoplysninger er selvstændige rettigheder, selvom de er tæt forbundet. Retten til privatlivets fred – omtalt i EU-retten som retten til respekt for privatlivet – blev grundlagt som en af de grundlæggende beskyttede menneskerettigheder i international menneskerettighedslovgivning ved verdenserklæringen om menneskerettighederne (Universal Declaration of Human Rights – UDHR), der blev vedtaget i 1948. Kort efter vedtagelsen af UDHR blev denne rettighed også bekræftet i den europæiske

menneskerettighedskonvention (EMRK), som er en retligt bindende traktat for dens kontraherende parter, der blev udarbejdet i 1950. EMRK fastlægger, at alle har ret til respekt for hans eller hendes privatliv og familieliv, hjem og korrespondance. En offentlig myndighed må ikke blande sig i denne rettighed, medmindre indgrebet sker i overensstemmelse med loven, skyldes vigtige og legitime offentlige interesser og er nødvendig i et demokratisk samfund.

UDHR og EMRK blev vedtaget lang tid inden udviklingen af computere og internettet og informationssamfundets opståen. Disse udviklinger har givet fysiske personer og samfundet betragtelige fordele og forbedret livskvalitet, effektivitet og produktivitet. På samme tid udgør de nye trusler for retten til respekt for privatliv. Som svar på behovet for særlige regler for indsamling og brug af personoplysninger opstod der et nyt koncept for privatliv, som i nogle områder kaldes for »fortrolighed« og i andre for »retten til selvbestemmelse med hensyn til oplysninger« ([1]). Dette koncept førte til udviklingen af særlige lovbestemmelser, som beskytter personoplysninger.

Databeskyttelse i Europa startede i 1970'erne med indførelsen af lovgivning – i nogle stater – for at kontrollere offentlige myndigheders og store virksomheders behandling af personoplysninger ([2]). Der blev derefter etableret databeskyttelsesinstrumenter på EU-plan ([3]), og over flere år udviklede databeskyttelse sig til en selvstændig menneskeret, der ikke er underordnet retten til respekt for privatlivet. I EU's retsorden anerkendes databeskyttelse som en grundlæggende rettighed, der er særskilt fra den grundlæggende ret til respekt for privatlivet. Denne adskillelse stiller spørgsmålstegn ved forholdet og forskellene mellem disse to rettigheder.

Retten til respekt for privatlivet og retten til beskyttelse af personoplysninger er tæt forbundet. De er begge rettet mod at beskytte ensartede værdier, såsom fysiske

([1]) Den tyske forfatningsdomstol bekræftede en ret til selvbestemmelse med hensyn til oplysninger i en dom afsagt i 1983 i *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Domstolen mente, at selvbestemmelse med hensyn til oplysninger stammer fra den grundlæggende ret til respekt for personlighed, som er beskyttet i den tyske forfatning. EMD anerkendte i en dom fra 2017, at artikel 8 i EMRK giver ret til en form for selvbestemmelse med hensyn til oplysninger. Se EMD, *Satakunnan Markkinapörssi Oy og Satamedia Oy mod Finland*, nr. 931/13, 27. juni 2017, præmis 137.

([2]) Den tyske delstat Hessen vedtog den første lov om databeskyttelse i 1970, som kun var gældende i den delstat. I 1973 vedtog Sverige verdens første nationale lov om databeskyttelse. Ved slutningen af 1980'erne havde flere europæiske stater (Det Forenede Kongerige, Frankrig, Tyskland og Nederlandene) også indført lovgivning om databeskyttelse.

([3]) Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108) blev vedtaget i 1981. EU vedtog sit første omfattende databeskyttelsesinstrument i 1995: Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

personers selvstændighed og menneskelige værdighed, ved at give dem en personlig sfære, hvor de frit kan udvikle deres personligheder, tænke og forme deres holdninger. De er derfor en nødvendig forudsætning for udøvelsen af andre grundlæggende friheder, såsom ytringsfrihed, frihed til at deltage i fredelige forsamlinger, foreningsfrihed og religionsfrihed.

De to rettigheder adskiller sig ud fra deres formulering og omfang. Retten til respekt for privatlivet består af et generelt forbud mod indgreb, med visse undtagelser, der beror på almene hensyn, som i nogle tilfælde kan begrunde et indgreb. Beskyttelsen af personoplysninger betragtes som en moderne og aktiv rettighed ([4]), som fastlægger et system bestående af kontrolforanstaltninger til at beskytte fysiske personer, når deres personoplysninger behandles. Behandlingen skal overholde de væsentlige elementer af beskyttelsen af personoplysninger, navnlig uafhængigt tilsyn og respekt for den registreredes rettigheder ([5]) .

Artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder (Chartret) bekræfter ikke kun retten til beskyttelse af personoplysninger, men redegør også for de kerneværdier, som er knyttet til denne ret. Den fastlægger, at behandlingen af personoplysninger skal være rimelig, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Fysiske personer skal have ret til at få adgang til deres personoplysninger og til berigtigelse heraf, og overholdelse af denne ret er underlagt en uafhængig myndigheds kontrol.

Retten til beskyttelse af personoplysninger er gældende, når personoplysninger behandles. Den er dermed bredere end retten til respekt for privatlivet. Enhver behandlingsaktivitet med personoplysninger er underlagt hensigtsmæssig beskyttelse. Databeskyttelse omhandler alle former for personoplysninger og databehandling, uanset forholdet til og indvirkningen på privatlivet. Behandling af personoplysninger kan også overtræde retten til privatlivet, hvilket eksemplificeres nedenfor. Det er dog ikke nødvendigt at påvise en krænkelse af privatlivet, for at databeskyttelsesreglerne træder i kraft.

([4]) Generaladvokat Sharpston beskrev sagen som at omhandle to særskilte rettigheder, den »klassiske« ret til beskyttelse af privatlivet og en mere »moderne« ret, retten til databeskyttelse. Se EU-Domstolen, forenede sager C-92/09 og C-93/02, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen*, *Forslag til afgørelse fra generaladvokat Sharpston*, 17. juni 2010, præmis 71.

([5]) Hustinx, P., EDPS Speeches & Articles (taler og artikler), *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, juli 2013.

Retten til privatlivets fred vedrører situationer, hvor en privat interesse eller en fysisk persons »privatliv« tilsidesættes. Som denne håndbog viser, har retspraksis fortolket konceptet »privatliv« bredt, så det dækker private situationer, følsomme eller fortrolige oplysninger, oplysninger, der kan give offentligheden fordomme om en fysisk person, og sågar aspekter af en persons arbejdsliv og offentlige adfærd. Vurderingen af, om der er eller har været et indgreb i en persons »privatliv«, afhænger dog af konteksten og fakta i den enkelte sag.

I modsætning hertil kan enhver aktivitet, som omfatter behandlingen af personoplysninger, være omfattet af databeskyttelsesregler og udløse retten til beskyttelse af personoplysninger. Når en arbejdsgiver for eksempel registrerer oplysninger vedrørende navne på og godtgørelser betalt til medarbejdere, betragtes selve registreringen af disse oplysninger ikke som et indgreb i privatlivets fred. Der kan dog argumenteres for et sådant indgreb, hvis arbejdsgiveren, for eksempel, overførte medarbejderes personoplysninger til tredjeparter. Arbejdsgivere skal under alle omstændigheder overholde databeskyttelsesreglerne, da registrering af medarbejderes oplysninger udgør databehandling.

Eksempel: I *Digital Rights Ireland* ([6])-sagen blev EU-Domstolen bedt om at træffe afgørelse vedrørende gyldigheden af direktiv 2006/24/EF i lyset af de grundlæggende rettigheder til beskyttelse af personoplysninger og respekt for privatlivet, som er fastlagt i Den Europæiske Unions charter om grundlæggende rettigheder. Direktivet krævede, at udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller offentlige kommunikationsnetværk lagrede borgeres telekommunikationsdata i op til to år for at sikre, at dataene var tilgængelige i forbindelse med forebyggelse, efterforskning og retsforfølgelse af grov kriminalitet. Foranstaltningen omhandlede kun metadata, lokaliseringsdata og data, som er nødvendige til at identificere abonnenten eller brugeren. Den fandt ikke anvendelse for indholdet af elektroniske kommunikationer.

EU-Domstolen anså direktivet for at være et indgreb i den grundlæggende ret til beskyttelse af personoplysninger, »eftersom det foreskriver en behandling af personoplysninger« ([7]). Derudover konstaterede den, at direktivet

([6]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014.

([7]) *Ibid.*, præmis 36.

tilsidesatte retten til respekt for privatlivet ([8]). De personoplysninger, som blev lagret under direktivet, og som kunne tilgås af kompetente myndigheder, kunne tilsammen gøre det muligt »at drage meget præcise slutninger vedrørende privatlivet for de personer, hvis data er blevet lagret, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre færder, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer« ([9]). Indgrebet i de to rettigheder var vidtrækkende og af særligt alvorlig karakter.

EU-Domstolen erklærede direktiv 2006/24/EF for ugyldigt og konkluderede, at selvom det forfulgte et lovligt mål, så var indgrebet i rettighederne til beskyttelse af personoplysninger og privatlivet af alvorlig karakter og ikke begrænset til det strengt nødvendige.

1.1.2. Internationalt retsgrundlag: De Forenede Nationer

De Forenede Nationers retsgrundlag anerkender ikke beskyttelse af personoplysninger som en grundlæggende rettighed, selvom retten til privatlivets fred er en veletableret grundlæggende rettighed inden for den internationale retsorden. Artikel 12 i FN's Verdenserklæring om Menneskerettighederne om respekt for private forhold og familie ([10]) var første gang et internationalt instrument fastlagde en fysisk persons ret til beskyttelse af deres private sfære mod indblanding fra andre, navnlig staten. Selvom UDHR er en ikke-bindende erklæring, er den anerkendt som værende det instrument, der har ligget til grund for international menneskerettighedslovgivning, og den har påvirket udviklingen af andre menneskerettighedsinstrumenter i Europa. Den internationale konvention om borgerlige og politiske rettigheder (ICCPR) trådte i kraft i 1976. Den erklærede, at ingen må udsættes for vilkårlig eller ulovlig indblanding i sit privatliv eller familieliv, sit hjem eller sin brevveksling, eller for ulovlige angreb på sin ære og sit omdømme. ICCPR er en international traktat, der forpligter sine 169 parter til at respektere og sikre udøvelsen af det enkelte menneskes borgerlige rettigheder, herunder privatliv.

([8]) *Ibid.*, præmis 32-35.

([9]) *Ibid.*, præmis 27.

([10]) De Forenede Nationer (FN), verdenserklæring om menneskerettighederne (UDHR), 10. december 1948.

Siden 2013 har De Forenede Nationer vedtaget to resolutioner om privatliv benævnt »the right to privacy in the digital age« ([11]) som svar på udviklingen af nye teknologier og afsløringer af masseovervågningssystemer i nogle stater (Snowdens afsløringer). De fordømmer på det kraftigste masseovervågning og fremhæver virkningerne, som en sådan overvågning kan have på de grundlæggende rettigheder til privatliv og ytringsfrihed, og på den måde et levende og demokratisk samfund fungerer på. Selvom de ikke er retligt bindende, startede de en vigtig, international politisk debat på højt niveau om privatliv, nye teknologier og overvågning. De førte også til etableringen af en særlig rapportør om retten til privatlivet, som har mandat til at fremme og beskytte denne rettighed. Rapportørens specifikke opgaver omfatter indsamling af oplysninger om nationale praksisser og erfaringer i forbindelse med privatliv og de udfordringer, som opstår ved nye teknologier, udveksling og fremme af bedste praksis og identifikation af potentielle hindringer.

Selvom tidligere resolutioner fokuserede på de negative virkninger ved masseovervågning og staters ansvar for at begrænse efterretningsmyndigheders beføjelser, afspejler nyere resolutioner en vigtig udvikling i debatten om privatliv i De Forenede Nationer ([12]). Resolutionerne vedtaget i 2016 og 2017 bekræfter behovet for at begrænse efterretningstjenesters beføjelser og fordømme masseovervågning. De giver dog også tydeligt udtryk for, at »virksomheders stigende muligheder for at indsamle, behandle og benytte personoplysninger kan udgøre en fare for nydelsen af retten til privatliv i den digitale tidsalder«. Resolutionerne peger dermed mod privatsektorernes (og statsmyndighedernes) ansvar for at respektere menneskerettigheder og opfordrer virksomheder til at oplyse brugere om indsamling, brug, deling og lagring af personoplysninger og fastlægge gennemsigtige politikker for behandling.

1.1.3. Den europæiske menneskerettighedskonvention

Europarådet blev dannet i kølvandet på Anden Verdenskrig for at samle de europæiske stater med det formål at fremme retsstatsprincippet, demokrati, menneskerettigheder og social udvikling. Til det formål vedtog det i 1950 EMRK (den europæiske menneskerettighedskonvention), som trådte i kraft i 1953.

([11]) Se FN's Generalforsamling, Resolution on the right to privacy in the digital age, A/RES/68/167, New York, 18. december 2013; og FN's Generalforsamling, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, New York, 19. november 2014.

([12]) FN's Generalforsamling, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/Rev.1, New York, 16. november 2016; FN's Menneskerettighedsråd, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22. marts 2017.

Kontraherende parter har en international forpligtelse til at overholde EMRK. Alle Europarådets medlemsstater har nu indarbejdet eller gennemført EMRK i deres nationale ret, og det kræver, at de handler i overensstemmelse med konventionens bestemmelser. Kontraherende parter skal respektere rettighederne anført i konventionen, når de udfører en aktivitet eller udøver en beføjelse. Dette omfatter aktiviteter, som vedrører national sikkerhed. Principielle domme ved Den Europæiske Menneskerettighedsdomstol (EMD) har omhandlet statslige aktiviteter inden for følsomme områder med lovgivning og praksis for national sikkerhed ([13]). Domstolen tøvede ikke med at bekræfte, at overvågningsaktiviteter udgør et indgreb i respekten for privatlivet ([14]).

For at sikre, at de kontraherende parter overholder deres forpligtelser i henhold til EMRK, blev EMD etableret i Strasbourg, Frankrig, i 1959. EMD sikrer, at landene overholder deres forpligtelser i henhold til konventionen, ved at behandle klager fra enkeltpersoner, grupper af personer, NGO'er eller juridiske personer over overtrædelser af konventionen. EMD kan også undersøge mellemstatslige sager anlagt af én eller flere af Europarådets medlemsstater mod en anden medlemsstat.

I 2018 havde Europarådet 47 kontraherende parter, hvoraf 28 også er EU-medlemsstater. En sagsøger ved EMD behøver ikke være statsborger i en af de kontraherende parter, dog skal påståede overtrædelser finde sted inden for en af de kontraherende parters område.

Retten til beskyttelse af personoplysninger er en del af de rettigheder, der er beskyttet under artikel 8 i EMRK, som garanterer retten til respekt for privatliv og familieliv, hjem og korrespondance og fastlægger de omstændigheder, hvorunder begrænsninger af denne rettighed tillades ([15]).

EMD har undersøgt adskillige problemstillinger vedrørende databeskyttelse. Disse omfatter opfangelse af kommunikationer ([16]), forskellige former for overvågning af

([13]) Se f.eks.: EMD, *Klass m.fl. mod Tyskland*, nr. 5029/71, 6. september 1978; EMD, *Rotaru mod Rumænien* [GC], nr. 28341/95, 4. maj 2000 og EMD, *Szabó og Vissy mod Ungarn*, nr. 37138/14, 12. januar 2016.

([14]) *Ibid.*

([15]) Europarådet, Den europæiske menneskerettighedskonvention, CETS nr. 005, 1950.

([16]) Se f.eks.: EMD, *Malone mod Det Forenede Kongerige*, nr. 8691/79, 2. august 1984; EMD, *Copland mod Det Forenede Kongerige*, nr. 62617/00, 3. april 2007 eller EMD, *Mustafa Sezgin Tanrıkulu mod Tyrkiet,* nr. 27473/06, 18. juli 2017.

både de private og offentlige sektorer ([17]) og beskyttelse mod offentlige myndigheders lagring af personoplysninger ([18]). Respekt for privatlivet er ikke en absolut ret, da udøvelsen af retten til privatliv kan tilsidesætte andre rettigheder, såsom ytringsfrihed og adgang til informationer, og omvendt. Domstolen sigter derfor efter at finde en balance mellem de forskellige rettigheder, der er på spil. Den har præciseret, at artikel 8 i EMRK ikke kun forpligter stater til at undlade at foretage handlinger, der kan være i strid med denne konventionssikrede rettighed, men også at de under visse omstændigheder er underlagt positive forpligtelser til aktivt at sikre effektiv beskyttelse af privatliv og familieliv ([19]). Mange af disse sager er beskrevet i detaljer i de relevante kapitler.

1.1.4. Europarådets konvention 108

Med indførelsen af informationsteknologi i 1960'erne opstod der et stigende behov for mere detaljerede regler, der kunne beskytte enkeltpersoners personoplysninger. I midten af 1970'erne vedtog Europarådets Ministerkomité en række resolutioner om beskyttelse af personoplysninger under henvisning til artikel 8 i EMRK ([20]). I 1981 blev en konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108) ([21]) åbnet for undertegnelse. Konvention 108 var og er stadig det eneste retligt bindende internationale instrument vedrørende databeskyttelse.

Konvention 108 finder anvendelse på enhver databehandling, der udføres af både den private sektor og offentlige sektor, inklusive databehandling ved retsvæsnet og retshåndhævende myndigheder. Konventionen beskytter det enkelte menneske mod misbrug i forbindelse med behandling af personoplysninger og har samtidig til formål at regulere grænseoverskridende overførsler af personoplysninger. Hvad angår behandling af personoplysninger, vedrører konventionens principper

([17]) Se f.eks.: EMD, *Klass m.fl. mod Tyskland*, nr. 5029/71, 6. september 1978; EMD, *Uzun mod Tyskland*, nr. 35623/05, 2. september 2010.

([18]) Se f.eks.: EMD, *Roman Zakharov mod Rusland*, nr. 47143/06, 4. december 2015; EMD, *Szabó og Vissy mod Ungarn*, nr. 37138/14, 12. januar 2016.

([19]) Se f.eks.: EMD, *I mod Finland*, nr. 20511/03, 17. juli 2008; EMD, *K.U. mod Finland*, nr. 2872/02, 2. december 2008.

([20]) Europarådet, Ministerkomité (1973), resolution (73)22 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger i den private sektor, 26. september 1973; Europarådet, Ministerkomité (1974), resolution (74)29 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger i den offentlige sektor, 20. september 1974.

([21]) Europarådet, konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, ETS nr. 108, 1981.

især rimelig og lovlig indsamling og automatisk behandling af personoplysninger til nærmere bestemte, legitime formål. Dette betyder, at personoplysningerne ikke må anvendes på en måde, der er uforenelig med disse formål, og de bør ikke lagres i længere tid end nødvendigt. De vedrører også kvaliteten af personoplysninger, navnlig at de skal være relevante, tilstrækkelige, ikke omfatte mere end nødvendigt (proportionalitet) og være nøjagtige.

Ud over at give garantier om behandlingen af personoplysninger og datasikkerhedsforpligtelser forbyder den behandling af »følsomme« personoplysninger, som f.eks. en persons race, politiske tilhørsforhold, sundhed, religion, seksualitet eller straffeattest, hvis der ikke foreligger tilstrækkelige retsgarantier.

Konventionen sikrer også det enkelte menneskes ret til at vide, hvilke oplysninger der er lagret om ham eller hende, og om nødvendigt at få dem korrigeret. Begrænsninger af de rettigheder, der er fastlagt ved konventionen, tillades kun, når samfundsmæssige hensyn, herunder statens sikkerhed eller forsvar, kræver det. Derudover sikrer konventionen fri udveksling af personoplysninger mellem dennes kontraherende parter og indfører visse begrænsninger for overførsler til stater, hvis retssystem ikke yder tilsvarende beskyttelse.

Det bør bemærkes, at konvention 108 er bindende for stater, som har ratificeret den. Den er ikke underlagt EMD's retslige tilsyn, men konventionen er taget i betragtning i EMD's retspraksis i forbindelse med artikel 8 i EMRK. Igennem årene har domstolen fastslået, at beskyttelse af personoplysninger er en vigtig del af retten til respekt for privatliv (artikel 8), og den har fulgt principperne i konvention 108 ved bestemmelse af, om der har været et indgreb i denne grundlæggende rettighed ([22]) .

For yderligere at udvikle de generelle principper og regler, der er fastlagt ved konvention 108, har Europarådets Ministerkomité vedtaget en række henstillinger, som ikke er retligt bindende. Disse henstillinger har påvirket databeskyttelseslovgivningens udvikling i Europa. For eksempel var henstillingen om politiets brug af personoplysninger i mange år det eneste instrument i Europa, som vejledte omkring brugen af personoplysninger inden for politisektoren ([23]). Henstillingens principper, såsom metoder til lagring af datafiler og behovet for at gennemføre klare regler om, hvilke personer der har lov til at tilgå disse filer, blev udviklet i større grad og

([22]) Se f.eks.: EMD, *Z mod Finland*, nr. 22009/93, 25. februar 1997.

([23]) Europarådet, Ministerkomité (1987), Henstilling Rec(87)15 til medlemsstaterne om politiets brug af personoplysninger, Strasbourg, 17. september 1987.

afspejles i den efterfølgende EU-lovgivning ([24]). Nylige henstillinger har sigtet efter at håndtere den digitale tidsalders udfordringer, såsom databehandling i forbindelse med beskæftigelse (se kapitel 9).

Alle EU's medlemsstater har ratificeret konvention 108. I 1999 blev ændringer af konvention 108 foreslået, så EU kunne blive en part, men de trådte aldrig i kraft ([25]). I 2001 blev der vedtaget en tillægsprotokol til konvention 108. Den indførte bestemmelser om grænseoverskridende videregivelse af personoplysninger til såkaldte tredjelande, der ikke er parter, og om obligatorisk oprettelse af nationale databeskyttelsesmyndigheder ([26]).

Konvention 108 kan tiltrædes af lande, som ikke er kontraherende parter i Europarådet. Konventionens potentiale som en universel standard og dens åbne karakter kan være et grundlag for at fremme databeskyttelse på globalt plan. Indtil videre er 51 lande kontraherende parter i konvention 108. De omfatter alle Europarådets medlemsstater (47 lande), Uruguay, som i august 2013 var det første land uden for EU til at tiltræde, og Mauritius, Senegal og Tunesien, der tiltrådte i 2016 og 2017.

Konventionen gennemgik for nylig en moderniseringsproces. En offentlig høring udført i 2011 bekræftede arbejdets to primære mål: forstærkning af beskyttelsen af privatliv på det digitale område og forstærkning af konventionens opfølgningsmekanisme. Moderniseringsprocessen fokuserede på disse mål og blev fuldført med vedtagelsen af en ændringsprotokol til konvention 108 (protokol, CETS nr. 223). Arbejdet blev udført på samme tid som andre reformer af internationale databeskyttelsesinstrumenter og sammen med reformen af EU's databeskyttelsesregler, der blev lanceret i 2012. Kontrolorganer hos Europarådet og på EU-plan har så vidt muligt sikret sammenhæng og forenelighed mellem de to retsgrundlag. Moderniseringen bevarer konventionens generelle og fleksible karakter og forstærker dens potentiale som et universalt instrument om databeskyttelseslovgivning. Den

([24]) Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, EFT L 281 af 23. november 1995.

([25]) Europarådet, ændringer af konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (ETS nr. 108), der blev vedtaget af Ministerkomitéen i Strasbourg den 15. juni 1999.

([26]) Europarådet, tillægsprotokol til konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger omkring tilsynsmyndigheder og grænseoverskridende videregivelse af personoplysninger, CETS nr. 181, 2001. Med moderniseringen af konvention 108 finder denne protokol ikke længere anvendelse, da dens bestemmelser er blevet ajourført og integreret i den moderniserede konvention 108.

bekræfter og stabiliserer vigtige principper og tildeler fysiske personer nye rettigheder, mens den på samme tid øger ansvarsområderne for enheder, der behandler personoplysninger, og sikrer større ansvarlighed. For eksempel har fysiske personer, hvis personoplysninger behandles, ret til at få baggrunden for denne databehandling at vide og ret til at gøre indsigelse mod behandlingen. For at modarbejde den stigende grad af profilering i den digitale verden fastlægger konventionen også fysiske personers ret til ikke at være underlagt afgørelser udelukkende på baggrund af automatisk behandling, uden at personernes egne holdninger tages under overvejelse. Det, at kontraherende parters uafhængige tilsynsmyndigheder effektivt håndhæver databeskyttelsesregler, anses som værende centralt for konventionens praktiske gennemførelse. Til det formål understreger den moderniserede konvention behovet for, at tilsynsmyndigheder pålægges effektive beføjelser og funktioner og er reelt uafhængige under opfyldelse af deres opgave.

1.1.5. EU's databeskyttelseslovgivning

EU-retten består af primær og afledt EU-ret. Traktaterne, navnlig traktaten om Den Europæiske Union (TEU) og traktaten om Den Europæiske Unions funktionsmåde (TEUF), er blevet ratificeret af alle EU's medlemsstater og kaldes også »EU's primære ret«. EU's forordninger, direktiver og afgørelser er blevet vedtaget af de EU-institutioner, som har beføjelse hertil i medfør af traktaterne. De betegnes ofte som »afledt EU-ret«.

Databeskyttelse i primær EU-ret

De Europæiske Fællesskabers oprindelige traktater indeholdt ingen henvisninger til menneskerettigheder eller deres beskyttelse, da det Europæiske Økonomiske Fællesskab oprindeligt blev planlagt som værende en regional organisation, der fokuserede på økonomisk integration og oprettelsen af et fælles marked. Et grundlæggende princip bag oprettelsen og udviklingen af De Europæiske Fællesskaber — og ét som stadig er gældende idag — er princippet om kompetencetildeling. I henhold til dette princip handler EU kun inden for grænserne af de kompetencer, som den har fået tildelt af sine medlemsstater, hvilket afspejles af EU-traktaterne. I modsætning til Europarådet indeholder EU-traktaterne ingen eksplicitte kompetencer inden for grundlæggende rettigheder.

Efterhånden som sager med påstande om krænkelser af menneskerettighederne blev indbragt for EU-Domstolen inden for rammerne af EU-retten, gav EU-Domstolen dog en vigtig fortolkning af traktaterne. For at beskytte enkeltpersoner blev grundlæggende rettigheder gjort til en del af europæisk rets såkaldte generelle

principper. I henhold til EU-Domstolen afspejler disse generelle principper indholdet af de bestemmelser om menneskerettigheder, der findes i nationale forfatninger og menneskerettighedstraktater, navnlig EMRK. EU-Domstolen fastlagde, at den vil sikre, at EU-retten er i overensstemmelse med disse principper.

I erkendelse af, at EU's politikker kan have betydning for menneskerettighederne, og for at få borgerne til at føle sig »tættere« på EU, bekendtgjorde EU i 2000 Den Europæiske Unions charter om grundlæggende rettigheder (Chartret). Dette Charter omfatter de europæiske borgeres civile, politiske, økonomiske og sociale rettigheder, idet det forener de forfatningsmæssige traditioner og internationale forpligtelser, som er fælles for medlemsstaterne. De rettigheder, der er beskrevet i Chartret, er opdelt i seks afsnit: værdighed, friheder, ligestilling, solidaritet, borgerrettigheder og retfærdighed.

Chartret var oprindeligt kun et politisk dokument, men det blev retligt bindende ([27]) som primær EU-ret (se artikel 6, stk. 1, i TEU) med Lissabontraktatens ikrafttræden den 1. december 2009 ([28]). Chartrets bestemmelser er rettet mod EU's institutioner og organer og forpligter dem til at respektere de rettigheder, som Chartret indeholder, når de udfører deres pligter. Chartrets bestemmelser binder også medlemsstater, når de implementerer EU-ret.

Chartret sikrer ikke kun respekt for privatliv og familieliv (artikel 7), men fastlægger også retten til beskyttelse af personoplysninger (artikel 8). Chartret ophøjer derved udtrykkeligt denne beskyttelse til samme niveau som en grundlæggende rettighed i EU-retten. EU-institutioner og -organer skal respektere og garantere denne rettighed, som også gælder for medlemsstaterne, når de gennemfører EU-retten (Chartrets artikel 51). Chartrets artikel 8 blev formuleret flere år efter databeskyttelsesdirektivet og skal fortolkes således, at den omfatter EU's allerede eksisterende lovgivning om databeskyttelse. Chartret nævner derfor ikke kun udtrykkeligt retten til databeskyttelse i artikel 8, stk. 1, men henviser også til vigtige principper for databeskyttelse i artikel 8, stk. 2. Endelig kræver Chartrets artikel 8, stk. 3, at gennemførelsen af disse principper er underlagt en uafhængig myndigheds kontrol.

Vedtagelsen af Lissabontraktaten er en milepæl inden for udviklingen af databeskyttelseslovgivning. Den ophøjede Chartrets status til et bindende retligt dokument inden for primær ret, og fastlagde retten til beskyttelse af personoplysninger. Denne ret er specifikt fastlagt i artikel 16 i TEUF i den del af traktaten, som er dedikeret til

([27]) EU (2012), Den Europæiske Unions charter om grundlæggende rettigheder, EUT 2012 C 326.

([28]) Se konsoliderede udgaver af De Europæiske Fællesskaber (2012), traktaten om Den Europæiske Union, EUT 2012 C 326, og De Europæiske Fællesskaber (2012), TEUF, EUT 2012 C 326.

EU's generelle principper. Artikel 16 opretter også et nyt retsgrundlag, hvor EU tildeles kompetencer til at lovgive omkring databeskyttelse. Dette er en vigtig udvikling, da EU's databeskyttelsesregler — navnlig databeskyttelsesdirektivet — oprindeligt var baseret på retsgrundlaget for det indre marked samt behovet for at tilnærme sig de nationale lovgivninger, så den frie udveksling af oplysninger inden for EU ikke begrænses. Artikel 16 i TEUF giver nu et uafhængigt retsgrundlag for en moderne, udførlig tilgang til databeskyttelse, der omfatter alle aspekter af EU's kompetencer, inklusive politisamarbejde og retligt samarbejde i kriminalsager. Artikel 16 i TEUF bekræfter også, at overholdelse af databeskyttelsesregler, som er vedtaget i medfør heraf, skal være underlagt uafhængige tilsynsmyndigheders kontrol. Artikel 16 fungerede som retsgrundlag for vedtagelsen af den omfattende reform af databeskyttelsesregler i 2016, dvs. den generelle forordning om databeskyttelse og databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder (se nedenfor).

Den generelle forordning om databeskyttelse

Fra 1995 og indtil maj 2018 var EU's primære retslige instrument om databeskyttelse Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesdirektivet) ([29]). Det blev vedtaget i 1995 på et tidspunkt, hvor flere medlemsstater allerede havde vedtaget nationale databeskyttelseslove ([30]), og opstod ud fra behovet om at harmonisere disse love og sikre et højere beskyttelsesniveau og den frie udveksling af personoplysninger imellem de forskellige medlemsstater. Den frie bevægelighed for varer, kapital, tjenesteydelser og personer inden for det indre marked forudsatte fri udveksling af personoplysninger, og det ville ikke være muligt, medmindre medlemsstaterne etablerede et ensartet højt niveau af databeskyttelse.

Databeskyttelsesdirektivet afspejler de databeskyttelsesprincipper, som allerede findes i nationale love og i konvention 108, og udvidede dem ofte. Den tog udgangspunkt i muligheden for at udvide beskyttelsesinstrumenter, som er fastlagt i artikel 11 i konvention 108. Navnlig viste direktivets introduktion om uafhængigt tilsyn som et instrument til at forbedre overholdelse af databeskyttelsesregler sig

([29]) Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, EUT L 281 af 23. november 1995.

([30]) Den tyske delstat Hessen vedtog verdens første lov om databeskyttelse i 1970, som kun var gældende i den delstat. Sverige vedtog *Datalagen* i 1973, Tyskland vedtog *Bundesdatenschutzgestez* i 1976 og Frankrig vedtog *Loi relatif à l'informatique, aux fichiers et aux libertés* i 1977. I Det Forenede Kongerige blev **Data Protection Act** vedtaget i 1984. Endelig vedtog Nederlandene *Wet Persoonregistraties* i 1989.

at være en vigtig del af den effektive funktion af europæisk databeskyttelseslovgivning. Som følge heraf blev denne funktion indarbejdet i Europarådets lovgivning i 2001 ved tillægsprotokollen til konvention 108. Dette viser, hvordan de to instrumenter har haft et tæt samspil og en positiv indflydelse på hinanden i løbet af årene.

Databeskyttelsesdirektivet fastlagde et detaljeret og omfattende databeskyttelsessystem i EU. I overensstemmelse med EU's retsorden finder direktiver dog ikke direkte anvendelse og skal gennemføres i medlemsstaternes nationale lovgivning. Derfor har medlemsstater skønsbeføjelser ved gennemførelse af direktivets bestemmelser. Selvom direktivets formål var fuldstændig harmonisering ([31]) (og et fuldstændigt beskyttelsesniveau), blev det i praksis gennemført på anden vis i medlemsstaterne. Dette førte til etablering af forskellige databeskyttelsesregler i EU, hvor definitioner og regler blev fortolket på forskellige måder i nationale lovgivninger. Håndhævelsesniveauer og sanktionernes omfang var også forskellige i medlemsstaterne. Endelig har der været væsentlige ændringer inden for informationsteknologi siden direktivets udarbejdelse i midten af 1990'erne. Samlet set dannede disse årsager grundlaget for reformen af EU's databeskyttelseslovgivning.

Reformen førte til vedtagelsen af den generelle forordning om databeskyttelse i april 2016 efter mange års intens debat. Debatterne om behovet for at modernisere EU's databeskyttelsesregler begyndte i 2009, da Kommissionen iværksatte en offentlig høring om det fremtidige retsgrundlag for den grundlæggende ret til beskyttelse af personoplysninger. Forslaget til forordningen blev offentliggjort af Kommissionen i januar 2012, hvilket startede en lang lovgivningsprocedure med forhandlinger imellem Europa-Parlamentet og EU-Rådet. Den generelle forordning om databeskyttelse fastsatte en to-årig overgangsperiode efter sin vedtagelse. Den trådte fuldstændig i kraft den 25. maj 2018, hvor databeskyttelsesdirektivet blev ophævet.

Vedtagelsen af den generelle forordning om databeskyttelse i 2016 moderniserede EU's databeskyttelseslovgivning, hvilket gjorde den egnet til at beskytte grundlæggende rettigheder på baggrund af den digitale tidsalders økonomiske og sociale udfordringer. GDPR bevarer og udvikler de kerneprincipper og den registreredes rettigheder, som er fastlagt i databeskyttelsesdirektivet. Desuden indførte den nye forpligtelser med krav om, at organisationer implementerer databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, udpeger

([31]) EU-Domstolen, forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado*, 24. november 2011, præmis 29.

en databeskyttelsesrådgiver under visse omstændigheder, overholder en ny ret til dataportabilitet samt overholder ansvarlighedsprincippet. Under EU-retten gælder forordninger umiddelbart, og det er ikke nødvendigt med en national gennemførelse. Den generelle forordning om databeskyttelse fastlægger derfor et enkelt sæt databeskyttelsesregler for hele EU. Databeskyttelsesreglerne er derfor konsistente i hele Unionen, og det giver et retssikkerhedsmiljø, som erhvervsdrivende og fysiske personer kan drage nytte af som »registrerede«.

Selvom den generelle forordning om databeskyttelse gælder umiddelbart, forventes det dog, at medlemsstater ajourfører deres eksisterende nationale databeskyttelseslove, så de bringes helt i overensstemmelse med forordningen, hvilket også er et udtryk for skønsbeføjelsen over specifikke bestemmelser i betragtning 10. Forordningens hovedregler og -principper og de stærke rettigheder, som den tildeler fysiske personer, udgør en stor del af håndbogen og er beskrevet i de følgende kapitler. Forordningen har omfattende regler om territorialt anvendelsesområde. Den gælder både for virksomheder etableret i EU og for dataansvarlige og databehandlere, som ikke er etableret i EU og udbyder varer eller tjenesteydelser til registrerede i EU eller overvåger de registreredes adfærd. Da flere oversøiske virksomheder besidder en væsentlig andel i det europæiske marked og har mange millioner europæiske kunder, er det vigtigt at underkaste disse organisationer for EU's databeskyttelsesregler for at sikre beskyttelsen af det enkelte menneske samt lige konkurrencevilkår.

Databeskyttelse i forbindelse med retshåndhævelse — direktiv (EU) 2016/680

Det ophævede databeskyttelsesdirektiv fastlagde en omfattende databeskyttelsesordning. Denne ordning er nu forbedret med vedtagelsen af den generelle forordning om databeskyttelse. Det ophævede databeskyttelsesdirektivs omfang var omfattende, men begrænset til aktiviteter, som hører under det indre marked, og til aktiviteter for offentlige myndigheder, som ikke er retshåndhævende myndigheder. Vedtagelsen af særlige instrumenter var derfor et krav for at opnå den nødvendige klarhed og balance mellem databeskyttelse og andre legitime interesser samt at håndtere de udfordringer, som er særligt gældende for specifikke sektorer. Dette er tilfældet for regler om retshåndhævende myndigheders behandling af personoplysninger.

EU's første retslige instrument på dette område var Rådets rammeafgørelse 2008/977/RIA om beskyttelse af personoplysninger i forbindelse med

politisamarbejde og retligt samarbejde i kriminalsager. Rammeafgørelsens regler fandt kun anvendelse for politimæssige og retlige oplysninger, der udveksles mellem medlemsstater. Retshåndhævende myndigheders indenlandske behandling af personoplysninger var derfor ikke en del af dens anvendelsesområde.

Direktiv (EU) 2016/680 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger ([32]), benævnt som databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder, korrigerede denne situation. Direktivet blev vedtaget på samme tid som den generelle forordning om databeskyttelse ophævede rammeafgørelse 2008/977/RIA og fastlagde et omfattende system til beskyttelse af personoplysninger i forbindelse med retshåndhævelse, hvor det stadig tog hensyn til de særlige aspekter ved databehandling vedrørende offentlig sikkerhed. Selvom den generelle forordning om databeskyttelse fastlægger generelle regler for at beskytte fysiske personer i forbindelse med behandlingen af deres personoplysninger, og for at sikre den frie udveksling af sådanne oplysninger inden for EU, fastlægger direktivet specifikke regler for databeskyttelse på områderne for politisamarbejde og retligt samarbejde i kriminalsager. Når en kompetent myndighed behandler personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, finder direktiv (EU) 2016/680 anvendelse. Når kompetente myndigheder behandler personoplysninger til andre formål end de ovennævnte, finder de generelle regler i den generelle forordning om databeskyttelse anvendelse. Anvendelsesområdet for direktiv (EU) 2016/680 omfatter retshåndhævende myndigheders indenlandske behandling af personoplysninger, hvilket ikke var tilfældet for direktivets forgænger (Rådets rammeafgørelse 2008/977/RIA), og det er ikke begrænset til udvekslinger af sådanne oplysninger imellem medlemsstater. Derudover sigter direktivet mod at opnå en balance mellem fysiske personers rettigheder og de legitime mål med databehandling vedrørende offentlig sikkerhed.

Til dette formål bekræfter direktivet retten til beskyttelse af personoplysninger og de kerneprincipper, som bør omfatte databehandling, hvilket tæt følger de regler og principper, der er fastlagt i den generelle forordning om databeskyttelse. Fysiske personers rettigheder og forpligtelser pålagt dataansvarlige — for eksempel

([32]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger, EUT L 119 af 4. maj 2016.

i forbindelse med datasikkerhed, databeskyttelse gennem design og standardindstillinger og anmeldelse af databrud — ligner rettighederne og forpligtelserne i den generelle forordning om databeskyttelse. Direktivet tager også hensyn til, og prøver at løse, alvorlige nye teknologiske udfordringer, der kan have særligt belastende konsekvenser for fysiske personer, såsom retshåndhævende myndigheders brug af profileringsteknikker. Principielt skal afgørelser udelukkende baseret på automatisk behandling, herunder profilering, forbydes ([33]). Derudover må de ikke være baseret på følsomme oplysninger. Sådanne principper er underlagt visse undtagelser fastlagt i direktivet. Endelig må en sådan behandling ikke resultere i diskrimination mod en person ([34]).

Direktivet indeholder også regler for at sikre ansvarlighed hos de dataansvarlige. De skal udpege en databeskyttelsesrådgiver til at overvåge overholdelse af databeskyttelsesreglerne, underrette og rådgive enheden og ansatte, som behandler personoplysninger, om deres forpligtelser og samarbejde med tilsynsmyndigheden. Behandling af personoplysninger inden for politi- og strafferetsområdet er nu underlagt tilsyn ved uafhængige tilsynsmyndigheder. Både den generelle retlige ordning for databeskyttelse og den særlige ordning for databeskyttelse for retshåndhævelse og straffesager skal overholde kravene i Den Europæiske Unions charter om grundlæggende rettigheder.

Den særlige ordning for databehandling i forbindelse med politisamarbejde og retligt samarbejde etableret ved databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder er beskrevet i detaljer i kapitel 8.

Direktiv om databeskyttelse inden for elektronisk kommunikation

Man fandt det også nødvendigt at fastlægge særlige databeskyttelsesregler inden for den elektroniske kommunikationssektor. Med udviklingen af internettet, fastnet- og mobiltelefoni blev det vigtigt at sikre, at brugeres ret til privatliv og fortrolighed blev overholdt. Direktiv 2002/58/EF ([35]) om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation

([33]) Databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder, artikel 11, stk. 1.

([34]) *Ibid.*, artikel 11, stk. 2 og 3.

([35]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation eller e-databeskyttelsesdirektivet), EFT 201 af 31. juli 2002.

eller e-databeskyttelsesdirektivet) fastlægger regler for sikkerheden af personoplysninger inden for disse netværk, meddelelse af personlige databrud og kommunikationshemmeligheden.

I forbindelse med sikkerhed skal udbydere af elektroniske kommunikationstjenester, bl.a., sikre, at adgangen til personoplysninger udelukkende er begrænset til godkendte personer, og træffe foranstaltninger til at forhindre destruktion, tab eller utilsigtet beskadigelse af personoplysninger ([36]). Når der er en særlig risiko for brud på sikkerheden for det offentlige kommunikationsnet, skal udbydere oplyse abonnenter om risikoen ([37]). Hvis et brud på sikkerheden på trods af de implementerede sikkerhedsforanstaltninger finder sted, skal udbydere meddele den kompetente nationale myndighed, som er ansvarlig for at gennemføre og håndhæve direktivet, om bruddet på persondatasikkerheden. Udbydere skal til tider også meddele brud på persondatasikkerheden til enkeltpersoner, navnlig når bruddet med sandsynlighed påvirker deres personoplysninger eller privatliv på negativ vis ([38]). Kommunikationshemmeligheden kræver, at aflytning, registrering, lagring eller enhver form for overvågning eller opfangelse af kommunikationer og metadata principielt er forbudt. Direktivet forbyder også uanmodet kommunikation (ofte kaldet »spam«), medmindre brugeren har afgivet samtykke hertil, og indeholder regler om lagring af »cookies« på computere og enheder. Disse primære negative forpligtelser angiver tydeligt, at kommunikationshemmeligheden er væsentligt knyttet til beskyttelse af retten til respekt for privatliv, der er fastlagt i artikel 7 i Chartret, og retten til beskyttelse af personoplysninger, der er fastlagt i artikel 8 i Chartret.

I januar 2017 offentliggjorde Kommissionen et forslag til en forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation, som skulle erstatte e-databeskyttelsesdirektivet. Reformen har til formål at tilpasse reglerne for elektronisk kommunikation med de nye regler for databeskyttelse fastlagt i den generelle forordning om databeskyttelse. Den nye forordning gælder umiddelbart i hele EU. Alle fysiske personer vil modtage samme grad af beskyttelse af deres elektroniske kommunikationer, og teleoperatører og virksomheder vil nyde godt af klarhed, retssikkerhed og tilstedeværelsen af et enkelt regelsæt for hele EU. De foreslåede regler om fortroligheden af elektroniske kommunikationer finder også anvendelse for nye aktører, som leverer elektroniske kommunikationstjenester, der ikke er omfattet af e-databeskyttelsesdirektivet.

([36]) Direktiv om databeskyttelse inden for elektronisk kommunikation, artikel 4, stk. 1.

([37]) *Ibid*., artikel 4, stk. 2.

([38]) *Ibid*., artikel 4, stk. 3.

Sidstnævnte omfattede kun traditionelle udbydere af telekommunikationstjenester. Med den voldsomme stigning i brugen af tjenester, såsom Skype, WhatsApp, Facebook Messenger og Viber, til at sende beskeder eller foretage opkald, er disse OTT-tjenester nu omfattet af forordningen og skal overholde dennes krav til databeskyttelse, privatliv og sikkerhed. Ved tidspunktet for offentliggørelsen af denne håndbog var en lovgivningsprocedure om e-databeskyttelsesreglerne stadig igangværende.

Forordning (EF) nr. 45/2001

Da databeskyttelsesdirektivet kun gælder for EU-medlemsstater, var det nødvendigt med et nyt retsligt instrument for at sikre databeskyttelse for EU-institutioners og -organers behandling af personoplysninger. Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (forordning om databeskyttelse inden for EU-institutionerne) opfylder denne opgave ([39]).

Forordning (EF) nr. 45/2001 følger principperne i den generelle databeskyttelsesordning for EU tæt, og disse principper gælder for databehandling, som udføres af EU's institutioner og organer under udøvelsen af deres funktioner. Desuden fastlægger den en uafhængig kontrolmyndighed til at overvåge anvendelsen af forordningens bestemmelser: den europæiske tilsynsførende for databeskyttelse (EDPS). EDPS er tillagt tilsynsbeføjelser og er forpligtet til at overvåge behandlingen af personoplysninger inden for EU's institutioner og organer samt behandle og undersøge klager om påståede brud på databeskyttelsesreglerne. Den rådgiver også EU's institutioner og organer om alle spørgsmål vedrørende beskyttelse af personoplysninger, hvilket spænder fra forslag til ny lovgivning til udkast til interne regler omkring databehandling.

I januar 2017 fremsatte Europa-Kommissionen et forslag om en ny forordning om EU-institutioners databehandling, som skulle ophæve den gældende forordning. Ligesom reformen af e-databeskyttelsesdirektivet skal reformen af forordning (EF) nr. 45/2001 modernisere og tilpasse reglerne deri til de nye regler for databeskyttelse fastlagt i den generelle forordning om databeskyttelse.

([39]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, EFT L 8 af 12. januar 2001.

EU-Domstolens rolle

EU-Domstolen har kompetence til at bestemme, om en medlemsstat har opfyldt sine forpligtelser under EU's databeskyttelseslovgivning, og til at fortolke EU-ret for at sikre den effektive og ensartede anvendelse heraf i medlemsstaterne. Siden vedtagelsen af databeskyttelsesdirektivet i 1995 er der opbygget en omfattende retspraksis, som præciserer omfanget og betydningen af principperne for databeskyttelse og den grundlæggende ret til beskyttelse af personoplysninger, som er fastlagt i artikel 8 i Chartret. Selvom direktivet er ophævet, og et nyt retsligt instrument — den generelle forordning om databeskyttelse — er gældende, forbliver den allerede eksisterende retspraksis relevant og gyldig i forbindelse med fortolkning og anvendelse af principperne for databeskyttelse i det omfang, at databeskyttelsesdirektivets kerneprincipper og -begreber blev bevaret i GDPR.

1.2. Begrænsninger af retten til beskyttelse af personoplysninger

Hovedpunkter

- Retten til beskyttelse af personoplysninger er ikke en absolut rettighed. Den kan være begrænset, hvis det er nødvendigt til at opnå et mål af almen interesse eller til at beskytte andres rettigheder og friheder.
- Betingelserne for begrænsning af retten til respekt for privatlivet og beskyttelse af personoplysninger er anført i artikel 8 i EMRK og artikel 52, stk. 1, i Chartret. De er udviklet og fortolket igennem EMD og EU-Domstolens retspraksis.
- I medfør af Europarådets databeskyttelseslovgivning er behandling af personoplysninger kun en lovlig indblanding i retten til respekt for privatlivet og må kun udføres, hvis denne:
  - er i overensstemmelse med loven
  - forfølger et legitimt mål
  - respekterer disse rettigheders og friheders væsentligste indhold
  - er nødvendig og forholdsmæssig i et demokratisk samfund til at opfylde et legitimt mål.

- EU's retsorden har lignende betingelser for begrænsninger af udøvelsen af grundlæggende rettigheder, som er beskyttet af Chartret. Enhver begrænsning af en grundlæggende rettighed, inklusive beskyttelse af personoplysninger, er kun lovlig, hvis den:
  - er i overensstemmelse med loven
  - respekterer rettighedens væsentligste indhold
  - under iagttagelse af proportionalitetsprincippet er nødvendig
  - forfølger et mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder.

Den grundlæggende rettighed til beskyttelse af personoplysninger under artikel 8 i Chartret er ikke en absolut rettighed, »men skal ses i sammenhæng med sin funktion i samfundet« ([40]). Chartrets artikel 52, stk. 1, giver endvidere mulighed for, at der kan indføres begrænsninger i udøvelsen af rettighederne fastsat i Chartrets artikel 7 og 8, for så vidt som disse begrænsninger er fastlagt i , respekterer disse rettigheders og friheders væsentligste indhold, og at de under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder ([41]). På lignende vis sikres databeskyttelse af artikel 8 under EMRK-systemet, og udøvelsen af den ret kan om nødvendigt være begrænset for at forfølge et legitimt mål. Dette afsnit henviser til betingelserne for indgreb under EMRK, som fortolket i EMD's retspraksis, samt betingelserne for lovlige begrænsninger under Chartrets artikel 52.

1.2.1. Kravene til begrundede indgreb i henhold til EMRK

Behandlingen af personoplysninger kan udgøre et indgreb i den registreredes ret til respekt for privatlivet, som er beskyttet ved artikel 8 i EMRK ([42]). Som forklaret tidligere (se afsnit 1.1.1. og afsnit 1.1.4.) fastlægger EMRK dog ikke, at retten til respekt for privatlivet er en selvstændig grundlæggende rettighed, i modsætning til EU's retsorden. Beskyttelse af personoplysninger er nærmere en del af rettighederne,

([40]) Se, f.eks., EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 9. november 2010, præmis 48.

([41]) *Ibid.*, præmis 50.

([42]) EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 8. december 2008, præmis 67.

som er beskyttet under retten til respekt for privatlivet. Ingen aktivitet, som involverer behandling af personoplysninger, kan derfor være omfattet af artikel 8 i EMRK. For at artikel 8 kan udløses, skal det først fastlægges, om en privat interesse eller en persons privatliv er kompromitteret. EMD har igennem sin retspraksis fortolket begrebet »privatliv« som et bredt koncept, der sågar omfatter aspekter af en persons arbejdsliv og offentlige adfærd. Den har også fastslået, at beskyttelsen af personoplysninger er en vigtig del af retten til respekt for privatlivet. På trods af den brede fortolkning af privatliv er det ikke alle former for behandling, som alene overtræder rettighederne beskyttet under artikel 8.

Hvis EMD mener, at den pågældende behandlingsaktivitet påvirker en fysisk persons ret til respekt for privatliv, undersøger den, om indgrebet er begrundet. Retten til respekt for privatlivet er ikke en absolut ret, men skal afvejes i forhold til og forenes med andre legitime interesser og rettigheder, uanset om det drejer sig om andre personers interesser (private interesser) eller samfundsmæssige interesser (offentlige interesser).

De kumulative betingelser, hvorunder indgreb kan begrundes, er:

I overensstemmelse med loven

I henhold til EMD's retspraksis er indgreb i overensstemmelse med loven, hvis de er baseret på en bestemmelse i en national retsforskrift, som opfylder bestemte kriterier. Retsforskriften skal være tilgængelig, og virkningerne af den skal være forudsigelige ([43]). En regel betragtes som forudsigelig, hvis den er formuleret tilstrækkelig præcist til, at enhver person – om nødvendigt med passende rådgivning – kan regulere sin adfærd ([44]). Kravene til retsgrundlagets klarhed afhænger i denne forbindelse af den konkrete sag ([45]).

([43]) EMD, *Amann mod Schweiz* [GC], nr. 27798/95, 16. februar 2000, præmis 50. Se også EMD, *Kopp mod Schweiz*, nr. 23224/94, 25. marts 1998, præmis 55 og EMD, *Iordachi m.fl. mod Moldova*, nr. 25198/02, 10. februar 2009, præmis 50.

([44]) EMD, *Amann mod Schweiz* [GC], nr. 27798/95, 16. februar 2000, præmis 56. Se også EMD, *Malone mod Det Forenede Kongerige*, nr. 8691/79, 2. august 1984, præmis 66, EMD, *Silver m.fl. mod Det Forenede Kongerige*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 og 7113/75, 25. marts 1983, præmis 88.

([45]) EMD, *The Sunday Times mod Det Forenede Kongerige*, nr. 6538/74, 26. april 1979, præmis 49. Se også EMD, *Silver m.fl. mod Det Forenede Kongerige*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marts 1983, præmis 88.

Eksempler: I sagen *Rotaru mod Rumænien* ([46]) påstod sagsøgeren, at hans ret til respekt for hans privatliv var blevet overtrådt af den rumænske efterretningstjenestes besiddelse og brug af et dokument med vedkommendes personoplysninger. EMD konkluderede, at selvom national lovgivning tillod indsamling, registrering og arkivering af oplysninger, der havde betydning for den nationale sikkerhed, i hemmelige arkiver, fastslog den ikke betingelser for udøvelsen af disse beføjelser, som var overladt til myndighedernes skøn. Den rumænske lovgivning definerede f.eks. ikke den type information, der kunne behandles, de kategorier af mennesker, der kunne gøres til genstand for overvågningsforanstaltninger, de omstændigheder, hvorunder sådanne foranstaltninger kunne træffes, eller den procedure, der skulle følges. Som følge af disse mangler konkluderede EMD, at den rumænske lovgivning ikke opfyldte kravene om forudsigelighed i artikel 8 i EMRK, og at den pågældende artikel var blevet overtrådt.

I sagen *Taylor-Sabori mod Det Forenede Kongerige* ([47]) havde sagsøgeren været genstand for politiovervågning. Ved hjælp af en »klon« af sagsøgerens personsøger kunne politiet opfange meddelelser, der blev sendt til ham. Sagsøgeren blev derefter arresteret og anklaget for planer om at sælge et stof underlagt kontrol. En del af anklagerens sag mod ham bestod af de samtidige udskrifter af personsøgermeddelelser, som politiet havde transskriberet. På tidspunktet for retssagen mod sagsøgeren var der dog ingen bestemmelser i britisk lovgivning vedrørende opfangelse af kommunikation overført via private telekommunikationssystemer. Indgrebet i hans rettigheder havde derfor ikke været »i overensstemmelse med loven«. EMD konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Vukota-Bojić mod Schweiz ([48])-sagen omhandlede en socialforsikringsansøger, som blev hemmeligt overvåget af privatdetektiver, der var hyret af hendes forsikringsselskab. EMD fastholdt, at selvom den pågældende overvågningsforanstaltning i tvisten var bestilt af et privat forsikringsselskab, havde staten berettiget det selskab til at udrede ydelser på baggrund af lovpligtig sygesikring og til at indsamle forsikringspræmier. En stat kunne

([46]) EMD, *Rotaru mod Rumænien* [GC], nr. 28341/95, 4. maj 2000, præmis 57. Se også EMD, *Association for European Integration and Human Rights og Ekimdzhiev mod Bulgarien*, nr. 62540/00, 28. juni 2007, EMD, *Shimovolos mod Rusland*, nr. 30194/09, 21. juni 2011 og EMD, *Vetter mod Frankrig*, nr. 59842/00, 31. maj 2005.

([47]) EMD, *Taylor-Sabori mod Det Forenede Kongerige*, nr. 47114/99, 22. oktober 2002.

([48]) EMD, *Vukota-Bojić mod Schweiz*, nr. 61838/10, 18. oktober 2016, præmis 77.

ikke fratage sig ansvaret under konventionen ved at tildele sine forpligtelser til private organer eller fysiske personer. Rumænsk lovgivning var nødt til at fastlægge tilstrækkelige sikkerhedsforanstaltninger mod misbrug, for at indgreb i rettighederne under artikel 8 i EMRK var »i overensstemmelse med loven«. I den pågældende sag konkluderede EMD, at EMRK's artikel 8 var overtrådt, da rumænsk lovgivning ikke tilstrækkeligt klart fastlægger, hvorvidt og hvordan forsikringsvirksomheder, der fungerer som offentlige myndigheder i forsikringstvister, kan udøve det skøn, de er tildelt, for at udføre hemmelig overvågning af en forsikret person. Navnlig indeholdte den ikke tilstrækkelige sikkerhedsforanstaltninger mod misbrug.

Forfølgelse af et legitimt mål

Det legitime mål kan være en af de nævnte samfundsinteresser eller beskyttelse af andres rettigheder og friheder. De legitime mål, der kan berettige indgreb, er i medfør af artikel 8, stk. 2, i EMRK national sikkerhed, offentlig tryghed eller landets økonomiske velfærd, forebyggelse af uro eller forbrydelse, beskyttelse af sundheden eller sædeligheden eller beskyttelse af andre personers rettigheder og friheder.

Eksempel: I sagen *Peck mod Det Forenede Kongerige* ([49]) forsøgte sagsøgeren at begå selvmord på åben gade ved at skære i sine håndled uden at vide, at et overvågningskamera havde filmet ham under selvmordsforsøget. Efter at politiet, som så kameraets optagelser, havde reddet ham, udleverede de optagelserne til medierne, som offentliggjorde dem uden at tildække sagsøgerens ansigt. EMD fandt, at der ikke forelå relevant eller tilstrækkelig begrundelse, for at myndighederne videregav optagelserne til offentligheden uden først at have indhentet sagsøgerens samtykke eller tilsløret hans identitet. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Nødvendig i et demokratisk samfund

EMD har fastslået, at begrebet nødvendighed betyder, at indgrebet skal opfylde et presserende samfundsmæssigt behov, og navnlig at det skal stå i forhold til det legitime formål, der forfølges ([50]). Ved vurdering af, om en foranstaltning er nødvendig til at håndtere et presserende samfundsmæssigt behov, undersøger EMD dennes

([49]) EMD, *Peck mod Det Forenede Kongerige*, nr. 44647/98, 28. januar 2003, præmis 85.

([50]) EMD, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987, præmis 58.

relevans og egnethed i forhold til det forfulgte mål. Med henblik herpå kan den overveje, om indgrebet prøver at afhjælpe et problem, som, hvis det ikke afhjælpes, kan have en samfundsskadelig virkning, om der er dokumentation for, at indgrebet kan mindske en sådan skadelig virkning, og hvad samfundets generelle opfattelse af det pågældende problem er ([51]). For eksempel vil sikkerhedstjenesters indsamling og lagring af personoplysninger for bestemte enkeltpersoner, som har forbindelser til terrorbevægelser, være et indgreb i den enkelte persons ret til respekt for privatliv, men som ikke desto mindre opfylder et alvorligt, presserende socialt behov: national sikkerhed og bekæmpelse af terrorisme. For at opfylde nødvendighedskriteriet skal indgrebet også være proportionelt. I EMD's retspraksis er proportionalitet underlagt nødvendighedsbegrebet. Proportionalitet kræver, at et indgreb i rettighederne beskyttet under EMRK ikke må være mere vidtgående, end hvad der er nødvendigt for at opfylde det legitime mål, som forfølges. De vigtige faktorer, der skal tages hensyn til ved udførelse af proportionalitetstesten, er indgrebets rækkevidde, navnlig antallet af berørte personer, og de garantier eller forbehold, som er fastlagt for at begrænse dets rækkevidde eller negative følger for fysiske personers rettigheder ([52]).

Eksempel: I *sagen Khelili mod Schweiz* ([53]) opdagede politiet under en politikontrol, at sagsøgeren bar visitkort med teksten: »Pæn, smuk kvinde, sidst i 30'erne, vil gerne lejlighedsvis møde en mand til drinks og restaurantbesøg. Tlf. […]«. Sagsøgeren påstod, at politiet efter denne opdagelse indtastede hende i deres register som prostitueret, en beskæftigelse, hun nægtede at have. Sagsøgeren krævede, at betegnelsen »prostitueret« blev slettet fra politiets computerregister. EMD anerkendte i princippet, at det under visse omstændigheder kan være forholdsmæssigt at lagre personoplysninger om en person med den begrundelse, at den pågældende person kan begå en anden lovovertrædelse. I sagsøgerens tilfælde var påstanden om ulovlig prostitution angiveligt for vag og generel. Den var ikke underbygget af konkrete beviser, da hun aldrig var blevet dømt for ulovlig prostitution, og registreringen kunne derfor ikke anses for at opfylde et presserende samfundsmæssigt behov som defineret i artikel 8 i EMRK. Domstolen fandt, at det var myndighedernes opgave at bevise rigtigheden af de oplysninger, der

([51]) Artikel 29-Gruppen vedrørende databeskyttelse (Artikel 29-Gruppen) (2014), *Udtalelse om anvendelsen af nødvendigheds- og proportionalitetsbegreberne og databeskyttelse i retshåndhævelsessektoren*, WP 211, Bruxelles, 27. februar 2014, s. 7-8.

([52]) *Ibid.*, s. 9-11.

([53]) EMD, *Khelili mod Schweiz*, nr. 16188/07, 18. oktober 2011.

var lagret om sagsøgeren, og fastslog ud fra alvoren af indgrebet i sagsøgerens rettigheder, at lagringen af ordet »prostitueret« i politiets fortegnelser i årevis ikke havde været nødvendig i et demokratisk samfund. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Eksempel: I sagen *S. og Marper mod Det Forenede Kongerige* ([54]) blev de to sagsøgere arresteret og anklaget for strafferetlige forseelser. Politiet tog deres fingeraftryk og DNA-prøver som fastlagt i lov om politiet og strafferetligt bevismateriale. Sagsøgerne blev aldrig dømt for lovovertrædelserne: Én blev frikendt i retten, og retsforfølgningen af den anden sagsøger blev indstillet. Alligevel beholdt og opbevarede politiet deres fingeraftryk, DNA-profiler og celleprøver i en database, og national lovgivning tillod den ubegrænsede opbevaring heraf. Selvom Det Forenede Kongerige argumenterede, at opbevaringen hjalp med at identificere fremtidige overtrædelser og dermed forfulgte det legitime mål med forebyggelse og opklaring af kriminalitet, fastslog EMD, at indgrebet i sagsøgerens ret til respekt for privatlivet var ubegrundet. Den mindede om, at kerneprincipperne for databeskyttelse kræver, at opbevaringen af personoplysninger er proportionel med indsamlingens formål, og at opbevaringsperioder skal være begrænset. Domstolen accepterede, at udvidelsen af databasen til både at indeholde DNA-profiler for dømte personer og alle fysiske personer, som har været mistænkt men ikke idømt en dom, kan have bidraget til afsløring og forebyggelse af kriminalitet i Det Forenede Kongerige. Den var dog »overrasket over den omfattende og vilkårlige karakter af opbevaringsbeføjelsen« ([55]).

Grundet den store mængde af genetiske og sundhedsmæssige oplysninger i celleprøverne var indgrebet i sagsøgernes ret til privatlivet særligt krænkende. Fingeraftryk og prøver kan tages fra arresterede personer og opbevares på ubestemt tid i politiets database, uanset lovovertrædelsens natur og alvor, og selv for mindre lovovertrædelser, der ikke medfører fængselsstraf. Derudover var mulighederne for, at frikendte fysiske personer kunne få deres data fjernet fra databasen, begrænsede. Endelig bed EMD særligt mærke i det faktum, at én sagsøger var elleve år, da vedkommende blev arresteret. Opbevaring af personoplysninger af en mindreårig, som ikke er idømt en dom, kan være særdeles skadeligt grundet mindreåriges

([54]) EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 4. december 2008.

([55]) *Ibid*., præmis 119.

sårbarhed, og hvor vigtig deres udvikling og integration i samfundet er ([56]). Domstolen fastholdt enstemmigt, at opbevaringen udgjorde et uproportionalt indgreb i retten til privatliv, der ikke kunne anses som værende nødvendig i et demokratisk samfund.

Eksempel: I sagen *Leander mod Sverige* ([57]) fastslog EMD, at sikkerhedsundersøgelsen af personer, der ansøgte om beskæftigelse i stillinger af betydning for den nationale sikkerhed, i sig selv ikke var i strid med kravet om at være nødvendig i et demokratisk samfund. De særlige garantier, der er fastlagt i den nationale ret for at beskytte den registreredes interesser — f.eks. kontrol udøvet af parlamentet og justitsministeren — bevirkede, at EMD konkluderede, at det svenske system til kontrol af medarbejdere opfyldte kravene i artikel 8, stk. 2, i EMRK. På grundlag af de brede muligheder for skøn, som den sagsøgte stat rådede over, havde den ret til at vurdere, at de nationale sikkerhedsinteresser vejede tungere end enkeltpersoners interesser i sagsøgerens tilfælde. Domstolen konkluderede, at EMRK's artikel 8 ikke var blevet overtrådt.

1.2.2. Betingelserne for lovlige begrænsninger i henhold til EU-chartret om grundlæggende rettigheder

Chartrets struktur og ordlyd adskiller sig fra EMRK. Chartret taler ikke om indgreb i garanterede rettigheder, men indeholder en bestemmelse om begrænsning(er) af udøvelsen af de rettigheder og friheder, der anerkendes af Chartret.

I henhold til Chartrets artikel 52, stk. 1, kan der kun indføres begrænsninger for udøvelsen af de rettigheder og friheder, der anerkendes af Chartret, og dermed for udøvelsen af retten til beskyttelse af personoplysninger, såfremt disse:

- er fastlagt i lovgivningen
- respekterer det væsentligste indhold i retten til databeskyttelse

([56]) *Ibid.*, præmis 124.

([57]) EMD, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987, præmis 59 og 67.

- er nødvendige under iagttagelse af proportionalitetsprincippet ([58])

- faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller behovet for beskyttelse af andres rettigheder og friheder.

Da beskyttelse af personoplysninger er en særskilt og selvstændig grundlæggende rettighed i EU's retsorden, som er beskyttet ved Chartrets artikel 8, udgør enhver behandling af personoplysninger i sig selv et indgreb i denne ret. Det er irrelevant, om de pågældende personoplysninger vedrører en fysisk persons privatliv, er følsomme eller om de registrerede på nogen måde har været ulejliget. Indgrebet skal for at være lovligt overholde alle betingelserne angivet i Chartrets artikel 52, stk. 1.

Fastlagt i lovgivningen

Begrænsninger af retten til beskyttelse af personoplysninger skal være fastlagt i lovgivningen. Dette krav betyder, at begrænsninger skal være baseret på et retsgrundlag, som er tilpas tilgængeligt, forudsigeligt og formuleret tilstrækkelig præcist til, at enkelte personer forstår deres forpligtelser og kan regulere deres adfærd. Retsgrundlaget skal også tydeligt definere omfanget og måden kompetente myndigheder udøver deres beføjelse til at beskytte enkelte mennesker mod vilkårlig indgriben. Denne fortolkning ligner kravet om »lovligt indgreb« i EMD's retspraksis ([59]), og man har argumenteret for, at udtrykket »fastlagt i lovgivningen«, som Chartret benytter, skal have samme betydning som i EMRK ([60]). Ved fortolkning af omfanget af Chartrets artikel 52, stk. 1, er det relevant for EU-Domstolen at tage hensyn til EMD's retspraksis og navnlig konceptet »lovgivningens kvalitet«, som denne har udviklet igennem årene ([61]).

([58]) Med hensyn til vurdering af nødvendigheden af foranstaltninger, der begrænser den grundlæggende ret til beskyttelse af personoplysninger, se: EDPS (2017), *Necessity Toolkit*, Bruxelles, 11. april 2017.

([59]) EDPS (2017), *Necessity Toolkit*, Bruxelles, 11. april 2017, s. 4. Se også EU-Domstolen, *Udtalelse 1/15: Domstolens udtalelse (Store Afdeling)*, 26. juli 2017.

([60]) EU-Domstolen, forenede sager C-203/15 og C-698/15, *Tele2 Sverige AB mod Post- och telestyrelsen* og *Secretary of State for the Home Department mod Tom Watson m.fl.*, *Forslag til afgørelse fra generaladvokat H. Saugmandsgaard Øe*, fremsat den 19. juli 2016, præmis 140.

([61]) EU-Domstolen, C-70/10, *Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, *Forslag til afgørelse fra generaladvokat Cruz Villalón,* fremsat den 14. april 2011, præmis 100.

Respekt for rettighedens væsentligste indhold

Under EU's retsorden skal enhver begrænsning af de grundlæggende rettigheder, der er beskyttet i Chartret, respektere disse rettigheders væsentligste indhold. Dette betyder, at begrænsninger, der er så omfattende og indgående, at en grundlæggende rettigheds essentielle indhold tilsidesættes, ikke kan begrundes. Hvis rettighedens væsentligste indhold tilsidesættes, skal begrænsningen anses som værende ulovlig, uden at det er nødvendigt at vurdere, om det har et formål af almen interesse og opfylder nødvendigheds- og proportionalitetskriterierne.

Eksempel: *Schrems*-sagen ([62]) omhandlede beskyttelse af enkeltpersoner i forbindelse med overførsel af deres personoplysninger til tredjelande — i dette tilfælde De Forenede Stater. Schrems er en østrigsk statsborger, som har brugt Facebook i mange år, og han indgav en klage til den irske tilsynsmyndighed for databeskyttelse for at undsige sig overførslen af hans personoplysninger fra Facebooks irske datterselskab til Facebook Inc. og serverne placeret i USA, hvor dataene blev behandlet. I lyset af de afsløringer, der kom fra Edward Snowden, en amerikansk whistleblower, i 2013 omkring amerikanske overvågningstjenesters overvågningsaktiviteter argumenterede han for, at USA's love og praksisser ikke beskyttede personoplysninger overført til USA's område i tilstrækkelig grad. Snowden havde afsløret, at National Security Agency havde direkte adgang til servere hos virksomheder som Facebook og kunne læse indholdet af samtaler og private beskeder.

Dataoverførsler til USA var baseret på Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet, som blev vedtaget i 2000, hvilket tillod overførsler til amerikanske virksomheder, der har selvcertificeret, at de ville beskytte personoplysninger overført fra EU samt overholde de såkaldte »safe harbour-principper«. Da sagen blev indbragt for EU-Domstolen, undersøgte den gyldigheden af Kommissionens beslutning på baggrund af Chartret. Den mindede om, at beskyttelse af grundlæggende rettigheder i EU kræver, at undtagelser for og begrænsninger af de rettigheder kun omfatter det strengt nødvendige. EU-Domstolen anså lovgivning, der gør det muligt for de offentlige myndigheder på generel vis at få adgang til indholdet af elektronisk kommunikation, for at »udgøre et indgreb i det væsentligste indhold af den grundlæggende ret til respekt for privatlivet, således som denne er

([62]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015.

sikret ved Chartrets artikel 7«. Rettigheden ville ikke have nogen rækkevidde, hvis amerikanske myndigheder havde tilladelse til at tilgå kommunikationer på et vilkårligt grundlag uden en objektiv begrundelse baseret på konkrete hensyn til national sikkerhed eller forebyggelse af kriminalitet, som specifikt er knyttet til de berørte personer, og uden at der stilles passende og verificerbare garantier mod magtmisbrug for denne overvågningspraksis.

Derudover bemærkede EU-Domstolen, at »en lovgivning, der ikke fastsætter nogen mulighed for retssubjektet til at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet« ikke opfylder den grundlæggende ret til en effektiv domstolsbeskyttelse (Chartrets artikel 47). Som følge heraf formåede safe harbour-beslutningen ikke at sikre et beskyttelsesniveau for grundlæggende rettigheder i USA, som i det væsentlige svarer til det niveau, der er sikret i EU under direktivet sammenholdt med Chartret. EU-Domstolen erklærede følgeligt beslutningen for ugyldig ([63]).

Eksempel: I *Digital Rights Ireland*-sagen ([64]) undersøgte EU-Domstolen foreneligheden af direktiv 2006/24/EF (datalagringsdirektivet) med Chartrets artikel 7 og 8. Direktivet forpligtede udbydere af elektroniske kommunikationstjenester til at opbevare trafik- og lokaliseringsdata i mindst seks måneder og op til 24 måneder samt tillade, at nationale myndigheder får adgang til disse data i forbindelse med forebyggelse, efterforskning, afsløring og retsforfølgelse af grov kriminalitet. Direktivet tillod ikke opbevaring af de elektroniske kommunikationers indhold. EU-Domstolen bemærkede, at de data, som udbyderne var tvunget til at opbevare under direktivet, omfattede data, der er nødvendige for at spore og identificere kilden og destinationen for en kommunikation; datoen, tidspunktet og varigheden af en kommunikation; det opkaldende nummer, kaldte numre og IP-adresser. Disse data »vil tilsammen kunne gøre det muligt at drage meget præcise

([63]) EU-Domstolens beslutning om at erklære Kommissionens beslutning 520/2000/EF for ugyldig var også baseret på andre begrundelser, der vil blive gennemgået i andre afsnit i denne håndbog. Navnlig betragtede EU-Domstolen beslutningen for at begrænse nationale databeskyttelsesmyndigheders beføjelser på ulovlig vis. Derudover var der ikke nogen tilgængelige retsmidler for enkeltpersoner under safe harbour-ordningen, hvis de ønskede at få adgang til de personoplysninger, som omhandlede dem, og/eller få sådanne oplysninger berigtiget eller slettet. Det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som denne er sikret ved Chartrets artikel 47, var derfor heller ikke overholdt.

([64]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014.

slutninger vedrørende privatlivet for de personer, hvis data er blevet lagret, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer«.

Opbevaringen af personoplysninger i henhold til direktivet udgjorde derfor et særlig alvorligt indgreb i rettighederne til privatliv og beskyttelse af personoplysninger. EU-Domstolen fastholdt dog, at indgrebet ikke krænkede det væsentligste indhold af disse rettigheder. Det væsentligste indhold af retten til privatliv var ikke krænket, da direktivet ikke giver adgang til at gøre sig bekendt med selve indholdet af de elektroniske kommunikationer. På tilsvarende vis var det væsentligste indhold af retten til beskyttelse af personoplysninger ikke krænket, da direktivet krævede, at udbydere af elektroniske kommunikationstjenester skulle respektere visse principper for databeskyttelse og datasikkerhed samt gennemføre fornødne tekniske og organisatoriske foranstaltninger med henblik herpå.

Nødvendighed og proportionalitet

Artikel 52, stk. 1, i Chartret fastlægger, at begrænsninger af udøvelsen af de grundlæggende rettigheder og friheder, der anerkendes af Chartret, kun må indføres, hvis de er nødvendige.

En begrænsning kan være **nødvendig**, hvis der er et behov for at tilpasse foranstaltninger til de forfulgte mål af almen interesse — men nødvendighed, som fortolket af EU-Domstolen, betyder også, at vedtagne foranstaltninger skal være mindre krænkende sammenlignet med andre alternativer til at opnå samme mål. I forbindelse med rettighederne til respekt for privatlivet og beskyttelse af personoplysninger gør EU-Domstolen brug af et stringent nødvendighedskriterie, og den fastholder, at undtagelser og begrænsninger kun gælder, hvis det holdes inden for det strengt nødvendige. Hvis en begrænsning anses for at være strengt nødvendig, er der også et behov for at vurdere, om den er proportionel.

Proportionalitet betyder, at fordelene ved begrænsningen bør opveje ulemperne, som begrænsningen har på udøvelsen af de pågældende grundlæggende rettigheder ([65]). Det er vigtigt, at begrænsninger indeholder passende garantier for

([65]) EDPS (2017), *Necessity Toolkit*, s. 5.

at reducere ulemper og risici for, at rettighederne til privatliv og databeskyttelse tilsidesættes.

Eksempel: I sagen *Volker und Markus Schecke* ([66]) fastslog EU-Domstolen, at Rådet og Kommissionen med kravet om offentliggørelse af personoplysninger om enhver modtager af støtte fra visse landbrugsfonde uden at foretage en sondring i henhold til relevante kriterier, såsom i hvilken periode disse personer har modtaget disse midler, hyppigheden af en sådan modtagelse eller midlernes art og omfang, havde overskredet de grænser, som en overholdelse af proportionalitetsprincippet opstiller.

EU-Domstolen fandt det derfor nødvendigt at erklære visse bestemmelser i Rådets forordning (EF) nr. 1290/2005 og hele forordning nr. 259/2008 for ugyldige ([67]).

Eksempel: I *Digital Rights Ireland*-sagen ([68]) fastholdt EU-Domstolen, at indgrebet i retten til privatliv som følge af datalagringsdirektivet ikke krænkede det væsentligste indhold af retten, da den forbød opbevaring af indholdet af elektroniske kommunikationer. Den konkluderede dog, at direktivet ikke var kompatibelt med Chartrets artikel 7 og 8 og erklærede det for ugyldigt. Da trafik- og lokaliseringsdata tilsammen kunne analyseres og gøre det muligt at drage meget præcise slutninger vedrørende fysiske personers privatliv, udgjorde det et alvorligt indgreb i disse rettigheder. EU-Domstolen overvejede, at direktivet krævede lagring af alle metadata vedrørende fastnettelefoni, mobiltelefoni, internetadgang, e-mail og telefoni via internettet, hvilket omfatter alle former for elektronisk kommunikation — og brugen heraf er meget udbredt i folks dagligdag. Praktisk set var det et indgreb, som påvirkede hele Europas befolkning. I betragtning af omfanget og alvoren af dette indgreb kunne lagring af trafik- og lokaliseringsdata i henhold til

([66]) EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 9. november 2010, præmis 89 og 86.

([67]) Rådets forordning (EF) nr. 1290/2005 af 21. juni 2005 om finansiering af den fælles landbrugspolitik, EUT L 209 af 11. august 2005; Kommissionens forordning (EF) nr. 259/2008 af 18. marts 2008 om gennemførelsesbestemmelser til Rådets forordning (EF) nr. 1290/2005 for så vidt angår offentliggørelsen af oplysninger om modtagerne af midler fra Den Europæiske Garantifond for Landbruget (EGFL) og Den Europæiske Landbrugsfond for Udvikling af Landdistrikterne (ELFUL), EUT L 76 af 19. marts 2008.

([68]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl. og Kärntner Landesregierung m.fl.* [GC], 8. april 2014, præmis 39.

EU-Domstolen kun begrundes med henblik på bekæmpelse af grov kriminalitet. Derudover fastlagde direktivet ikke nogle objektive kriterier, som ville sikre, at kompetente nationale myndigheders adgang til de opbevarede data begrænses til det strengt nødvendige. Desuden indeholdt det ikke nogen materielle og processuelle betingelser for nationale myndigheders adgang og brug af de lagrede data, som ikke var undergivet en forudgående kontrol ved en retsinstans eller en anden uafhængig enhed.

EU-Domstolen drog en lignende konklusion i de forenede sager *Tele2 Sverige AB mod Post- och telestyrelsen* og *Secretary of State for the Home Department mod Tom Watson m.fl.* ([69]). Disse omhandlede lagring af trafik- og lokaliseringsdata for »alle abonnenter og registrerede brugere generelt, og som er rettet mod alle elektroniske kommunikationsmidler og samtlige trafikdata« med »ingen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål« ([70]). Selvom en person var knyttet direkte eller indirekte til grove straffelovsovertrædelser, eller en persons kommunikationer var relevante for den nationale sikkerhed, var det i den pågældende sag ikke en betingelse for, at vedkommendes data skulle lagres. Grundet fraværet af enten en krævet sammenhæng mellem de lagrede data og en trussel mod den offentlige sikkerhed eller begrænsninger i forbindelse med tidsrum og/eller et geografisk område konkluderede EU-Domstolen, at den nationale lovgivning overskrider det strengt nødvendige med henblik på bekæmpelse af grov kriminalitet ([71]).

Den Europæiske Tilsynsførende for Databeskyttelse har en lignende tilgang til nødvendighed i dennes *Necessity Toolkit* ([72]). Toolkittet er rettet mod at hjælpe med at vurdere foreslåede foranstaltningers overholdelse af EU's databeskyttelseslovgivning. Det blev udviklet for at udstyre EU's beslutningstagere og lovgivere, der er ansvarlige for at udarbejde og undersøge foranstaltninger, som involverer behandling af personoplysninger og begrænser retten til beskyttelse af personoplysninger og andre rettigheder og friheder fastlagt i Chartret, med bedre værktøjer.

([69]) EU-Domstolen, forenede sager C-203/15 og C-698/15, *Tele2 Sverige AB mod Post- och telestyrelsen og Secretary of State for the Home Department mod Tom Watson m.fl.*, [GC], 21. december 2016, præmis 105-106.

([70]) *Ibid.*, præmis 105.

([71]) *Ibid.*, præmis 107.

([72]) EDPS (2017), *Necessity Toolkit*, Bruxelles, 11. april 2017.

Mål af almen interesse

En begrænsning af udøvelsen af de rettigheder, som er anerkendt i Charteret, skal, for at være begrundet, også faktisk opfylde mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder. I forbindelse med behovet for beskyttelse af andres rettigheder og friheder er der ofte et indbyrdes forhold mellem retten til beskyttelse af personoplysninger og andre grundlæggende rettigheder. Afsnit 1.3. giver en detaljeret analyse over sådanne indbyrdes forhold. Mål af almen interesse omfatter EU's generelle mål, som er fastlagt i artikel 3 i traktaten om Den Europæiske Union (TEU), såsom at fremme fred og sine befolkningers velfærd, social retfærdighed, oprettelse af et område med frihed, sikkerhed og retfærdighed, hvor der er fri bevægelighed for personer, sammen med passende foranstaltninger til at forebygge og bekæmpe kriminalitet samt andre mål og interesser, som er beskyttet af traktaternes enkelte bestemmelser ([73]). Den generelle forordning om databeskyttelse uddyber i denne sammenhæng Chartrets artikel 52, stk. 1: Forordningens artikel 23, stk. 1, angiver en liste over mål af almen interesse, der anses som værende legitime til at begrænse fysiske personers rettigheder, såfremt begrænsningen respekterer det væsentligste indhold i retten til beskyttelse af personoplysninger samt er nødvendig og proportionel. Statens sikkerhed og forsvaret, forebyggelse af kriminalitet, beskyttelsen af EU's eller medlemsstaters væsentlige økonomiske eller finansielle interesser, folkesundhed og social sikkerhed er blandt de mål af generel samfundsinteresse, som er nævnt deri.

Det er vigtigt at definere og forklare målet af almen interesse, som begrænsningen forfølger, i tilstrækkelige detaljer, da begrænsningens nødvendighed vurderes ud fra den baggrund. Det er nødvendigt med en tydelig, detaljeret beskrivelse af målet med begrænsningen og de foreslåede foranstaltninger, så det er muligt at vurdere, om den er nødvendig eller ej ([74]). Det forfulgte mål og begrænsningens nødvendighed og proportionalitet er tæt forbundet.

Eksempel: Sagen *Michael Schwarz mod Stadt Bochum* ([75]) vedrørte begrænsninger af retten til respekt for privatliv og retten til beskyttelse af personoplysninger som følge af optagelse og lagring af fingeraftryk, når myndigheder

([73]) Forklaringer til Chartret om grundlæggende rettigheder (2007/C 303/02), EUT C 303, 14. december 2007, s. 17-35.

([74]) EDPS (2017), *Necessity Toolkit*, Bruxelles, 11. april 2017, s. 4.

([75]) EU-Domstolen, C-291/12, *Michael Schwarz mod Stadt Bochum*, 17. oktober 2013.

i medlemsstater udsteder pas ([76]). Sagsøgeren anmodede Stadt Bochum om et pas, men afviste at hans fingeraftryk skulle optages. Som følge heraf afviste Stadt Bochum hans pasansøgning. Han anlagde derefter sag ved en tysk domstol for at få udstedt et pas uden at hans fingeraftryk skulle optages. Den tyske domstol henviste sagen til EU-Domstolen og spurgte, om artikel 1, stk. 2, i forordning (EF) nr. 2252/2004 om standarder for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder, er gyldig.

EU-Domstolen påpegede, at fingeraftryk **er personoplysninger**, da de objektivt set indeholder unikke oplysninger om fysiske personer og gør det muligt præcist at identificere dem, og optagelse og opbevaring af fingeraftryk udgør behandling. Sidstnævnte behandling, som er underlagt artikel 1, stk. 2, i forordning (EF) nr. 2252/2004, er et indgreb i retten til respekt for privatliv og beskyttelse af personoplysninger ([77]). Chartrets artikel 52, stk. 1, tillader dog, at der kan indføres begrænsninger i udøvelsen af disse rettigheder, for så vidt som disse begrænsninger er fastlagt i lovgivningen, respekterer disse rettigheders væsentligste indhold, og at de under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Den Europæiske Union, eller behovet for beskyttelse af andres rettigheder og friheder.

I den nærværende sag bemærkede EU-Domstolen for det første, at begrænsningen, som følger af optagelse og lagring af fingeraftryk ved udstedelse af pas, skal anses som værende **fastlagt i lovgivningen**, da disse aktiviteter er fastlagt i artikel 1, stk. 2, i forordning (EF) nr. 2252/2004. For det andet var sidstnævnte forordning beregnet til at forhindre forfalskning af pas og svigagtig brug heraf. Artikel 1, stk. 2, er derfor fastlagt for bl.a. at forhindre ulovlig indrejse af personer på Unionens område og forfølger derfor et mål af almen interesse, der er anerkendt af Unionen. For det tredje fremgår det ikke af de oplysninger, som EU-Domstolen havde til rådighed, og det er i øvrigt heller ikke blevet påstået, at de begrænsninger, der i det foreliggende tilfælde er fastsat for udøvelsen af rettighederne, ikke respekterer disse rettigheders væsentligste indhold. For det fjerde kræver lagringen af fingeraftryk på et lagringsmedium, der har et højt sikkerhedsniveau, som fastsat ved denne bestemmelse, et højt teknisk udviklingsniveau. Det er sandsynligt, at en sådan lagring nedsætter risikoen for forfalskning af pas

([76]) *Ibid.*, præmis 33-36.

([77]) *Ibid.*, præmis 27-30.

og letter opgaven for de myndigheder, der ved EU's grænser skal efterprøve passenes ægthed. Det faktum, at den nævnte metode ikke er fuldstændig pålidelig, er ikke afgørende. Selv om metoden ikke fuldstændig udelukker accepter af personer, der ikke må indrejse, er det tilstrækkeligt, at den nedsætter risikoen for sådanne accepter betydeligt. På baggrund af det forrige fastslog EU-Domstolen, at optagelse og lagring af fingeraftryk som omhandlet i artikel 1, stk. 2, i forordning (EF) nr. 2252/2004 var egnet til at nå de mål, der forfølges med denne forordning, og følgelig formålet om at forhindre ulovlig indrejse af personer på Unionens område ([78]).

Derefter vurderede EU-Domstolen, om en sådan behandling er **nødvendig**, hvor den bemærkede, at den pågældende aktivitet alene bestod i, at der blev taget et aftryk af to fingre. Disse fingre kan også normalt ses af andre, således at der ikke er tale om en operation af intim karakter. Ligesom når der tages et ansigtsbillede, er der heller ikke tale om, at den pågældende udsættes for noget særligt fysisk eller psykisk ubehag. Det bør også bemærkes, at det eneste reelle alternativ til optagelse af fingeraftryk, der er blevet henvist til under sagen for EU-Domstolen, består i iris-scanning. Intet i de sagsakter, der er fremlagt for EU-Domstolen, pegede i retning af, at sidstnævnte procedure er mindre indgribende i de rettigheder, der er anerkendt ved Chartrets artikel 7 og 8, end optagelsen af fingeraftryk. Hvad angår effektiviteten af disse to metoder er det desuden ubestridt, at det teknologiske modenhedsniveau for metoden for iris-genkendelse ikke har nået det samme niveau som for metoden for fingeraftryk, som for nærværende er betydeligt dyrere end proceduren for sammenligning af fingeraftryk, og iris-genkendelse er derfor mindre egnet til generel anvendelse. Det er dermed ikke blevet bragt til EU-Domstolens kendskab, at der findes foranstaltninger, der på tilstrækkelig effektiv måde kunne bidrage til målet om at beskytte pas mod svigagtig brug, samtidig med at de gør mindre indgreb i de rettigheder, der er anerkendt ved Chartrets artikel 7 og 8, end de foranstaltninger, som metoden på grundlag af fingeraftryk indebærer ([79]).

EU-Domstolen bemærkede, at artikel 4, stk. 3, i forordning (EF) nr. 2252/2004 udtrykkeligt præciserer, at fingeraftryk kun må anvendes med det ene formål at kontrollere ægtheden af passet og indehaverens identitet, og forordningens artikel 1, stk. 2, fastlægger, at fingeraftryk skal lagres i selve passet, som alene tilhører indehaveren. Forordningen gav dermed ikke hjemmel for

([78]) *Ibid.*, præmis 35-45.

([79]) EU-Domstolen, C-291/12, *Michael Schwarz mod Stadt Bochum*, 17. oktober 2013, præmis 46-53.

en centralisering af oplysninger, der er indsamlet på grundlag heraf, eller for en anvendelse af disse oplysninger til andre formål end at forhindre ulovlig indrejse af personer på Unionens område ([80]). Henset til alt det ovenfor anførte konkluderede EU-Domstolen, at gennemgangen af det forelagte spørgsmål intet har frembragt, der kan rejse tvivl om gyldigheden af artikel 1, stk. 2, i forordning (EF) nr. 2252/2004.

Forholdet mellem Chartret og EMRK

Selvom ordlyden er forskellig, minder betingelserne for lovlige begrænsninger af rettighederne i Chartrets artikel 52, stk. 1, om artikel 8, stk. 2, i EMRK vedrørende retten til respekt for privatliv. EU-Domstolen og EMD henviser ofte i deres retspraksis til hinandens domme, hvilket er en del af de to domstoles konstante dialog for at opnå en ensartet fortolkning af databeskyttelsesreglerne. Det fremgår af Chartrets artikel 52, stk. 3, at i »det omfang dette Charter indeholder rettigheder svarende til dem, der er sikret ved den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, har de samme betydning og omfang som i konventionen«. Chartrets artikel 8 svarer dog ikke direkte til en artikel i EMRK ([81]). Chartrets artikel 52, stk. 3, omhandler mere indholdet og omfanget af de rettigheder, som er beskyttet af hver retsorden, end betingelserne for deres begrænsning. Ud fra den bredere kontekst for dialogen og samarbejdet mellem de to domstole, kan EU-Domstolen i dennes analyser dog tage hensyn til kriterierne for lovlig begrænsning i artikel 8 i EMRK, som de fortolkes af EMD. Det modsatte scenarie, hvor EMD kan henvise til betingelserne for lovlig begrænsning under Chartret, er også muligt. Under alle omstændigheder bør der også tages hensyn til, at der ikke er noget fuldkomment modstykke til Chartrets artikel 8 i EMRK, som omhandler beskyttelse af personoplysninger, og navnlig den registreredes rettigheder, legitime behandlingsgrunde og tilsyn ved en uafhængig myndighed. Nogle dele af Chartrets artikel 8 kan findes i EMD's retspraksis, som er udviklet under EMD's artikel 8 og omhandler konvention 108 ([82]). Denne forbindelse sikrer, at der er en gensidig inspiration mellem EU-Domstolen og EMRK ved spørgsmål om databeskyttelse.

([80]) *Ibid.*, præmis 56-61.

([81]) EDPS (2017), *Necessity Toolkit*, Bruxelles, 11. april 2017, s. 6.

([82]) Forklaringer til Chartret om grundlæggende rettigheder (2007/C 303/02), artikel 8.

1.3. Påvirkning af andre rettigheder og legitime interesser

Hovedpunkter

- Retten til databeskyttelse påvirker ofte andre rettigheder, såsom ytringsfrihed og retten til at modtage og give oplysninger.
- Denne påvirkning er ofte ambivalent: Selvom der er situationer, hvor retten til beskyttelse af personoplysninger er i konflikt med en bestemt rettighed, er der også situationer, hvor retten til beskyttelse af personoplysninger effektivt sikrer respekt for selvsamme rettighed. Dette er for eksempel tilfældet for ytringsfrihed, da tavshedspligt er en del af retten til respekt for privatliv.
- Behovet for at beskytte andres rettigheder og friheder er ét af de kriterier, der benyttes til at vurdere den lovlige begrænsning af retten til beskyttelse af personoplysninger.
- Når forskellige rettigheder står på spil, skal domstolene afveje en måde at forlige dem på.
- Den generelle forordning om databeskyttelse kræver, at medlemsstater forliger retten til beskyttelse af personoplysninger med ytrings- og informationsfrihed.
- Medlemsstater kan også vedtage specifikke regler i national lovgivning for at forlige retten til beskyttelse af personoplysninger med offentlig adgang til officielle dokumenter og tavshedspligter.

Retten til beskyttelse af personoplysninger er ikke en absolut rettighed. Betingelserne for den lovlige begrænsning af denne ret er beskrevet i ovenstående. Ét af kriterierne for lovlige begrænsninger af rettigheder, som er anerkendt i både Europarådets og EU's lovgivning, er, at det er nødvendigt med indgreb i databeskyttelse for at beskytte andres rettigheder og friheder. Når databeskyttelse påvirker andre rettigheder, har både EMD og EU-Domstolen gentagne gange udtalt, at det er nødvendigt at foretage en afvejning af de andre rettigheder ved anvendelse og fortolkning af EMRK's artikel 8 og Chartrets artikel 8 ([83]). Flere vigtige eksempler vil vise, hvordan denne balance opnås.

([83]) EMD, *Von Hannover mod Tyskland (nr. 2)* [GC], nr. 40660/08 og 60641/08, 7. februar 2012; EU-Domstolen, forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado*, 24. november 2011, præmis 48; EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU* [GC], 29. januar 2008, præmis 68.

Udover afvejningen udført af disse domstole kan stater, om nødvendigt, vedtage lovgivning til at forene retten til beskyttelse af personoplysninger med andre rettigheder. Den generelle forordning om databeskyttelse fastlægger af denne årsag nationale undtagelser på forskellige områder.

I forbindelse med ytringsfrihed kræver GDPR, at medlemsstater i deres lovgivning forener »retten til beskyttelse af personoplysninger i henhold til denne forordning med retten til ytrings- og informationsfrihed, herunder behandling i journalistisk øjemed og med henblik på akademisk, kunstnerisk eller litterær virksomhed« ([84]). Medlemsstater kan også vedtage love for at forene databeskyttelse med offentlig adgang til officielle dokumenter og tavshedspligter, der er beskyttet som en form af retten til respekt for privatliv ([85]).

1.3.1. Ytringsfrihed

Én af de rettigheder, der i væsentligste grad påvirker retten til databeskyttelse, er retten til ytringsfrihed.

Ytringsfrihed er beskyttet af Chartrets artikel 11 (»Ytrings- og informationsfrihed«). Denne ret omfatter »meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker uden indblanding fra offentlig myndighed og uden hensyn til landegrænser«. Informationsfrihed beskytter i medfør af Chartrets artikel 11 og EMRK's artikel 10 både retten til at meddele og *modtage* oplysninger.

Begrænsninger af ytringsfriheden skal overholde kriterierne anført i Chartrets artikel 52, stk. 1, som beskrevet tidligere. Desuden svarer artikel 11 til artikel 10 i EMRK. Det fremgår af Chartrets artikel 52, stk. 3, at i det omfang Chartret indeholder rettigheder svarende til dem, der er sikret ved EMRK, »har de samme betydning og omfang som i konventionen«. De begrænsninger, som lovligt kan pålægges rettigheden garanteret af Chartrets artikel 11, må derfor ikke overstige dem, der er fastsat i artikel 10, stk. 2, i EMRK — med andre ord skal de være fastlagt i lovgivningen og være nødvendige i et demokratisk samfund »for at beskytte andres [...] rygte eller rettigheder«. Sådanne rettigheder omfatter navnlig retten til respekt for privatliv og retten til beskyttelse af personoplysninger.

([84]) Den generelle forordning om databeskyttelse, artikel 85.

([85]) *Ibid.*, artikel 86 og 90.

Forholdet mellem beskyttelsen af personoplysninger og ytringsfrihed er underlagt artikel 85 i den generelle forordning om databeskyttelse med titlen »Behandling og ytrings- og informationsfriheden«. I medfør af denne artikel skal medlemsstater forene retten til beskyttelse af personoplysninger med retten til ytrings- og informationsfrihed. Navnlig skal der fastsættes fritagelser og undtagelser fra specifikke kapitler i den generelle forordning om databeskyttelse i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, for så vidt som de er nødvendige for at forene retten til beskyttelse af personoplysninger med ytrings- og informationsfrihed.

Eksempel: I sagen *Tietosuojavaltuutettu mod Satakunnan Markkinapörssi Oy og Satamedia Oy* ([86]) blev EU-Domstolen anmodet om at definere forholdet mellem databeskyttelse og pressefrihed ([87]). Den skulle undersøge en virksomheds offentliggørelse af skatteoplysninger igennem en SMS-tjeneste om omkring 1,2 millioner fysiske personer, som lovligt var indhentet fra de finske myndigheder. Den finske tilsynsmyndighed for databeskyttelse havde udstedt en afgørelse, der krævede, at virksomheden standsede deres offentliggørelse af disse oplysninger. Virksomheden anfægtede denne afgørelse i en national domstol, der anmodede EU-Domstolen om at afklare fortolkningen af databeskyttelsesdirektivet. EU-Domstolen skulle navnlig afgøre, om behandlingen af personoplysninger, som skattemyndighederne havde offentliggjort for at give mobiltelefonbrugere mulighed for at modtage skatteoplysninger om andre fysiske personer, skal anses for en aktivitet, som udelukkende finder sted i journalistisk øjemed. Efter at have afgjort, at virksomhedens aktiviteter var »behandling af personoplysninger« som defineret i databeskyttelsesdirektivets artikel 3, stk. 1, analyserede EU-Domstolen direktivets artikel 9 (om behandling af personoplysninger og ytringsfrihed). Den bemærkede først den betydning, ytringsfriheden har i ethvert demokratisk samfund, og fastslog, at de begreber, som er knyttet hertil, herunder begrebet journalistik, skal fortolkes bredt. Den konstaterede derefter, at undtagelser fra og begrænsninger af retten til databeskyttelse

([86]) EU-Domstolen, C-73/07, *Tietosuojavaltuutettu mod Satakunnan Markkinapörssi Oy og Satamedia Oy* [GC], 16. december 2008, præmis 56, 61 og 62.

([87]) Sagen omhandlede fortolkningen af databeskyttelsesdirektivets artikel 9 – nu erstattet af artikel 85 i den generelle forordning om databeskyttelse – som havde ordlyden: »Medlemsstaterne fastsætter i forbindelse med behandling af personoplysninger, der udelukkende finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, kun fritagelser eller undtagelser fra bestemmelserne i dette kapitel og i kapitel IV og VI, for så vidt som de er nødvendige for at forene retten til privatlivets fred med reglerne for ytringsfrihed«.

skal holdes inden for det strengt nødvendige for at opnå en afbalanceret afvejning af de to grundlæggende rettigheder. I den pågældende sag fandt EU-Domstolen, at aktiviteter som dem, de pågældende virksomheder udførte på oplysninger fra dokumenter, som er offentlige i henhold til national lovgivning, kan kvalificeres som behandling »i journalistisk øjemed«, hvis de har til formål at udbrede oplysninger, synspunkter eller ideer til offentligheden, uanset hvilket middel der anvendes til videregivelsen. Domstolen afgjorde også, at disse aktiviteter ikke er forbeholdt medieselskaber og kan være forbundet med et ønske om at opnå en økonomisk gevinst. EU-Domstolen overlod det dog til den nationale domstol at afgøre, om dette var tilfældet i den pågældende sag.

Den samme sag blev også undersøgt af EMD, efter den nationale domstol på baggrund af EU-domstolens vejledning besluttede, at tilsynsmyndighedens krav om at standse offentliggørelsen af alle skatteoplysninger var et begrundet indgreb i virksomhedens ytringsfrihed. EMD gav medhold til denne beslutning ([88]). Den konkluderede, at indgrebet var i overensstemmelse med loven, forfulgte et legitimt mål og var nødvendig i et demokratisk samfund, selvom der var et indgreb i virksomhedernes ret til at meddele oplysninger.

Domstolen mindede om de kriterier i retspraksis, som skal vejlede nationale myndigheder og selve EMD, når de afvejer ytringsfrihed mod retten til respekt for privatliv. Når der er tale om en politisk udtale eller debat omkring et emne af almen interesse, er der ringe mulighed for at begrænse retten til at modtage og meddele oplysninger, da offentligheden har ret til at være oplyst, og dette er en væsentlig ret i et demokratisk samfund ([89]). Presseartikler, der udelukkende er rettet mod at tilfredsstille en bestemt læserskares nysgerrighed for detaljer om en persons privatliv, kan dog ikke anses for at bidrage til en debat af almen interesse. Afvigelsen fra databeskyttelsesregler i journalistisk øjemed er beregnet til at tillade, at journalister kan få adgang til, indsamle og behandle oplysninger, som gør dem i stand til at udføre deres journalistiske arbejde. Der var derfor bestemt en almen interesse i at give adgang til og tillade, at de sagsøgende virksomheder indsamlede og behandlede de pågældende store mængder af beskatningsdata. I modsætning hertil konkluderede Domstolen, at der ikke var nogen almen interesse i avisernes samlede offentliggørelse af disse rådata, uden at disse var i en

([88]) EMD, *Satakunnan Markkinapörssi Oy og Satamedia Oy mod Finland*, nr. 931/13, 27. juni 2017.

([89]) *Ibid.*, præmis 169.

redigeret form eller ledsaget af analyser. Beskatningsoplysningerne kan have gjort det muligt for nysgerrige medlemmer af offentligheden at klassificere enkeltpersoner ud fra deres økonomiske status og ville tilfredsstille offentlighedens tørst efter oplysninger om andres privatliv. Dette kan ikke betragtes som at bidrage til en debat af almen interesse.

Eksempel: I sagen *Google Spain* ([90]) vurderede EU-Domstolen, om Google var forpligtet til at slette forældede oplysninger om sagsøgerens finansielle vanskeligheder fra sin liste over søgeresultater. Ved udførelse af en søgning i Googles søgemaskine med sagsøgerens navn resulterede søgningen i links til gamle avisartikler, der nævnte vedkommendes forbindelse til konkursbehandlinger. Sagsøgeren betragtede dette som en overtrædelse af vedkommendes ret til respekt for privatliv og til beskyttelse af personoplysninger, da konkursbehandlingerne var afsluttet mange år tidligere, hvilket gjorde sådanne henvisninger irrelevante.

EU-Domstolen præciserede først, at søgemaskiner på internettet og søgeresultater, der indeholder personoplysninger, kan tegne en detaljeret profil af en fysisk person. Grundet den stigende digitalisering af samfundet er kravet om, at personoplysninger skal være nøjagtige, og at deres offentliggørelse skal begrænses til det nødvendige, dvs. oplyse offentligheden, grundlæggende for at sikre, at enkeltpersoner får et højt databeskyttelsesniveau. »Søgemaskineudbyderen skal i sin egenskab af registeransvarlig inden for rammerne af sit ansvar, sine kompetencer og sine muligheder således sikre, at behandlingen opfylder kravene« i EU-retten for at sikre fastlagte retsgarantiers fulde virkning. Dette betyder, at retten til at få sine personoplysninger slettet, når behandling heraf ikke længere er nødvendig eller forældet, også omfatter søgemaskiner, der er defineret som dataansvarlige og ikke bare behandlere (se afsnit 2.3.1.).

I forbindelse med undersøgelsen af, om Google skulle fjerne links vedrørende sagsøgeren, fastholdt EU-Domstolen, at fysiske personer under visse omstændigheder har ret til at få slettet deres personoplysninger fra søgeresultaterne fra en søgemaskine på internettet. Man kan påberåbe sig denne ret, når oplysninger om en fysisk person er ukorrekte, utilstrækkelige, irrelevante eller omfatter mere end, hvad der er nødvendigt i forhold til formålet

([90]) EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014, præmis 81-83.

med databehandlingen. EU-Domstolen anerkendte, at denne ret ikke er absolut. Den skal afvejes mod andre rettigheder, navnlig den brede offentligheds interesse og ret til at få adgang til oplysningerne. Hver sletningsanmodning skal vurderes individuelt for at afveje de grundlæggende rettigheder til beskyttelse af personoplysninger og den registreredes privatliv med alle internetbrugeres legitime interesser. EU-Domstolen vejledte omkring de faktorer, der skal tages i betragtning ved afvejningen. Arten af de pågældende oplysninger er en særlig vigtig faktor. Hvis oplysningerne er følsomme for den berørte persons privatliv, og hvis offentligheden ikke har nogen interesse i at råde over disse oplysninger, vil databeskyttelse og privatliv veje tungere end den brede offentligheds ret til at få adgang til oplysningerne. Hvis det på den anden side virker som om, at den registrerede er en fremtrædende person, eller at oplysningernes art begrunder, at den brede offentlighed gives adgang til dem, så er indgrebet i den grundlæggende ret til databeskyttelse og privatliv begrundet.

Efter dommen vedtog Artikel 29-Gruppen retningslinjer om gennemførelse af EU-Domstolens afgørelse. Retningslinjerne indeholder en liste over fælles kriterier, som tilsynsmyndighederne kan benytte ved håndtering af klager vedrørende fysiske personers sletningsanmodninger, og som kan vejlede dem under denne afvejning af rettigheder ([91]).

EMD har afsagt flere principielle domme omkring forening mellem retten til databeskyttelse og retten til ytringsfrihed.

Eksempel: I sagen *Axel Springer AG mod Tyskland* ([92]) fastslog EMD, at et forbud, som forhindrede den sagsøgende virksomhed i at offentliggøre en artikel om anholdelsen og domfældelsen af en kendt skuespiller, var i strid med artikel 10 i EMRK. EMD gentog de kriterier, som den havde fastlagt i sin retspraksis for afvejning af retten til ytringsfrihed i forhold til retten til respekt for privatlivet:

- om den pågældende offentliggjorte artikels emne var af almen interesse

([91]) Artikel 29-Gruppen (2014), *Guidelines on the implementation of the CJEU judgment on »Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González« C-131/12*, WP 225, Bruxelles, 26. november 2014.

([92]) EMD, *Axel Springer AG mod Tyskland* [GC], nr. 39954/08, 7. februar 2012, præmis 90 og 91.

- om den berørte person var en offentlig figur
- hvordan oplysningerne var blevet fremskaffet, og om de var pålidelige.

EMD fandt, at skuespillerens anholdelse og domfældelse var en del af en offentlig retshandling og dermed af samfundsmæssig interesse, at skuespilleren var tilstrækkeligt kendt til at blive betegnet som en offentlig figur, at oplysningerne var blevet udleveret af den offentlige anklager, og at rigtigheden af oplysningerne ikke blev anfægtet af parterne. Begrænsningerne med hensyn til offentliggørelse, der var blevet pålagt selskabet, havde derfor ikke været rimelige i forhold til det legitime mål om at beskytte sagsøgerens privatliv. Domstolen konkluderede, at EMRK's artikel 10 var blevet overtrådt.

Eksempel: Sagen *Coudec og Hachette Filipacchi Associés mod France* ([93]) omhandlede et fransk ugeblads offentliggørelse af et interview med fru Coste, som påstod, at fyrst Albert af Monaco var far til hendes søn. Interviewet beskrev også forholdet mellem fru Coste og fyrsten og den måde, som han reagerede på ved barnets fødsel, og var ledsaget af billeder af fyrsten med barnet. Fyrst Albert anlagde sag mod forlaget for at have overtrådt hans ret til beskyttelse af privatlivets fred. De franske domstole fastholdt, at artiklens offentliggørelse havde forårsaget uoprettelige skader for fyrst Albert og krævede, at udgiveren betalte en erstatning og offentliggjorde dommens detaljer på magasinets forside.

Udgiverne af magasinet indbragte sagen for EMD, hvor de påstod, at de franske domstoles dom var et uberettiget indgreb i deres ret til ytringsfrihed. EMD skulle afveje fyrst Alberts ret til respekt for privatlivets fred mod udgiverens ret til ytringsfrihed og den brede offentligheds ret til at besidde disse oplysninger. Fru Costes ret til at dele hendes historie med offentligheden og barnets interesse i officielt at fastlægge forholdet mellem far og barn var også vigtige overvejelser.

EMD fastholdt, at interviewets offentliggørelse var et indgreb i fyrstens privatliv og undersøgte derefter, om indgrebet var nødvendigt. Den vurderede, at offentliggørelsen omhandlede en offentlig figur og et emne af offentlig interesse, da Monacos borgere havde en interesse i at kende til eksistensen af fyrstens barn, siden et arveligt monarkis fremtid uløseligt afhænger af

([93]) EMD, *Coudec og Hachette Filipacchi Associés mod Frankrig* [GC], nr. 40454/07, 10. november 2015.

eksistensen af efterkommere, og det var derfor et emne, som var genstand for offentlighedens bekymring ([94]). Domstolen bemærkede også, at artiklen havde givet fru Coste og hendes barn mulighed for at udøve deres ret til ytringsfrihed. De nationale domstole havde ikke taget behørigt hensyn til de principper og kriterier, som er udviklet i EMD's retspraksis til afvejning af retten til respekt for privatliv mod retten til ytringsfrihed. Den konkluderede, at Frankrig havde overtrådt EMRK's artikel 10 om ytringsfrihed.

I EMD's retspraksis er et af de vigtigste kriterier i forbindelse med afvejningen af disse rettigheder, om den pågældende ytring bidrager til en debat af generel samfundsinteresse.

Eksempel: I sagen *Mosley mod Det Forenede Kongerige* ([95]) offentliggjorde en national ugeavis intime fotos af sagsøgeren, som var en velkendt skikkelse, der senere anlagde en erstatningssag mod udgiveren, som vedkommende fik tildelt. På trods af den tildelte økonomiske erstatning klagede han over, at hans ret til privatlivets fred stadig blev overtrådt, da han ikke havde haft mulighed for at få nedlagt forbud mod offentliggørelsen af de pågældende fotos, fordi avisen ikke var underlagt et anmeldelseskrav i forbindelse med offentliggørelse af materiale.

EMD bemærkede, at selv om sådant materiale generelt blev offentliggjort med henblik på underholdning snarere end undervisning, var offentliggørelsen uden tvivl beskyttet under artikel 10 i EMRK, som muligvis viger for kravene i artikel 8 i EMRK, såfremt oplysningerne var af privat og intim karakter, og offentliggørelsen ikke var af samfundsmæssig interesse. Begrænsninger, der kunne fungere som en form for censur inden offentliggørelse, skulle dog undersøges særligt nøje. Med hensyn til den afskrækkende virkning, som et anmeldelseskrav kunne have, tvivlen om dets effektivitet og de brede muligheder for skøn på området konkluderede EMD, at et retligt bindende anmeldelseskrav ikke var påkrævet i henhold til artikel 8. Domstolen konkluderede derfor, at EMRK's artikel 8 ikke var blevet overtrådt.

([94]) *Ibid*., præmis 104-116.

([95]) EMD, *Mosley mod Det Forenede Kongerige*, nr. 48009/08, 10. maj 2011, præmis 129 og 130.

Eksempel: I sagen *Bohlen mod Tyskland* ([96]) havde sagsøgeren, en kendt sanger, kunstner og producer, offentliggjort en selvbiografisk bog og derefter været tvunget til at fjerne bestemte passager som følge af retsafgørelser. Historien blev i stor udstrækning dækket i de nationale medier, og en tobaksvirksomhed iværksatte en humoristisk kampagne, der henviste til denne hændelse og brugte sagsøgerens fornavn uden tilladelse. Sagsøgeren søgte forgæves om erstatning fra reklamefirmaet, hvor han påstod, at hans rettigheder under EMRK's artikel 8 var blevet krænket. EMD gentog kriteriet, som vejleder afvejningen mellem retten til respekt for privatliv og retten til ytringsfrihed, og fastholdt, at der ikke var nogen overtrædelse af artikel 8. Sagsøgeren var en offentlig figur, og reklamen henviste ikke til detaljer for hans privatliv, men til en offentlig hændelse, som medierne allerede havde dækket og var blevet en del af en offentlig debat. Desuden havde reklamen en humoristisk karakter og indeholdt intet nedsættende eller negativt om sagsøgeren.

Eksempel: I sagen *Biriuk mod Litauen* ([97]) hævdede sagsøgeren for EMD, at Litauen ikke havde opfyldt dennes forpligtelse om at sikre, at hendes ret til privatlivets fred blev respekteret, da de nationale domstole, der havde behandlet hendes sag, havde tildelt hende et ubetydeligt beløb som erstatning, selvom en stor avis havde begået en alvorlig krænkelse af hendes privatliv. Ved tildeling af godtgørelsen for den ikke-økonomiske skade havde nationale domstole taget udgangspunkt i bestemmelserne i den nationale lovgivning om meddelelse af oplysninger til offentligheden, der fastlagde et lavt erstatningsloft for ikke-økonomiske skader, som forårsages af mediernes ulovlige offentliggørelse af oplysninger om en persons privatliv. Sagen startede ved, at det største litauiske dagblad havde offentliggjort en forsideartikel om, at sagsøgeren var hiv-positiv. Artiklen kritiserede også sagsøgerens opførsel og sådede tvivl om hendes moralske standarder.

EMD gentog, at beskyttelsen af personoplysninger, og ikke mindst medicinske data, er af afgørende betydning for retten til respekt for privatliv i henhold til EMRK. Fortroligheden af helbredsoplysninger er særlig vigtig, da offentliggørelse af medicinske data (i dette tilfælde sagsøgerens hiv-status) kan påvirke en persons privatliv og familieliv, hans eller hendes beskæftigelsessituation og integration i samfundet på dramatisk vis. Domstolen lagde især vægt på, at hospitalspersonalet i henhold til avisens rapport i klar strid med

([96]) EMD, *Bohlen mod Tyskland*, nr. 53495/09, 19. februar 2015, præmis 45-60.

([97]) EMD, *Biriuk mod Litauen*, nr. 23373/03, 25. november 2008.

dets tavshedspligt havde givet oplysninger om sagsøgerens hiv-status. Som følge deraf var det ikke et legitimt indgreb i sagsøgerens ret til respekt for sit privatliv.

Artiklen var offentliggjort af pressen, og ytringsfrihed er også en grundlæggende rettighed i henhold til EMRK. I løbet af undersøgelsen af, om eksistensen af en samfundsmæssig interesse begrundede offentliggørelsen af denne form for oplysninger om sagsøgeren, konstaterede Domstolen dog, at det primære formål med offentliggørelsen var at øge salget af aviser ved at tilfredsstille læsernes nysgerrighed. Et sådant formål kan ikke vurderes at bidrage til nogen debat af almen interesse for samfundet. Da dette var en sag med et skandaløst misbrug af pressefriheden, forsøget på at afhjælpe skaderne var stærkt begrænset, og godtgørelsens størrelse for den ikke-økonomiske skade fastlagt i national lovgivning var meget lille, betød det, at Litauen ikke havde opfyldt sin forpligtelse om at beskytte sagsøgerens ret til privatliv. EMD konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Retten til ytringsfrihed og retten til beskyttelse af personoplysninger er ikke altid i konflikt. Der er tilfælde, hvor den effektive beskyttelse af personoplysninger garanterer ytringsfrihed.

Eksempel: EU-Domstolen fastslog i *Tele2 Sverige*, at indgrebet fra direktiv 2006/24/EF (datalagringsdirektivet) i de grundlæggende rettigheder fastslået i Chartrets artikel 7 og 8 var »vidtrækkende og må anses for at være særligt alvorligt. Den omstændighed, at lagringen af data finder sted, uden at brugerne af de elektroniske kommunikationstjenester oplyses herom, er egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant overvågning«. EU-Domstolen fandt derudover, at den generelle lagring af trafik- og lokaliseringsdata kunne have en indvirkning på brugen af de elektroniske kommunikationsmidler og »følgelig på brugerne af disse midlers udøvelse af deres ytringsfrihed, som er sikret ved Chartrets artikel 11« ([98]). I den sammenhæng bidrager databeskyttelsesregler i sidste ende til udøvelsen af ytringsfrihed ved at kræve strenge krav for, at datalagring ikke udføres på generel vis.

([98]) EU-Domstolen, forenede sager C-203/15 og C-698/15, *Tele2 Sverige AB mod Post- och telestyrelsen og Secretary of State for the Home Department mod Tom Watson m.fl.* [GC], 21. december 2016, præmis 37 og 101; EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl. og Kärntner Landesregierung m.fl.* [GC], 8. april 2014, præmis 28.

I forbindelse med retten til at modtage oplysninger, der også er en del af ytringsfrihed, er der en voksende erkendelse af, hvor vigtig gennemsigtig forvaltning er for et demokratisk samfunds funktion. Gennemsigtighed er et mål af almen interesse, der derfor kan begrunde et indgreb i retten til databeskyttelse, hvis det er nødvendigt og proportionelt, som forklaret i afsnit 1.2. I de seneste to årtier er retten til at få adgang til dokumenter i offentlige myndigheders besiddelse som følge heraf blevet anerkendt som en vigtig rettighed for alle EU-borgere og alle fysiske eller juridiske personer, der er bosiddende eller har registreret kontor i en medlemsstat.

I Europarådets retsorden kan der henvises til principperne i henstillingen vedrørende adgang til officielle dokumenter, som var udgangspunkt for udformningen af konventionen om aktindsigt (konvention 205) ([99]).

I EU-retten er retten til aktindsigt sikret ved forordning (EF) nr. 1049/2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (forordningen om aktindsigt) ([100]). Denne ret til aktindsigt er ved Chartrets artikel 42 og artikel 15, stk. 3, i TEUF blevet udvidet til »aktindsigt i dokumenter, uanset medium, fra Unionens institutioner, organer, kontorer og agenturer«.

Denne ret kan komme i konflikt med retten til databeskyttelse, hvis aktindsigt i et dokument afslører andre personers personoplysninger. Artikel 86 i den generelle forordning om databeskyttelse fastlægger tydeligt, at personoplysninger i officielle dokumenter i offentlige myndigheders og organers besiddelse kan videregives af myndigheden eller organet i overensstemmelse med EU-retten ([101]) eller medlemsstaternes nationale ret for at forene aktindsigt i officielle dokumenter med retten til beskyttelse af personoplysninger i henhold til forordningen.

Anmodninger om aktindsigt i dokumenter eller information, som myndighederne er i besiddelse af, skal derfor afvejes i forhold til retten til databeskyttelse for de personer, hvis data er indeholdt i de pågældende dokumenter.

([99]) Europarådet, Ministerudvalget (2002), Henstilling R (81) 19 og Rec(2002)2 til medlemsstaterne om aktindsigt, 21. februar 2002; Europarådet, konvention om aktindsigt, CETS nr. 205, 18. juni 2009. Konventionen er endnu ikke trådt i kraft.

([100]) Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter, EFT L 145 af 31. maj 2001.

([101]) Artikel 42 i Chartret, artikel 15, stk. 3, i TEUF og forordning nr. 1049/2009.

Eksempel: I sagen *Volker und Markus Schecke og Hartmut Eifert mod Land Hessen* ([102]) skulle EU-Domstolen vurdere proportionaliteten af offentliggørelsen i medfør af EU-retten af navnene på modtagerne af EU-landbrugsstøtte og de beløb, de havde modtaget. Offentliggørelsens mål var at forbedre gennemsigtighed og bidrage til at kontrollere, at forvaltningen anvender de offentlige midler korrekt. Flere støttemodtagere har anfægtet proportionaliteten af denne offentliggørelse.

EU-Domstolen, som bemærkede, at retten til databeskyttelse ikke er absolut, anførte, at offentliggørelsen af personoplysninger om de omhandlede modtagere og de nøjagtige beløb, som de har modtaget fra de to EU-landbrugsfonde, på en hjemmeside, udgør et indgreb i støttemodtagernes ret til privatliv i almindelighed og et indgreb i deres ret til beskyttelse af deres personoplysninger i særdeleshed.

EU-Domstolen fandt, at et sådant indgreb i Chartrets artikel 7 og 8, skulle anses for at være fastlagt i lovgivningen og forfulgte et mål af almen interesse, der er anerkendt af EU, nemlig at styrke gennemsigtigheden omkring anvendelsen af fællesskabsmidlerne. EU-Domstolen fastslog dog, at offentliggørelsen af navnene på fysiske personer, som modtager EU-landbrugsstøtte fra disse to fonde, og de nøjagtige beløb, som de har modtaget, udgør en uforholdsmæssig foranstaltning og ikke er berettiget, for så vidt angår Chartrets artikel 52, stk. 1. Den anerkendte vigtigheden af at holde skatteydere informeret om brugen af offentlige midler i et demokratisk samfund. Men formålet »om åbenhed er dog ikke tillagt en automatisk forrang for beskyttelsen af personoplysninger« ([103]), og EU-institutioner var forpligtede til at foretage en afvejning mellem Unionens interesse i gennemsigtighed og begrænsningen i udøvelsen af de rettigheder til privatliv og databeskyttelse, som støttemodtagere blev udsat for som følge af offentliggørelsen.

EU-Domstolen mente, at EU-institutionerne ikke havde foretaget denne afvejning korrekt, da det var muligt at forestille sig foranstaltninger, der i mindre grad ville påvirke de enkelte personers grundlæggende rettigheder, mens de på samme tid effektivt bidrager til målet om gennemsigtighed forfulgt af offentliggørelsen. I stedet for en generel offentliggørelse, der påvirker alle

([102]) EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 9. november 2010, præmis 47-52, 58, 66-67, 75, 86 og 92.

([103]) *Ibid.*, præmis 85.

støttemodtagere ved at angive deres navn og de nøjagtige beløb, hver af dem har modtaget, kunne man foretage en sondring i henhold til relevante kriterier, såsom i hvilken periode de har modtaget disse midler, hyppigheden af en sådan modtagelse eller midlernes art og omfang ([104]). EU-Domstolen erklærede derfor EU-bestemmelserne om offentliggørelsen af oplysninger vedrørende modtagere af støtte fra de europæiske landbrugsfonde for delvist ugyldige.

Eksempel: I sagen *Rechnungshof mod Österreichischer Rundfunk m.fl.* ([105]) gennemgik EU-Domstolen foreneligheden mellem visse bestemmelser i østrigsk lovgivning og EU's databeskyttelseslovgivning. Lovgivningen krævede, at et statsligt organ indsamlede og overførte data om indkomst med henblik på at offentliggøre navnet på og indkomsten for medarbejdere hos forskellige offentlige enheder i en årlig rapport, der blev gjort tilgængelig for den brede offentlighed. Nogle enkelte personer afviste at meddele deres data på baggrund af databeskyttelse.

I sin udtalelse henviste EU-Domstolen til, at beskyttelsen af grundlæggende rettigheder er et generelt princip i EU-ret, samt artikel 8 i EMRK, hvor den mindede om, at Chartret ikke var bindende på daværende tidspunkt. Den fastholdt, at indsamlingen af data om enkeltpersoners erhvervsmæssige indkomst, og navnlig deres videregivelse til tredjemænd, er omfattet af retten til respekt for privatliv og overtræder denne rettighed. Indgrebet kunne have været berettiget, hvis det havde været i overensstemmelse med loven, forfulgte et legitimt mål, og det havde været nødvendigt i et demokratisk samfund til at opnå dette mål. EU-Domstolen bemærkede, at den østrigske lovgivning forfulgte et legitimt mål, da dets mål var at holde lønnen til offentlige medarbejdere inden for rimelige grænser – en overvejelse, der også hænger sammen med landets økonomiske velfærd. Østrigs interesse i at sikre den bedste udnyttelse af offentlige midler skulle dog afvejes mod alvoren af indgrebet i de pågældende personers ret til respekt for deres privatliv.

EU-Domstolen lod det være op til den nationale domstol at vurdere, om offentliggørelsen af dataene om de enkelte personers indkomst var nødvendig og proportionel med lovgivningens mål, og opfordrede den nationale

([104]) *Ibid.*, præmis 89.

([105]) EU-Domstolen, forenede sager C-465/00, C-138/01 og C-139/01, *Rechnungshof mod Österreichischer Rundfunk m.fl. og Christa Neukomm og Jospeh Lauermann mod Österreichischer Rundfunk*, 20. maj 2003.

domstol til at undersøge, om et sådant mål kunne være opnået ved mindre krænkende midler med samme effektivitet. Et eksempel ville være, at personoplysninger kun overføres til de offentlige tilsynsorganer og ikke den brede offentlighed.

I de efterfølgende sager blev det klart, at afvejningen mellem databeskyttelse og aktindsigt i dokumenter kræver en detaljeret analyse af den enkelte sag. Ingen af disse rettigheder tilsidesætter automatisk den anden. EU-Domstolen havde mulighed for at fortolke retten til aktindsigt i dokumenter med personoplysninger i to sager.

Eksempel: I sagen *Europa-Kommissionen mod The Bavarian Lager* ([106]) definerede EU-Domstolen anvendelsesområdet for beskyttelse af personoplysninger i forbindelse med aktindsigt i EU-institutionernes dokumenter og forholdet mellem forordning (EF) nr. 1049/2001 (forordningen om aktindsigt) og forordning (EF) nr. 45/2001 (forordningen om databeskyttelse inden for EU-institutionerne). Bavarian Lager, som blev etableret i 1992, importerer tysk øl på flasker til Det Forenede Kongerige, især til pubber og barer. Virksomheden stødte dog på vanskeligheder, fordi den britiske lovgivning i realiteten begunstigede nationale producenter. Som svar på Bavarian Lagers klage besluttede Europa-Kommissionen at rejse en sag mod Det Forenede Kongerige for dets manglende opfyldelse af dets forpligtelser, hvilket fik landet til at ændre de anfægtede bestemmelser og tilpasse dem til EU-retten. Bavarian Lager anmodede derefter Kommissionen om bl.a. en kopi af referatet af et møde, der var blevet afholdt med deltagelse af repræsentanter for Kommissionen, de britiske myndigheder og *Confédération des Brasseurs du Marché Commun* (CBMC). Kommissionen indvilgede i at fremlægge visse dokumenter vedrørende mødet, men udelod fem navne fra referatet af mødet, da to personer udtrykkeligt var imod offentliggørelsen af deres identitet, og Kommissionen ikke havde fået kontakt til de tre øvrige personer. Ved beslutning af 18. marts 2004 afslog Kommissionen en bekræftende begæring fra Bavarian Lager med henblik på at få udleveret det fulde referat af mødet med særlig henvisning til beskyttelsen af disse personers privatliv som sikret ved forordningen om databeskyttelse inden for EU-institutionerne.

([106]) EU-Domstolen, C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd.* [GC], 29. juni 2010.

Da Bavarian Lager ikke kunne acceptere dette, indbragte virksomheden sagen for Retten. Retten annullerede Kommissionens beslutning ved dennes dom af 8. november 2007 (sag T-194/04, *The Bavarian Lager Co. Ltd mod Kommissionen for De Europæiske Fællesskaber*) med den begrundelse, at den blotte omstændighed, at der gives oplysning om, at en fysisk person som repræsentant for et organ har deltaget i et møde, ikke anses for et indgreb i privatlivets fred og ikke var til skade for de berørte personers ret til privatlivets fred.

Efter Kommissionens appel annullerede EU-Domstolen Rettens dom. EU-Domstolen fastslog, at forordningen om aktindsigt »fastsætter en særlig ordning, som styrker beskyttelsen af personer, hvis personoplysninger i givet fald vil kunne udbredes til offentligheden«. Når formålet med en begæring, som er baseret på forordningen om aktindsigt, er at få aktindsigt i dokumenter, der indeholder personoplysninger, gælder bestemmelserne i forordningen om databeskyttelse inden for EU-institutionerne således fuldt ud i henhold til EU-Domstolen. EU-Domstolen konkluderede derefter, at Kommissionen med rette gav afslag på anmodningen om aktindsigt i det fulde referat af mødet, som blev afholdt i oktober 1996. Da Kommissionen ikke havde fået de fem mødedeltageres samtykke, opfyldte den i tilstrækkelig grad sin forpligtelse til åbenhed ved at udlevere en version af det pågældende dokument, hvor deres navne var udeladt.

EU-Domstolen fastslog videre: »Eftersom Bavarian Lager hverken er fremkommet med nogen udtrykkelig og lovlig begrundelse eller har fremført noget overbevisende argument for at godtgøre, at en videregivelse af disse personoplysninger var nødvendig, har Kommissionen ikke kunnet foretage en afvejning af de berørte parters forskellige interesser. Kommissionen kunne heller ikke kontrollere, om der fandtes nogen grund til at antage, at denne videregivelse ville kunne skade de berørte personers legitime interesser«, således som foreskrevet i forordningen om databeskyttelse inden for EU-institutionerne.

Eksempel: I sagen *ClientEarth og PAN Europa mod EFSA* ([107]) undersøgte EU-Domstolen, om Den Europæiske Fødevaresikkerhedsautoritets (EFSA) afgørelse om at afvise sagsøgernes fulde aktindsigt i dokumenter var

([107]) EU-Domstolen, C-615/13 P, *ClientEarth og Pesticide Action Network Europe (PAN Europe) mod Den Europæiske Fødevaresikkerhedsautoritet (EFSA) og Europa-Kommissionen*, 16. juli 2015.

nødvendig for at beskytte retten til privatliv og databeskyttelse for de personer, som dokumenterne henviste til. Dokumenterne omhandlede et udkast til en vejledende rapport, som var udarbejdet af en arbejdsgruppe ved EFSA i samarbejde med eksterne eksperter, om markedsføring af plantebeskyttelsesmidler. Til at starte med tildelte EFSA delvis adgang til sagsøgerne, hvor den afviste adgang til visse arbejdsversioner af udkastet til vejledning. Derefter tildelte den adgang til udkastet, som indeholdt enkelte bemærkninger fra de eksterne eksperter. Den udelod dog navnene på eksperterne under henvisning til artikel 4, stk. 1, litra b), i forordning (EF) nr. 45/2001 om behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og behovet for at beskytte de eksterne eksperters privatliv. I første instans gav Den Europæiske Unions Ret medhold til EFSA's afgørelse.

Efter appel fra sagsøgerne omstødte EU-Domstolen dommen fra den første instans. Den konkluderede, at overførslen af personoplysninger i det pågældende tilfælde var nødvendig for at vurdere upartiskheden for hver af de eksterne eksperter under udførelsen af deres opgaver som forskere og for at sikre, at beslutningsprocessen hos EFSA forbliver gennemsigtig. I henhold til EU-Domstolen angav EFSA ikke, hvordan afsløring af navnene på de eksterne eksperter, som havde fremført specifikke bemærkninger om udkastet til vejledning, ville beskadige deres legitime interesser. Et generelt argument om, at udbredelsen sandsynligvis vil være til skade for privatlivet, er ikke nok, hvis det ikke understøttes af dokumentation i den enkelte sag.

I medfør af disse domme er det nødvendigt med en specifik og behørig begrundelse ved indgreb i retten til databeskyttelse i forbindelse med aktindsigt i dokumenter. Retten til aktindsigt i dokumenter tilsidesætter ikke automatisk retten til databeskyttelse ([108]).

Denne tilgang minder om EMD's i forbindelse med privatliv og aktindsigt i dokumenter, hvilket følgende dom demonstrerer. I *Magyar Helsinki*-dommen fastslog EMD, at artikel 10 ikke giver en fysisk person ret til aktindsigt i oplysninger, som en offentlig myndighed er i besiddelse af, eller forpligter regeringen til at meddele sådanne oplysninger til en fysisk person. En sådan ret eller forpligtelse kan dog opstå i tilfælde, hvor offentliggørelse af oplysningerne er pålagt ved en retsgyldig kendelse, eller hvor adgang til oplysningerne er nødvendig for, at en fysisk person

([108]) Se dog den detaljerede gennemgang i EDPS (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bruxelles, 24. marts 2011.

kan udøve hans eller hendes ret til ytringsfrihed — navnlig friheden til at modtage og meddele oplysninger — og hvor nægtelse heraf ville krænke den ret ([109]). Om, og i hvilket omfang, nægtelse af adgang til oplysninger udgør et indgreb i en sagsøgers ytringsfrihed, skal vurderes i det enkelte tilfælde og på baggrund af de pågældende omstændigheder, herunder: i) formålet med anmodningen om oplysninger, ii) arten af de begærede oplysninger, iii) sagsøgerens rolle og iv) hvorvidt oplysningerne var klargjorte og tilgængelige.

Eksempel: I sagen *Magyar Helsinki Bizottság mod Ungarn* ([110]) anmodede sagsøgeren, en menneskerettigheds-NGO, om oplysninger fra politiet vedrørende en *ex officio*-forsvarer for at udføre en undersøgelse af driften af Ungarns system for offentlige forsvarere. Politiet afviste at fremkomme med oplysningerne, da de argumenterede, at det var personoplysninger, som ikke var undergivet oplysningspligt. Ved brug af ovenstående kriterier fastholdt EMD, at der havde været et indgreb i en rettighed beskyttet under artikel 10. Mere præcist ønskede sagsøgeren at udøve retten til at meddele oplysninger om et emne af almen interesse, vedkommende havde anmodet om oplysninger til det formål, og de oplysninger var nødvendige til, at sagsøgeren kunne udøve sin ret til ytringsfrihed. Oplysningerne om udpegelsen af offentlige forsvarere var i offentlighedens interesse. Der var ingen grund til at tvivle på, at den pågældende undersøgelse indeholdt oplysninger, som sagsøgeren meddelte til offentligheden, og som offentligheden havde en ret til at modtage. Domstolen accepterede derfor, at det var nødvendigt for sagsøgeren at få adgang til de anmodede oplysninger for at fuldføre opgaven. Endelig var oplysningerne klargjorte og tilgængelige.

EMD konkluderede, at nægtelse af adgang til oplysninger i dette tilfælde havde krænket selve kernen af friheden til at modtage oplysninger. Efter at have draget denne konklusion undersøgte EMD især formålet med de oplysninger, der var anmodet om, og deres bidrag til en vigtig offentlig debat, arten af de efterspurgte oplysninger, og hvorvidt de har en samfundsmæssig interesse, og den samfundsrolle, som sagsøgeren havde spillet i sagen.

Domstolen bemærkede i sin begrundelse, at undersøgelsen udført af den pågældende NGO omhandlede retfærdighed og retten til en retfærdig rettergang, hvilket er en rettighed, som er af altafgørende betydning i henhold til

([109]) EMD, *Magyar Helsinki Bizottság mod Ungarn* [GC], nr. 18030/11, 8. november 2016, præmis 148.

([110]) *Ibid*., præmis 181, 187-200.

EMRK. Da de oplysninger, der var anmodet om, kun omfattede data, som er frit tilgængelige, ville privatlivsrettighederne for de pågældende registrerede (de *ex officio*-offentlige forsvarere) ikke være krænket, hvis politiet havde givet sagsøgeren adgang til oplysningerne. Oplysningerne, som sagsøgeren havde anmodet om, var af statistisk art og omhandlede de antal gange, som *ex officio*-advokaten havde været udpeget til at repræsentere anklagede i offentlige strafferetlige sager.

Domstolen var af den holdning, at enhver begrænsning af NGO'ens foreslåede offentliggørelse burde været blevet underlagt en grundig kontrol, da undersøgelsens mål var at bidrage til en vigtig debat om et emne af almen interesse. De pågældende oplysninger var af almen interesse, da almen interesse omfatter emner, der kan give anledning til betydelige uoverensstemmelser, der omhandler et vigtigt socialt problem, eller der omfatter et problem, som offentligheden har en interesse i at blive informeret om ([111]). Denne definition omfatter uden tvivl en diskussion om retfærdighed og udførelse af retfærdig rettergang, hvilket var emnet for sagsøgerens undersøgelse. Under afvejning af de forskellige rettigheder, som er på spil, og brug af proportionalitetsprincippet fastholdt EMD, at der havde været en ubegrundet krænkelse af sagsøgerens rettigheder i medfør af EMRK's artikel 10.

1.3.2. Tavshedspligt

Visse kommunikationer kan som følge af national lovgivning være underlagt tavshedspligt. Tavshedspligt kan forstås som en særlig etisk pligt, der medfører en lovbestemt forpligtelse, og som er en fast del af visse erhverv og funktioner, der er baseret på tro og tillid. Personer og institutioner, der opfylder disse funktioner, er forpligtede til ikke at afsløre fortrolige oplysninger, de har modtaget i løbet af udførelsen af deres arbejdsopgaver. Tavshedspligt er navnligt gældende for sundhedssektoren og forholdet mellem advokater og deres klienter. Mange områder anerkender også tavshedspligt inden for finanssektoren. Tavshedspligt er ikke en grundlæggende rettighed, men er beskyttet som en form af retten til respekt for privatliv. EU-Domstolen har for eksempel fastslået, at under nogle omstændigheder »kan det være nødvendigt ikke at videregive bestemte fortrolige oplysninger med henblik på at beskytte en virksomheds grundlæggende ret til privatlivets fred, som er knæsat i artikel 8 i den europæiske konvention til beskyttelse

([111]) *Ibid.*, præmis 156.

af menneskerettigheder og grundlæggende frihedsrettigheder, undertegnet i Rom den 4. november 1950 (herefter »EMRK«), og i chartrets artikel 7« ([112]). EMD er også blevet bedt om at tage stilling til, om begrænsninger af tavshedspligt udgør en overtrædelse af EMRK's artikel 8, som illustreret i de fremhævede eksempler.

Eksempel: I sagen *Pruteanu mod Rumænien* ([113]) fungerede sagsøgeren som advokat for en kommerciel virksomhed, som havde fået forbud mod at udføre banktransaktioner efter anklager om svindel. I løbet af undersøgelsen af sagen gav de rumænske domstole anklagemyndigheden lov til at aflytte og optage en virksomhedspartners telefonsamtaler over en bestemt periode. Optagelserne og aflytningerne omfattede hans kommunikationer med sin advokat.

Pruteanu påstod, at dette var et indgreb i hans ret til respekt for privatliv og korrespondance. I sin dom fremhævede EMD statussen og betydningen af en advokats forhold til vedkommendes klient. Aflytningen af en advokats samtaler med sin klient overtrådte uden tvivl tavshedspligten, som var grundlaget for forholdet mellem disse to personer. I dette tilfælde kan advokaten også klage over et indgreb i dennes ret til respekt for privatliv og korrespondance. EU-Domstolen fastholdt, at EMRK's artikel 8 var blevet overtrådt.

Eksempel: I sagen *Brito Ferrinho Bexiga Villa-Nova mod Portugal* ([114]) afviste sagsøgeren, en advokat, at offentliggøre dennes personlige banksaldoer til skattemyndighederne på grundlag af tavshedspligt og bankhemmelighed. Anklagemyndigheden indledte en undersøgelse i skattesvig og bad om tilladelse til at suspendere tavhedspligten. De nationale domstole krævede, at reglerne om tavshedspligt og bankhemmelighed skulle suspenderes, da den mente, at almene interesser vejede tungere end sagsøgerens private interesser.

Da sagen nåede EMD, fastholdt Domstolen, at tilgåelsen af sagsøgerens banksaldoer var et indgreb i dennes ret til respekt for tavshedspligt, hvilket hører under privatliv. Indgrebet havde et retsgrundlag, da det var baseret på

([112]) EU-Domstolen, sag T-462/12 R, *Pilkington Group Ltd mod Europa-Kommissionen*, kendelse afsagt af Rettens præsident, 11. marts 2013, præmis 44.

([113]) EMD, *Pruteanu mod Rumænien*, nr. 30181/05, 3. februar 2015.

([114]) EMD, *Brito Ferrinho Bexiga Villa-Nova mod Portugal*, nr. 69436/10, 1. december 2015.

strafferetsplejeloven og forfulgte et legitimt mål. Men efter undersøgelse af indgrebets nødvendighed og proportionalitet påpegede EMD, at søgsmålet om ophævelse af fortrolighed blev gennemført uden sagsøgerens deltagelse eller viden. Sagsøgeren havde derfor ikke mulighed for at fremføre sine argumenter. Derudover var sammenslutningen af advokater ikke blev rådført, selvom det er fastlagt som et krav i national lovgivning i forbindelse med sådanne søgsmål. Endelig havde sagsøgeren hverken mulighed for at anfægte ophævelsen af fortrolighed på effektiv vis eller noget retsmiddel, der kunne anfægte foranstaltningen. Grundet manglen på proceduremæssige garantier og effektiv retslig kontrol over foranstaltningen, som ophævede tavshedspligten, konkluderede EMD, at EMRK's artikel 8 var overtrådt.

Samspillet mellem tavshedspligt og databeskyttelse er ofte ambivalent. På den ene side hjælper databeskyttelsesregler og garantier fastlagt i lovgivningen med at sikre tavshedspligt. For eksempel er et af formålene med regler, som kræver, at dataansvarlige og databehandlere implementerer robuste datasikkerhedsforanstaltninger, at undgå tab af fortrolighed for personoplysninger beskyttet af tavshedspligt. Derudover muliggør EU's generelle forordning om databeskyttelse behandling af helbredsoplysninger, der udgør særlige kategorier af personoplysninger, som begrunder bedre beskyttelse, men denne behandling er underlagt tilstedeværelsen af egnede og særlige foranstaltninger til at sikre registreredes rettigheder, navnlig tavshedspligt ([115]).

På den anden side kan tavshedspligter pålagt dataansvarlige og databehandlere i forbindelse med bestemte personoplysninger begrænse de registreredes rettigheder, navnlig retten til at modtage oplysninger. Selvom den generelle forordning om databeskyttelse indeholder en omfattende liste med oplysninger, som principielt skal leveres til den registrerede, når personoplysninger ikke er indhentet fra vedkommende. Dette oplysningskrav er ikke gældende, hvis personoplysningerne skal forblive fortrolige som følge af en tavshedspligt krævet ved enten national lovgivning eller EU-ret ([116]).

Den generelle forordning om databeskyttelse (GDPR) fastlægger muligheden for, at medlemsstater ved lov kan vedtage specifikke regler for at sikre faglig eller anden

([115]) Den generelle forordning om databeskyttelse, artikel 9, stk. 2, litra h), og artikel 9, stk. 3.

([116]) *Ibid.*, artikel 14, stk. 5, litra d).

tilsvarende tavshedspligt, for så vidt det er nødvendigt for at forene retten til beskyttelse af personoplysninger med tavshedspligt ([117]).

GDPR fastlægger, at medlemsstater kan vedtage specifikke regler om tilsynsmyndighedernes beføjelser i forbindelse med dataansvarlige eller databehandlere, som er underlagt en tavshedspligt. Disse specifikke regler omhandler beføjelsen til at få adgang til alle lokaler hos en dataansvarlig eller databehandler, herunder til databehandlingsudstyr og lagrede personoplysninger, hvor sådanne personoplysninger er blevet modtaget i løbet af en aktivitet, som er omfattet af tavshedspligt. De tilsynsmyndigheder, som er ansvarlige for databeskyttelse, skal overholde tavshedspligter, som er gældende for dataansvarlige eller databehandlere. Derudover er tilsynsmyndigheders medlemmer også selv underlagt en tavshedspligt under og efter deres embedsperiode. Medlemmer og personalet hos tilsynsmyndigheder kan i løbet af udøvelsen af deres arbejdsopgaver få kendskab til fortrolige oplysninger. Forordningens artikel 54, stk. 2, fastlægger tydeligt, at de er underlagt tavshedspligt i forbindelse med sådanne fortrolige oplysninger.

GDPR kræver, at medlemsstater meddeler Kommissionen om de regler, de vedtager for at forene databeskyttelse og principperne fastlagt i forordningen med tavshedspligten.

1.3.3. Religions- og trosfrihed

Religions- og trosfrihed er beskyttet under artikel 9 i EMRK (ret til at tænke frit og til samvittigheds- og religionsfrihed) og artikel 10 i EU's charter om grundlæggende rettigheder. Personoplysninger, som afslører religiøse eller filosofiske overbevisninger, betragtes som »følsomme oplysninger« under både EU's og Europarådets retsorden, og deres behandling og brug er underlagt øget beskyttelse.

Eksempel: Sagsøgeren i sagen *Sinak Isik mod Tyrkiet* ([118]) var et medlem af det aleviske trossamfund, hvis tro er påvirket af sufisme og andre præislamiske overbevisninger og betragtes af nogle forskere som en særskilt religion og af andre som en del af den islamiske religion. Sagsøgeren klagede over, at hans identitetskort imod hans vilje indeholdt et felt, der angav hans religion som værende »islam« og ikke »alevi«. De nationale domstole afviste hans anmodning om at ændre sit identitetskort til »alevi« ud fra den baggrund,

([117]) *Ibid.*, betragtning 164 og artikel 90.

([118]) EMD, *Sinan Işık mod Tyrkiet*, nr. 21924/05, 2. februar 2010.

at ordet henviste til en undergruppe af islam og ikke en særskilt religion. Han indgav derefter en klage til EMD om, at han havde været tvunget til at meddele sin tro uden sit samtykke, da det var obligatorisk at angive en persons religion på identitetskortet, og at dette var et brud på hans ret til religions- og samvittighedsfrihed, især da betegnelsen »islam« på hans identitetskort ikke var korrekt.

EMD gentog, at religionsfrihed betyder friheden til, at en person kan udøve sin religion i fællesskab med andre, i det offentlige og inden for personkredsen, som deler samme tro, men også alene og i det private. Den nationale lovgivning, som var gældende på tidspunktet, forpligtede fysiske personer til at bære et identitetskort, som er et dokument, der skal vises ved anmodning fra en offentlig myndighed eller privat virksomhed, med angivelse af deres religion. Denne forpligtelse anerkendte ikke, at retten til at udøve ens religion også omfatter retten til ikke at afsløre ens religion. Selv om regeringen argumenterede, at den nationale lovgivning var blevet ændret, så fysiske personer kunne anmode om, at efterlade religionsfeltet på deres identitetskort tomt, havde Domstolen den holdning, at det faktum, at man er tvunget til at ansøge om at få sin religion slettet, er en form for videregivelse af oplysninger omkring holdninger til religion. Desuden har et tomt religionsfelt på et identitetskort en særlig betydning, da holdere af et identitetskort uden oplysninger om religion ville skille sig ud fra dem, som har et kort med angivelse af deres trosforhold. EMD konkluderede, at den nationale lovgivning overtrådte EMRK's artikel 9.

Driften af kirker og religiøse sammenslutninger og fællesskaber kan dog kræve behandling af medlemmernes personoplysninger, således at menigheden kan kommunikere indbyrdes og organisere aktiviteter. Kirker og religiøse sammenslutninger har derfor ofte implementeret regler vedrørende behandling af personoplysninger. I henhold til artikel 91 i den generelle forordning om databeskyttelse kan sådanne regler fortsat finde anvendelse, hvis de er omfattende, og de bringes i overensstemmelse med forordningens bestemmelser. Kirker og religiøse sammenslutninger, som har sådanne regler, skal være underlagt tilsyn af en uafhængig tilsynsmyndighed, som kan være specifik for dem, forudsat de opfylder kravene i den generelle forordning om databeskyttelse for sådanne myndigheder ([119]).

([119]) Den generelle forordning om databeskyttelse, artikel 91, stk. 2.

Religiøse organisationer kan udføre behandlingen af personoplysninger af flere årsager: for eksempel til at bibeholde kontakten med deres menighed eller meddele oplysninger omkring religiøse eller velgørende begivenheder og fester, der arrangeres. I visse stater skal kirker føre registre over deres medlemmer af skattemæssige årsager, da medlemskab af religiøse institutioner kan påvirke fysiske personers skyldige skattebeløb. Under alle omstændigheder er data, som afslører religiøse overbevisning, følsomme data i medfør af EU-retten, og kirker er ansvarlige for deres håndtering og behandling af sådanne oplysninger, navnlig da oplysninger, der behandles af religiøse organisationer, ofte omhandler børn, ældre eller andre sårbare samfundsgrupper.

1.3.4. Frihed for kunst og videnskab

En anden ret, der skal afvejes i forhold til retten til respekt for privatlivet og til databeskyttelse, er friheden for kunst og videnskab, som udtrykkeligt er beskyttet i medfør af Chartrets artikel 13. Denne ret er først og fremmest afledt af tanke- og ytringsfriheden og udøves under overholdelse af Chartrets artikel 1 (Den menneskelige værdighed). EMD finder, at friheden for kunst er beskyttet ved artikel 10 i EMRK ([120]). Den ret, der er sikret ved Chartrets artikel 13, kan også være underlagt begrænsningerne i Chartrets artikel 52, stk. 1, der også kan fortolkes ud fra artikel 10, stk. 2, i EMRK ([121]).

Eksempel: I sagen *Vereinigung bildender Künstler mod Østrig* ([122]) forbød de østrigske domstole den sagsøgende sammenslutning at fortsætte udstillingen af et maleri, der indeholdt fotos af hovederne af forskellige offentlige figurer i seksuelle stillinger. Et medlem af det østrigske parlament, hvis foto var anvendt i maleriet, anlagde sag mod den sagsøgende sammenslutning med begæring om et forbud mod udstilling af maleriet. Den nationale domstol nedlagde et forbud. EMD gentog, at artikel 10 i EMRK finder anvendelse på formidling af idéer, der støder, chokerer eller forstyrrer staten eller en del af befolkningen. Alle, der opretter, udfører, distribuerer eller udstiller kunstværker, bidrager til udvekslingen af idéer og holdninger, og staten var forpligtet til ikke uden grund at begrænse deres ytringsfrihed. Maleriet var en kollage og anvendte kun fotos af personernes hoveder, og deres kroppe var malet på en urealistisk og overdrevet måde, som tydeligvis ikke havde

([120]) EMD, *Müller m.fl. mod Schweiz*, nr. 10737/84, 24. maj 1988.

([121]) Forklaringer til Chartret om grundlæggende rettigheder, EUT C 303, 14. december 2007.

([122]) EMD, *Vereinigung bildender Künstler mod Østrig*, nr. 68354/01, 25. januar 2007, præmis 26 og 34.

til formål at afspejle eller ligne virkeligheden, og EMD fastslog videre, at maleriet næppe kunne opfattes således, at det gengav detaljer om den afbildedes privatliv, men snarere vedkommendes position som politiker, og at den afbildede i denne kapacitet skulle udvise en større tolerance over for kritik. I afvejningen af de forskellige berørte interesser fandt EMD, at det ubegrænsede forbud mod yderligere udstilling af maleriet var uforholdsmæssigt. Domstolen konkluderede, at EMRK's artikel 10 var blevet overtrådt.

Europæisk databeskyttelseslovgivning anerkender også den særlige værdi, som videnskaben har for samfundet. Den generelle forordning om databeskyttelse og den moderniserede konvention 108 tillader lagring af data i længere perioder, sålænge personoplysningerne udelukkende vil blive behandlet til videnskabelige eller historiske formål. Endvidere og uanset en bestemt behandlingsaktivitets oprindelige formål skal viderebehandlingen af personoplysninger til videnskabelige formål ikke anses for at være et uforeneligt formål ([123]). På samme tid skal der implementeres passende garantier for denne behandling for at beskytte de registreredes rettigheder og frihedsrettigheder. EU's eller medlemsstaters lovgivning kan fastlægge undtagelser fra registreredes rettigheder, såsom retten til adgang, berigtigelse, begrænsning af behandling og til at gøre indsigelse mod behandlingen af deres personoplysninger til videnskabelig forskning, historiske eller statistiske formål (se også afsnit 6.1. og afsnit 9.4.).

1.3.5. Beskyttelse af intellektuel ejendomsret

Ejendomsretten er omhandlet i artikel 1 i den første protokol til EMRK og i Chartrets artikel 17, stk. 1. Et vigtigt aspekt af ejendomsretten, som har særlig relevans for databeskyttelse, er beskyttelsen af den intellektuelle ejendomsret, som udtrykkeligt nævnes i Chartrets artikel 17, stk. 2. EU-retten omfatter flere direktiver, der har til formål effektivt at beskytte intellektuel ejendomsret, herunder især ophavsret. Intellektuel ejendom dækker ikke kun litterære og kunstneriske værker, men også patentrettigheder, varemærkerettigheder og tilknyttede rettigheder.

Som EU-Domstolens retspraksis tydeligt viser, skal beskyttelsen af den grundlæggende ejendomsret afvejes i forhold til beskyttelsen af andre grundlæggende rettigheder, herunder retten til databeskyttelse ([124]). Der har været sager, hvor

([123]) Generel forordning om databeskyttelse, artikel 5, stk. 1, litra b), og den moderniserede konvention 108, artikel 5, stk. 4, litra b).

([124]) EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU* [GC], 29. januar 2008, præmis 62-68.

organisationer, der arbejder for beskyttelse af ophavsret, har krævet, at internetudbydere skulle afsløre identiteten af brugere af internetbaserede fildelingsplatforme. Sådanne platforme giver ofte internetbrugere mulighed for at hente musiknumre gratis, selv om disse musiknumre er beskyttet af ophavsret.

Eksempel: *Promusicae mod Telefónica de España* ([125]) vedrørte en spansk internetudbyders, Telefónica, afslag på at meddele Promusicae – en ikke-kommerciel sammenslutning af musikproducenter og udgivere af musik og audiovisuelle optagelser – personlige oplysninger om visse personer, som fik leveret internetadgangstjenester gennem Telefónica. Promusicae ønskede at få oplysningerne fremlagt, så organisationen kunne anlægge en civil retssag mod disse personer, som angiveligt anvendte et filudvekslingsprogram, der gav adgang til fonogrammer, som medlemmerne af Promusicae havde udnyttelsesrettighederne til.

Den spanske domstol forelagde sagen for EU-Domstolen og spurgte, om sådanne personoplysninger i henhold til fællesskabsretten skal videregives under en civil retssag med henblik på at sikre den effektive beskyttelse af ophavsretten. Den henviste til direktiv nr. 2000/31/EF, 2001/29/EF og 2004/48/EF set i relation til Chartrets artikel 17 og 47. Domstolen konkluderede, at disse tre direktiver og e-databeskyttelsesdirektivet (direktiv 2002/58/EF) ikke udelukker medlemsstaternes mulighed for at fastsætte pligten til under en civil retssag at videregive personoplysninger med henblik på at sikre den effektive beskyttelse af ophavsretten.

EU-Domstolen påpegede, at sagen derfor rejste spørgsmålet om, hvorledes man opnår den nødvendige forening af kravene, der er forbundet med forskellige grundlæggende rettigheder, nemlig forening af retten til respekt for privatlivets fred med retten til beskyttelse af ejendomsretten og adgang til effektive retsmidler.

Domstolen konkluderede, at det påhviler »medlemsstaterne under gennemførelsen af de ovennævnte direktiver at påse, at de lægger en fortolkning af disse direktiver til grund, som gør det muligt at sikre den rette afvejning af de forskellige grundlæggende rettigheder, der er beskyttet af Fællesskabets retsorden. Under iværksættelsen af foranstaltningerne til gennemførelse af

([125]) *Ibid.*, præmis 54 og 60.

disse direktiver påhviler det herefter ikke blot myndighederne og domstolene i medlemsstaterne at fortolke deres nationale ret på en måde, der er forenelig med de nævnte direktiver, men også at sikre, at de ikke lægger en fortolkning heraf til grund, som kommer i konflikt med disse grundlæggende rettigheder eller med andre almindelige fællesskabsretlige principper, såsom proportionalitetsprincippet« ([126]).

Eksempel: *Bonnier Audio AB m.fl. mod Perfect Communication Sweden AB* ([127]) omhandlede afvejningen mellem intellektuelle ejendomsrettigheder og beskyttelse af personoplysninger. Sagsøgerne, fem forlagsvirksomheder med ejendomsretten til 27 lydbøger, anlagde sag ved den svenske domstol, hvor de påstod, at disse ejendomsrettigheder var overtrådt ved brug af en FTP-server (en filoverførselsprotokol, der muliggør fildeling og dataoverførsel over internettet). Sagsøgerne anmodede internetudbyderen (ISP) om at afsløre navnet og adressen for den person, fra hvis IP-adresse filerne var sendt. ISP'en, ePhone, gjorde indsigelse mod anmodningen, da udbyderen påstod, at den var i strid med direktiv 2006/24/EF (datalagringsdirektivet, erklæret ugyldig i 2014).

Den svenske domstol forelagde sagen for EU-Domstolen og spurgte, om direktiv 2006/24/EF udelukker brugen af en national bestemmelse baseret på artikel 8 i direktiv 2004/48/EF (direktivet om håndhævelse af intellektuelle ejendomsrettigheder), som tillader nedlæggelsen af et påbud om, at ISP'ere overdrager oplysninger til indehavere af ophavsrettigheder omkring abonnenter, hvis IP-adresser angiveligt er blevet brugt i forbindelse med overtrædelser. Spørgsmålet var baseret på en formodning om, at sagsøgeren har fremlagt tydelig dokumentation for overtrædelsen af en bestemt ophavsrettighed, og at foranstaltningen er proportionel.

EU-Domstolen påpegede, at direktiv 2006/24/EF udelukkende omhandlede håndteringen og lagringen af data, som genereres af udbydere af elektroniske kommunikationstjenester med henblik på at undersøge, detektere og forfølge grov kriminalitet, og deres meddelelse til kompetente nationale

([126]) *Ibid.*, præmis 65 og 68. Se også EU-Domstolen, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) mod Netlog NV*, 16. februar 2012.

([127]) EU-Domstolen, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB og Storyside AB mod Perfect Communication Sweden AB*, 19. april 2012.

myndigheder. En national bestemmelse, der gennemfører direktivet om håndhævelse af intellektuelle ejendomsrettigheder, er ikke omfattet af direktiv 2006/24/EF og er derfor ikke udelukket af det direktiv ([128]).

EU-Domstolen fastholdt vedrørende meddelelsen af det pågældende navn og adresse, som sagsøgerne efterspurgte, at en sådan handling er en form for behandling af personoplysninger og er omfattet af direktiv 2002/58/EF (e-databeskyttelsesdirektivet). Den bemærkede også, at meddelelsen af disse data var påkrævet under civile retssager til fordel for, at en indehaver af ophavsrettigheder kan sikre effektiv beskyttelse af ophavsrettigheden, og er derfor ved sit formål omfattet af direktiv 2004/48/EF ([129]).

EU-Domstolen konkluderede, at direktiv 2002/58/EF og 2004/48/EF skal fortolkes som, at de ikke udelukker national lovgivning ligesom den, hovedsagen omhandler, sålænge den lovgivning gør det muligt for en national domstol, som har modtaget en begæring om at afgive kendelse vedrørende meddelelse af personoplysninger, at afveje de pågældende modstridende interesser på baggrund af faktaene i hver sag og under hensyntagen til kravene i proportionalitetsprincippet.

1.3.6. Databeskyttelse og økonomiske interesser

Under den digitale tidsalder eller big data-tidsalderen er data blevet beskrevet som »det nye olie« i forhold til økonomien og stimulering af innovation og kreativitet ([130]). Mange virksomheder har opbygget robuste forretningsmodeller på baggrund af databehandling, og en sådan behandling omfatter ofte personoplysninger. Visse virksomheder kan tro, at visse regler for beskyttelse af personoplysninger i praksis kan resultere i belastende forpligtelser, som kan påvirke deres økonomiske interesser. Spørgsmålet er derfor, om dataansvarliges og databehandleres, eller den brede offentligheds, økonomiske interesser kan begrunde en begrænsning af retten til databeskyttelse.

([128]) *Ibid.*, præmis 40-41.

([129]) *Ibid.*, præmis 52-54. Se også EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU* [GC], 29. januar 2008, præmis 58.

([130]) Se for eksempel *Financial Times* (2016) »Data is the new oil… who's going to own it?«, 16. november 2016.

Eksempel: I sagen *Google Spain* ([131]) fastholdt EU-Domstolen, at fysiske personer under visse omstændigheder har ret til at anmode søgemaskiner om at fjerne søgeresultater fra deres søgeindeks. I sin begrundelse lagde EU-Domstolen vægt på det faktum, at brugen af søgemaskiner og de angivne søgeresultater kan tegne en detaljeret profil af en fysisk person. Disse oplysninger kan omhandle meget af en fysisk persons privatliv og ville være langt sværere at finde eller kæde sammen uden en søgemaskine. Det var derfor et alvorligt indgreb i den registreredes grundlæggende rettigheder til privatliv og beskyttelse af personoplysninger.

EU-Domstolen undersøgte derefter, om indgrebet kunne begrundes. I forbindelse med søgemaskineudbyderens økonomiske interesse i at udføre behandlingen fastlog EU-Domstolen, at »[indgrebet] ikke kan berettiges alene ved søgemaskineudbyderens økonomiske interesse i behandlingen«, og at de grundlæggende rettigheder under Chartrets artikel 7 og 8 »i princippet går forud for ikke blot søgemaskineudbyderens økonomiske interesse, men også for offentlighedens interesse i at finde nævnte oplysning ved en søgning på denne persons navn« ([132]).

En af de vigtigste overvejelser i den europæiske databeskyttelseslovgivning er at give fysiske personer kontrol over deres personoplysninger. I den digitale tidsalder er der navnlig en ulighed mellem de beføjelser, som erhvervsmæssige enheder, der behandler og har adgang til enorme mængder af personoplysninger, har, og de beføjelser, som de fysiske personer, der ejer disse personoplysninger, har til at kontrollere deres egne oplysninger. EU-Domstolen har en individuel tilgang til afvejning af databeskyttelse og økonomiske interesser — såsom tredjemænds interesser i forbindelse med aktieselskaber og selskaber med begrænset ansvar, som illustreret i *Manni*-dommen.

Eksempel: *Manni*-sagen ([133]) omhandlede indførelsen af en fysisk persons personoplysninger i et offentligt handelsregister. Salvatore Manni havde anmodet Camera di Commercio di Lecce om at slette hans personoplysninger fra det pågældende register, efter at han opdagede, at potentielle kunder

([131]) EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014.

([132]) *Ibid.*, præmis 81 og 97.

([133]) EU-Domstolen, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 9. marts 2017.

kiggede i registret og så, at han havde administreret en virksomhed, som gik konkurs for mere end ti år siden. Disse oplysninger afskrækkede hans potentielle kunder og kunne have en negativ virkning på hans kommercielle interesser.

EU-Domstolen blev bedt om at beslutte, om EU-retten anerkendte en ret til sletning i den pågældende sag. I sin konklusion afvejede Domstolen EU's databeskyttelsesregler og Salvatore Mannis kommercielle interesse i at fjerne oplysningerne om hans tidligere selskabs konkurserklæring mod offentlighedens interesse i at have adgang til oplysningerne. Den bemærkede det faktum, at lovgivningen, og navnlig et EU-direktiv, som var rettet mod at gøre selskabsoplysninger mere lettilgængelige for tredjemænd, krævede, at selskaber blev offentliggjort i det offentlige register. Offentliggørelsen var vigtig for at beskytte interesserne for tredjemænd, som kan have lyst til at handle med en bestemt virksomhed, da aktieselskaber og selskaber med begrænset ansvar kun giver tredjemænd selskabsformuen at holde sig til som sikkerhed for fyldestgørelse. Derfor »skal offentlighed gøre det muligt for tredjemand at gøre sig bekendt med de væsentlige dokumenter vedrørende det pågældende selskab samt at få visse oplysninger om dette, navnlig om identiteten af de personer, som har ret til at forpligte selskabet« ([134]).

På baggrund af det legitime mål, som registret havde, fastholdt EU-Domstolen, at Salvatore Manni ikke havde ret til at få sine personoplysninger slettet, da behovet for at beskytte tredjemands interesser over for aktieselskaber og selskaber med begrænset ansvar samt for at sikre retssikkerhed, god handelsskik og dermed et velfungerende indre marked vejede tungere end hans rettigheder under databeskyttelseslovgivningen. Det var navnlig tilfældet på baggrund af det faktum, at fysiske personer, som vælger at deltage i samhandlen igennem et aktieselskab eller selskab med begrænset ansvar, ved, at de er forpligtede til at gøre oplysninger om deres identitet og funktioner offentligt tilgængelige.

EU-Domstolen fandt intet grundlag for at slette oplysningerne i denne sag, men Domstolen anerkendte dog tilstedeværelsen af en ret til at gøre indsigelse mod behandlingen, da den bemærkede, at det ikke kan udelukkes, at: »der kan findes specifikke situationer, i hvilke der foreligger vægtige legitime grunde, der vedrører den registreredes særlige situation, der undtagelsesvis

([134]) *Ibid.*, præmis 49.

berettiger, at aktindsigten i personoplysninger om vedkommende, der er indført i registret, efter udløb af en tilstrækkelig lang tidsfrist [...] begrænses til tredjemænd, som godtgør, at de har en specifik interesse i at foretage søgninger heri« ([135]).

EU-Domstolen fastslog, at det, under hensyntagen til den enkelte persons relevante omstændigheder i den enkelte sag, er op til de nationale domstole at vurdere, om der findes eller ikke findes legitime og vægtige grunde, som undtagelsesvist berettiger, at tredjemænds adgang til personoplysninger i selskabsregistre begrænses. I sagen med Salvatore Manni gjorde Domstolen det dog klart, at det faktum, at offentliggørelsen af hans personoplysninger i registret angiveligt påvirkede hans kundekreds, ikke kunne anses som værende en legitim og vægtig grund. Salvatore Mannis potentielle kunder havde en legitim interesse i oplysninger vedrørende hans tidligere virksomheds konkurserklæring.

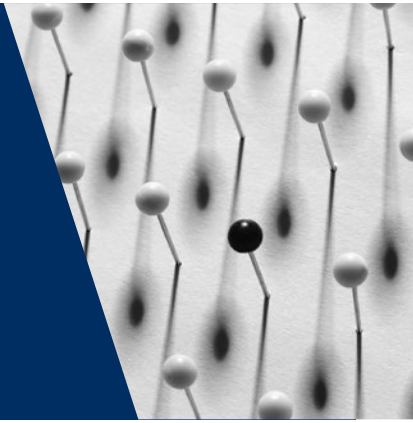
Indgrebet i de grundlæggende rettigheder til respekt for privatliv og beskyttelse af personoplysninger, der er garanteret ved Chartrets artikel 7 og 8, for Salvatore Manni og andre personer, som er optaget i registret, forfulgte et mål af almen interesse og var nødvendigt og proportionelt.

EU-Domstolen fastholdt derfor i *Manni*-sagen, at retten til databeskyttelse og privatliv ikke vejede tungere end tredjemænds interesse i at tilgå oplysninger i selskabsregistret vedrørende aktieselskaber og selskaber med begrænset ansvar.

([135]) *Ibid.*, præmis 60.

2

Databeskyttelses-terminologi



EU	Omhandlede emner	Europarådet
Personoplysninger		
Generel forordning om databeskyttelse, artikel 4, stk. 1 Generel forordning om databeskyttelse, artikel 4, stk. 5, og artikel 5, stk. 1, litra e) Generel forordning om databeskyttelse, artikel 9 EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 2010 EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU* [GC], 2008 EU-Domstolen, C-70/10, *Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 EU-Domstolen, C-582/14, *Patrick Breyer mod Bundesrepublik Deutschland*, 2016 EU-Domstolen, forenede sager C-141/12 og C-372/12, *YS mod Minister voor Immigratie, Integratie en Asiel* og *Minister voor Immigratie, Integratie en Asiel mod M og S*, 2014	Juridisk definition af databeskyttelse	Den moderniserede konvention 108, artikel 2, litra a) EMD, *Bernh Larsen Holding AS m.fl. mod Norge*, nr. 24117/08, 2013 EMD, *Uzun mod Tyskland*, nr. 35623/05, 2010 EMD, *Amann mod Schweiz* [GC], nr. 27798/95, 2000

EU	Omhandlede emner	Europarådet
EU-Domstolen, C-101/01, *Straffesag mod Bodil Lindqvist*, 2003	**Særlige kategorier af personoplysninger (følsomme oplysninger)**	Den moderniserede konvention 108, artikel 6, stk. 1
EU-Domstolen, C-434/16, *Peter Nowak mod Data Protection Commissioner*, 2017	**Anonymiserede og pseudonymiserede personoplysninger**	Den moderniserede konvention 108, artikel 5, stk. 4, litra e) Forklarende rapport til den moderniserede konvention 108, stk. 50
Databehandling		
Generel forordning om databeskyttelse, artikel 4, stk. 2 EU-Domstolen, C-212/13, *František Ryneš mod Úřad pro ochranu osobních údajů*, 2014 EU-Domstolen, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 2017 EU-Domstolen, C-101/01, *Straffesag mod Bodil Lindqvist*, 2003 EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 2014	**Definitioner**	Den moderniserede konvention 108, artikel 2, litra b) og c)
Databrugere		
Generel forordning om databeskyttelse, artikel 4, stk. 7 EU-Domstolen, C-212/13, *František Ryneš mod Úřad pro ochranu osobních údajů*, 2014 EU-Domstolen, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Dataansvarlig**	Den moderniserede konvention 108, artikel 2, litra d) Henstilling om profilering, artikel 1, litra g) (*)
Generel forordning om databeskyttelse, artikel 4, stk. 8	**Databehandler**	Den moderniserede konvention 108, artikel 2, litra f) Henstilling om profilering, artikel 1, litra h)
Generel forordning om databeskyttelse, artikel 4, stk. 9	**Modtager**	Den moderniserede konvention 108, artikel 2, litra e)
Generel forordning om databeskyttelse, artikel 4, stk. 10	**Tredjemand**	

EU	Omhandlede emner	Europarådet
Samtykke		
Generel forordning om databeskyttelse, artikel 4, stk. 11, og artikel 7 EU-Domstolen, C-543/09, *Deutsche Telekom AG mod Bundesrepublik Deutschland*, 2011 EU-Domstolen, C-536/15, *Tele2 (Netherlands) BV m.fl. mod Autoriteit Consument en Markt (ACM)*, 2017	Definition og krav for gyldigt samtykke	Den moderniserede konvention 108, artikel 5, stk. 2 Henstilling om medicinske oplysninger, artikel 6, og diverse efterfølgende henstillinger EMD, *Elberte mod Letland*, nr. 61243/08, 2015

Bemærk: (*) Europarådet, Ministerudvalget (2010), Henstilling CM/Rec(2010)13 til medlemsstaterne om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, for så vidt angår profilering (henstilling om profilering), 23. november 2010.

2.1. Personoplysninger

Hovedpunkter

- Oplysninger er personoplysninger, hvis de vedrører en identificeret eller identificerbar fysisk person (»den registrerede«).
- Ved vurdering af, om en fysisk person er identificerbar, bør en dataansvarlig eller en anden person tage alle midler i betragtning, som med rimelighed tages i anvendelse (såsom udpegning) til direkte eller indirekte identifikation af den fysiske person.
- Ved autentifikation bevises det, at en bestemt person besidder en bestemt identitet og/eller er bemyndiget til at udføre visse aktiviteter.
- Der er særlige kategorier af oplysninger, såkaldte følsomme oplysninger, som er anført i konvention 108 og EU's databeskyttelseslovgivning, der kræver øget beskyttelse og derfor er underlagt særlige regler.
- Oplysninger er anonymiserede, hvis de ikke længere peger på en identificeret eller identificerbar enkeltperson.
- Pseudonymisering er en foranstaltning, hvor personoplysninger ikke kan knyttes til den registrerede uden yderligere oplysninger, som opbevares separat. »Nøglen«, som muliggør genkendelse af de registrerede, skal lagres separat og sikkert. Oplysninger, der har gennemgået en pseudonymiseringsproces, er stadig personoplysninger. EU-retten har intet begreb for »pseudonymiserede oplysninger«.
- Principper og regler for databeskyttelse finder ikke anvendelse for anonymiserede oplysninger. De finder dog anvendelse for pseudonymiserede oplysninger.

2.1.1. De vigtigste aspekter af begrebet personoplysninger

I både **EU-retten** og **Europarådets** retsorden defineres »personoplysninger« som information om en identificeret eller identificerbar fysisk person ([136]). Det omhandler information om en person, hvis identitet umiddelbart fremgår eller kan fastslås ved at indhente yderligere oplysninger. For at afgøre, om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende ([137]).

Hvis oplysninger om en sådan person behandles, kaldes denne person »den registrerede«.

Den registrerede

I EU-retten er der kun fastsat regler om databeskyttelse for fysiske personer ([138]), og den europæiske databeskyttelseslovgivning beskytter kun levende mennesker ([139]). Den generelle forordning om databeskyttelse (GDPR) definerer personoplysninger som alle oplysninger, der vedrører en identificeret eller identificerbar person.

Europarådets retsorden, navnlig den moderniserede konvention 108, henviser også til beskyttelsen af enkelte mennesker i forbindelse med behandling af deres personoplysninger. I den sammenhæng betyder personoplysninger alle oplysninger, som kan henføres til en identificeret eller identificerbar person. Denne fysiske person eller det enkelte menneske, som angivet i henholdsvis GDPR og den moderniserede konvention 108, kaldes for den registrerede inden for databeskyttelseslovgivningen.

Juridiske personer har også en vis beskyttelse. Der findes EMD-retspraksis med domsafsigelser vedrørende begæringer fra juridiske personer, der påstår, at deres ret til beskyttelse mod misbrug af deres data omhandlet i artikel 8 i EMRK er krænket. Artikel 8 i EMRK omfatter både retten til respekt for privatliv og familieliv samt

([136]) Generel forordning om databeskyttelse, artikel 4, stk. 1, og den moderniserede konvention 108, artikel 2, litra a).

([137]) Generel forordning om databeskyttelse, betragtning 26.

([138]) *Ibid.*, artikel 1.

([139]) *Ibid.*, betragtning 27. Se også Artikel 29-Gruppen (2007), *Udtalelse 4/2007 om begrebet personoplysninger*, WP 136, 20. juni 2007, s. 22.

for hjem og korrespondance. Domstolen kan derfor undersøge sager med udgangspunkt i sidstnævnte i stedet for privatliv.

Eksempel: *Bernh Larsen Holding AS m.fl. mod Norge* ([140]) vedrørte en klage indgivet af tre norske selskaber over en beslutning truffet af skattemyndighederne, som pålagde dem at udlevere en kopi af alle data på en computerserver, som de tre brugte i fællesskab, til skatterevisorerne.

EMD fandt, at et sådant krav mod de sagsøgende selskaber udgjorde et indgreb i deres ret til respekt for »hjem« og »korrespondance«, for så vidt angår artikel 8 i EMRK. Domstolen fandt dog, at skattemyndighederne havde effektive og tilstrækkelige garantier mod misbrug. De sagsøgende selskaber var på forhånd blevet underrettet i god tid, de var til stede og kunne fremsætte indvendinger under indgrebet på stedet, og materialet skulle destrueres, når skattekontrollen var afsluttet. Under disse omstændigheder havde man sikret en rimelig balance mellem de sagsøgende selskabers ret til respekt for »hjem« og »korrespondance« og deres interesse i at beskytte privatlivets fred for deres medarbejdere på den ene side og den samfundsmæssige interesse i at sikre effektiv skattekontrol på den anden. Domstolen fastslog, at artikel 8 ikke var blevet overtrådt.

I henhold til den moderniserede konvention 108 vedrører databeskyttelse primært beskyttelsen af fysiske personer. Kontraherende parter kan dog udvide databeskyttelsen til juridiske personer, f.eks. erhvervsvirksomheder og foreninger, i deres nationale lovgivning. Den forklarende rapport til den moderniserede konvention fastlægger, at national lovgivning kan beskytte juridiske personers legitime interesser ved at udvide konventionens omfang til sådanne aktører ([141]). **EU's databeskyttelseslovgivning** finder ikke anvendelse for behandling af personoplysninger, der vedrører juridiske personer, og navnlig virksomheder, der er etableret som juridiske personer, herunder den juridiske persons navn, form og kontaktoplysninger ([142]). E-databeskyttelsesdirektivet beskytter dog fortroligheden af juridiske personers kommunikationer og legitime interesser, navnlig mod den voksende risiko, der er forbundet med automatiseret opbevaring og behandling af

([140]) EMD, *Bernh Larsen Holding AS m.fl. mod Norge*, nr. 24117/08, 14. marts 2013. Se dog også EMD, *Liberty m.fl. mod Det Forenede Kongerige*, nr. 58243/00, 1. juli 2008.

([141]) Forklarende rapport til den moderniserede konvention 108, stk. 30.

([142]) Den generelle forordning om databeskyttelse, betragtning 14.

oplysninger om abonnenter og brugere ([143]). På tilsvarende vis udvider udkastet til e-databeskyttelsesforordningen beskyttelsen til at omfatte juridiske personer.

Eksempel: I sagen *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* ([144]) fastslog EU-Domstolen med henvisning til offentliggørelsen af personoplysninger vedrørende modtagere af landbrugsstøtte, at juridiske personer med hensyn til en sådan identifikation kun kan »påberåbe sig beskyttelsen i chartrets artikel 7 og 8, for så vidt som den juridiske persons fulde navn identificerer en eller flere fysiske personer. [...R]etten til respekt for privatlivet med hensyn til behandling af personoplysninger, som anerkendt i chartrets artikel 7 og 8, henviser til enhver form for information om en identificeret eller identificerbar fysisk person [...]« ([145]).

Efter en afvejning af EU's interesser i at sikre gennemsigtighed under fordeling af støtte på den ene side og de grundlæggende rettigheder til privatliv og databeskyttelse for de enkeltpersoner, som modtog støtten, på den anden side vurderede EU-Domstolen, at indgrebet i de grundlæggende rettigheder var uforholdsmæssigt. Den vurderede, at målet om gennemsigtighed kunne være nået på effektiv vis via foranstaltninger, som var mindre krænkende for de pågældende enkeltpersoners rettigheder. I løbet af undersøgelsen af proportionaliteten af at offentliggøre oplysninger omkring juridiske personer, som modtog støtte, drog EU-Domstolen dog en anden konklusion, hvor den fastslog, at en sådan offentliggørelse ikke overskrider proportionalitetsprincippets grænser. Den udtalte, at alvorligheden »af et indgreb i retten til beskyttelse af personoplysninger er nemlig ikke ens for juridiske og fysiske personer« ([146]). Juridiske personer var underlagt en øget forpligtelse til at offentliggøre deres oplysninger. EU-Domstolen vurderede, at en forpligtelse for de nationale myndigheder til for hver juridisk person, der modtager midler, inden offentliggørelsen af de omhandlede oplysninger at undersøge, om den juridiske persons oplysninger identificerer en fysisk person, ville pålægge disse myndigheder en uforholdsmæssigt stor administrativ

([143]) E-databeskyttelsesdirektivet, betragtning 7, og artikel 1, stk. 2.

([144]) EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 9. november 2010, præmis 53.

([145]) *Ibid.*, præmis 52-53.

([146]) *Ibid.*, præmis 87.

byrde. Lovgivningen, som kræver en generel offentliggørelse af oplysninger vedrørende juridiske personer, havde derfor foretaget en korrekt afvejning mellem de forskellige foreliggende interesser.

Karakteren af personoplysninger

Enhver form for information kan være personoplysninger, hvis den vedrører en identificeret eller identificerbar person.

Eksempel: En overordnets vurdering af en medarbejders indsats, som er lagret i medarbejderens dossier, er personoplysninger om medarbejderen. Dette er selv om den kun helt eller delvist afspejler den overordnedes personlige holdning, som f.eks: »medarbejderen er ikke engageret i sit arbejde«, og ikke konkrete kendsgerninger, som f.eks: »medarbejderen har været fraværende i fem uger i løbet af de sidste seks måneder«.

Personoplysninger dækker information vedrørende en persons privatliv og information om den pågældendes erhvervsmæssige eller offentlige liv.

I *Amann*-sagen ([147]) fortolkede EMD udtrykket »personoplysninger« som ikke værende begrænset til forhold inden for en persons privatsfære. Denne betydning af udtrykket »personoplysninger« er også relevant for GDPR.

Eksempel: I sagen *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* ([148]) fastslog EU-Domstolen, at det i denne forbindelse er »uden betydning, at de offentliggjorte oplysninger vedrører erhvervsmæssig virksomhed […]. Den Europæiske Menneskerettighedsdomstol har i den forbindelse vedrørende fortolkningen af artikel 8 i EMRK fastslået, at udtrykket »privatlivet« ikke skal fortolkes indskrænkende, og at »der i princippet ikke er nogen grund til, at erhvervsmæssig virksomhed […] skulle være udelukket fra begrebet »privatlivet««.«

([147]) Se EMD, *Amann mod Schweiz*, nr. 27798/95, 16. februar 2000, præmis 65.

([148]) EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 9. november 2010, præmis 59.

Eksempel: I de forenede sager *YS mod Minister voor Immigratie, Integratie en Asiel* og *Minister voor Immigratie, Integratie en Asiel mod M og S* ([149]) fastlog EU-Domstolen, at den juridiske analyse i et udkast til afgørelse fra afdelingen for indvandring og indfødsret, som håndterer ansøgninger om opholdstilladelse, ikke alene udgør personoplysninger, selvom den kan indeholde personoplysninger.

EMD's retspraksis vedrørende EMRK's artikel 8 bekræfter, at det kan være vanskeligt at adskille private og erhvervsmæssige forhold ([150]).

Eksempel: I sagen *Bărbulescu mod Rumænien* ([151]) var sagsøgeren blevet afskediget for at bruge sin arbejdsgivers internet i arbejdstiden i strid med interne regler. Hans arbejdsgiver havde overvåget hans kommunikationer og registre, som var udarbejdet under den nationale retssag, med meddelelser udelukkende af privat karakter. Da EMD mente, at artikel 8 var gældende, efterlod det spørgsmålet om, hvorvidt arbejdsgiverens restriktive regler gav sagsøgeren en rimelig beskyttelse af privatlivets fred, ubesvaret, men domstolen konkluderede overordnet, at en arbejdsgivers anvisninger ikke kunne reducere en persons private socialliv til ingenting på arbejdspladsen. Hvad angår sagens grundlag, var det nødvendigt at tildele kontraherende stater brede muligheder for skøn ved vurdering af behovet for at fastlægge lovrammer for de betingelser, som en arbejdsgiver kan regulere sine arbejdstageres ikke-erhvervsmæssige kommunikationer – elektroniske eller andre former – under på arbejdspladsen. De nationale myndigheder skulle dog stadig sikre, at en arbejdsgivers foranstaltninger for overvågning af korrespondance og andre kommunikationer, uanset omfanget og varigheden af sådanne foranstaltninger, blev indført sammen med passende og tilstrækkelige garantier mod misbrug. Proportionalitet og proceduremæssige garantier mod vilkårlig behandling var nødvendige, og EMD udpegede en række faktorer, som var relevante i de pågældende omstændigheder. Eksempler på sådanne faktorer var: omfanget af arbejdsgiverens overvågning af arbejdstagere, graden af indblanding i arbejdstagerens privatliv, konsekvenserne for arbejdstageren og hvorvidt tilstrækkelige garantier var fastlagt. Derudover skulle nationale

([149]) EU-Domstolen, forenede sager C-141/12 og C-372/12, *YS mod Minister voor Immigratie, Integratie en Asiel* og *Minister voor Immigratie, Integratie en Asiel mod M og S*, 17. juli 2014, præmis 39.

([150]) Se for eksempel EMD, *Rotaru mod Rumænien* [GC], nr. 28341/95, 4. maj 2000, præmis 43; EMD, *Niemietz mod Tyskland*, nr. 13710/88, 16. december 1992, præmis 29.

([151]) EMD, *Bărbulescu mod Rumænien* [GC], nr. 61496/08, 5. september 2017, præmis 121.

myndigheder sikre, at en arbejdstager, hvis kommunikationer var blevet overvåget, havde adgang til retsmidler hos en retsinstans med kompetence til at bestemme, i realiteten som minimum, hvordan de pågældende kriterier skulle overholdes, og om de anfægtede foranstaltninger var lovlige. I denne sag konstaterede EMD, at artikel 8 var blevet overtrådt, da de nationale myndigheder ikke havde beskyttet sagsøgerens ret til respekt for hans privatliv og korrespondance i tilstrækkelig grad og dermed ikke havde sikret en rimelig balance mellem de foreliggende interesser.

I henhold til EU-retten samt **Europarådets retsorden** indeholder information oplysninger om en person:

- hvis en enkeltperson identificeres i den pågældende information, eller
- hvis en enkeltperson ikke er identificeret, men er beskrevet i denne information på en måde, som gør det muligt at finde frem til, hvem den registrerede er, ved at udføre yderligere undersøgelser.

Begge typer information er beskyttet på samme måde i den europæiske databeskyttelseslovgivning. Enkeltpersoners direkte eller indirekte identificerbarhed kræver løbende vurdering »under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling« ([152]). EMD har gentagne gange udtalt, at begrebet »personoplysninger« ifølge EMRK er det samme som i konvention 108, især for så vidt angår betingelsen vedrørende identificerede eller identificerbare personer ([153]).

GDPR fastlægger, at en person er identificerbar, hvis vedkommende »direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet« ([154]). Identifikation kræver naturligvis elementer, som beskriver en person på en sådan måde, at han eller hun kan skelnes fra alle andre personer og kan genkendes som individ. En persons navn er det mest indlysende eksempel på sådanne beskrivende elementer og kan direkte identificere en person. Undtagelsesvis kan andre identifikatorer have samme

([152]) Generel forordning om databeskyttelse, betragtning 26.

([153]) Se EMD, *Amann mod Schweiz* [GC], nr. 27798/95, 16. februar 2000, præmis 65.

([154]) Generel forordning om databeskyttelse, artikel 4, stk. 1.

virkning som et navn og gøre det muligt at identificere en person indirekte. Et telefonnummer, socialsikringsnummer og køretøjsregistreringsnummer er alle eksempler på oplysninger, der kan gøre en enkeltperson identificerbar. Det er også muligt at benytte identifikatorer — såsom elektroniske registre, cookies og værktøjer til overvågning af webtrafik — til at identificere enkeltpersoner ud fra deres adfærd og vaner. Som forklaret i udtalelsen fra Artikel 29-Gruppen: »Uden overhovedet at spørge om personens navn og adresse er det muligt at kategorisere den pågældende på grundlag af socioøkonomiske, psykologiske, filosofiske eller andre kriterier og tillægge den pågældende visse beslutninger, da vedkommendes kontaktpunkt (en computer) ikke længere nødvendigvis kræver, at vedkommendes identitet i snæver forstand afsløres« ([155]). Europarådets og EU's definition af personoplysninger er bred nok til at omfatte alle identifikationsmuligheder (og dermed alle grader af identificerbarhed).

Eksempel: I sagen *Promusicae mod Telefónica de España* ([156]) fremførte EU-Domstolen, at det er »ubestridt, at den kommunikation, som Promusicae har anmodet om — navne og adresser på visse brugere af [en bestemt internetbaseret fildelingsplatform] – indebærer videregivelsen af personlysninger, hvilket i henhold til definitionen i artikel 2, litra a), i direktiv 95/46/EF [i øjeblikket artikel 4, stk. 1, i GDPR] betyder information om en identificeret eller identificerbar fysisk person. Denne videregivelse af oplysninger, som ifølge Promusicae lagres af Telefónica — hvilket selskabet ikke bestrider – udgør en behandling af personoplysninger« ([157]).

Eksempel: *Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* ([158]) handlede om, at internetudbyderen, Scarlet, afviste at installere et system til at filtrere elektroniske kommunikationer, som benytter fildelingssoftware, til at forhindre fildeling, som overtræder ejendomsrettigheder beskyttet af SABAM, som er et administrationsselskab, der repræsenterer forfattere, komponister og redaktører. EU-Domstolen fastslog, at brugeres IP-adresser er »beskyttede personoplysninger, fordi de gør det muligt præcist at identificere de nævnte brugere«.

([155]) Artikel 29-Gruppen, *Udtalelse 4/2007 om begrebet personoplysninger*, WP 136, 20. juni 2007, s. 15.

([156]) EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU* [GC], 29. januar 2008, præmis 45.

([157]) Det tidligere direktiv 95/46/EF, artikel 2, litra b), som nu er den generelle forordning om databeskyttelse, artikel 4, stk. 2.

([158]) EU-Domstolen, C-70/10, *Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. november 2011, præmis 51.

Da mange navne ikke er unikke, kræves der i nogle tilfælde yderligere identifikatorer for at sikre, at en person ikke forveksles med en anden. Nogle gange skal direkte og indirekte identifikatorer kombineres for at identificere den enkeltperson, som oplysningerne omhandler. Ofte anvendes fødselsdato og -sted. Nogle lande har desuden indført personnumre for bedre at kunne skelne mellem borgerne. Overførte skatteoplysninger ([159]), oplysninger vedrørende en ansøger om opholdstilladelse i et administrativt dokument ([160]) og dokumenter vedrørende bank- og forvaltningsmæssige forhold ([161]) kan være personoplysninger. Biometriske data, som f.eks. fingeraftryk, digitale fotos eller irisscanninger, og lokaliseringsdata og onlineidentifikatorer anvendes i stigende grad til at identificere personer i den teknologiske tidsalder.

Med hensyn til anvendelsesområdet for den europæiske databeskyttelseslovgivning er der dog ikke behov for faktisk identifikation af den registrerede. Det er nok, at den pågældende person er identificerbar. En person anses for at være identificerbar, hvis information indeholder identifikationselementer, som gør det muligt at identificere personen direkte eller indirekte ([162]). I henhold til GDPR's betragtning 26 er det afgørende, om rimelige midler til identifikation er tilgængelige og anvendes af de forventede brugere af informationen. Dette inkluderer information i tredjeparts-modtageres besiddelse (se afsnit 2.3.2.).

Eksempel: En lokal myndighed beslutter at indsamle data om biler, der kører for stærkt i lokalområdet. Den fotograferer bilerne og registrerer automatisk tid og sted med det formål at videregive oplysningerne til den kompetente myndighed, således at den kan udstede bøder til dem, der har overtrådt hastighedsgrænserne. En registreret indgiver en klage med påstand om, at den lokale myndighed ikke har retsgrundlag i databeskyttelseslovgivningen til at indsamle sådanne data. Den lokale myndighed fastholder, at den ikke indsamler personoplysninger. Den siger, at nummerplader er anonyme. Den lokale myndighed har ikke beføjelse til at få adgang til motorkøretøjsregistret for at finde frem til bilejerens eller førerens identitet.

([159]) EU-Domstolen, C-201/14, *Smaranda Bara m.fl. mod Casa Națională de Asigurări de Sănătate m.fl.*, 1. oktober 2015.

([160]) EU-Domstolen, forenede sager C-141/12 og C-372/12, *YS mod Minister voor Immigratie, Integratie en Asiel* og *Minister voor Immigratie, Integratie en Asiel mod M og S*, 17. juli 2014.

([161]) EMD, *M.N. m.fl. mod San Marino*, nr. 28005/12, 7. juli 2015.

([162]) Generel forordning om databeskyttelse, artikel 4, stk. 1.

Denne argumentation er ikke i overensstemmelse med GDPR's betragtning 26. Eftersom formålet med dataindsamlingen utvivlsomt er at identificere og udstede bøder til bilister, der overtræder hastighedsgrænsen, må det forventes, at identifikation vil blive forsøgt. Selv om de lokale myndigheder ikke direkte råder over et hjælpemiddel til identifikation, vil de videregive oplysningerne til den kompetente myndighed, politiet, som råder over sådanne hjælpemidler. Betragtning 26 omfatter også udtrykkeligt den situation, hvor det må forventes, at yderligere modtagere af oplysningerne end den umiddelbare databruger kan forsøge at identificere den pågældende person. På baggrund af betragtning 26 svarer den lokale myndigheds foranstaltning til at indsamle oplysninger om identificerbare personer og kræver derfor et retsgrundlag i henhold til databeskyttelseslovgivningen.

»For at fastslå, om midler med rimelighed kan tænkes bragt i anvendelse til at identificere en fysisk person, bør alle objektive forhold tages i betragtning, såsom omkostninger ved og tid der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling« ([163]).

Eksempel: I sagen *Breyer mod Bundesrepublik Deutschland* ([164]) undersøgte EU-Domstolen registreredes indirekte identificerbarhed. Sagen omhandlede dynamiske IP-adresser, som ændrer sig hver gang, der skabes forbindelse til internettet på ny. Websteder, som drives af tyske forbundsinstitutter, registrerede og lagrede dynamiske IP-adresser for at forhindre cyberangreb og indlede straffesager, om nødvendigt. Kun den internetudbyder, som Patrick Breyer benyttede, havde de yderligere oplysninger, der var nødvendige til at identificere ham.

EU-Domstolen vurderede, at en dynamisk IP-adresse, som en udbyder af online-medietjenester registrerer, når en person går ind på et websted, som udbyderen har gjort offentligt tilgængelig, udgør personoplysninger, hvor kun en tredjemand – i dette tilfælde internetudbyderen – besidder de yderligere

([163]) *Ibid.*, betragtning 26.

([164]) EU-Domstolen, C-582/14, *Patrick Breyer mod Bundesrepublik Deutschland*, 19. oktober 2016, præmis 43.

oplysninger, som er nødvendige til at identificere personen ([165]). Den fastholdt, at det »ikke er påkrævet, at alle de oplysninger, der gør det muligt at identificere den registrerede, skal befinde sig hos en enkelt person«, for at oplysninger udgør personoplysninger. Brugere af dynamiske IP-adresser registreret af en internetudbyder kan under nogle omstændigheder identificeres, for eksempel inden for rammerne af straffesager i tilfælde af cyberangreb, med hjælp fra andre personer ([166]). I henhold til EU-Domstolen, »når udbyderen råder over lovlige hjælpemidler, der gør det muligt for denne at få identificeret den registrerede gennem den yderligere viden, som denne persons internetudbyder råder over«, udgør dette midler, som med sandsynlighed benyttes til at identificere den registrerede. Sådanne oplysninger anses derfor som værende personoplysninger.

I henhold til Europarådets retsorden skal identificerbarhed forstås på en lignende måde. Den forklarende rapport til den moderniserede konvention 108 indeholder en lignende beskrivelse: Begrebet »identificerbar« henviser ikke kun som sådan til den enkelte persons civile eller juridiske identitet, men også til det, som gør, at én person »individualiseres« eller udvælges fremfor andre og som følge heraf potentielt behandles anderledes. Denne »individualisering« kunne for eksempel foregå ved at henvise til ham eller hende specifikt eller til en enhed eller en kombination af enheder (computer, mobiltelefon, kamera, spilleudstyr osv.) knyttet til et identifikationsnummer, et pseudonym, biometrisk eller genetisk data, lokaliseringsdata, en IP-adresse eller en anden identifikator ([167]). En enkeltperson betragtes ikke som »identificerbar«, hvis dennes identifikation kræver en uforholdsmæssig mængde tid, arbejde elle ressourcer. Det er for eksempel tilfældet, når identifikation af en registreret ville kræve unødigt komplekse, lange og dyre operationer. Der skal i den enkelte sag vurderes, om tiden, arbejdet eller ressourcerne er urimelige, under hensyntagen til faktorer, såsom formålet med behandlingen, identifikationens omkostninger og fordele, den dataansvarliges type og den brugte teknologi ([168]).

Det er vigtigt at bemærke, at formen, hvorpå personoplysningerne lagres eller anvendes, ikke er relevant for anvendelsen af databeskyttelseslovgivningen.

([165]) Europa-Parlamentets og Rådets tidligere direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, artikel 2, litra a).

([166]) EU-Domstolen, C-70/10, *Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. november 2011, præmis 47-48.

([167]) Forklarende rapport til den moderniserede konvention 108, stk. 18.

([168]) *Ibid*., stk. 17.

Skriftlig eller mundtlig kommunikation kan indeholde personoplysninger, og det samme gælder billeder ([169]), herunder kameraovervågning ([170]), eller lyd ([171]). Elektronisk registrerede oplysninger og oplysninger på papir kan også være personoplysninger. Selv celleprøver af menneskeligt væv – som registrerer en persons DNA – kan være kilder til biometriske data ([172]), sålænge dataene omhandler personens arvede eller erhvervede genetiske karakteristika, som giver entydig information om den fysiske persons fysiologi eller helbred, og som navnlig foreligger efter en analyse af en biologisk prøve fra den pågældende fysiske person ([173]).

Anonymisering

I medfør af princippet om opbevaringsbegrænsning beskrevet i både GDPR og den moderniserede konvention 108 (diskuteret i yderligere detaljer i kapitel 3) skal data »opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles« ([174]). Som følge heraf skal data slettes eller anonymiseres, hvis en dataansvarlig ønsker at opbevare dem, efter der ikke længere er behov for dem, og de ikke længere opfylder deres oprindelige formål.

Proceduren for anonymisering af data betyder, at alle identificerende elementer fjernes fra et sæt personoplysninger, så den registrerede ikke længere kan identificeres ([175]). I sin udtalelse 05/2014 analyserede Artikel 29-Gruppen effektiviteten og grænserne for forskellige anonymiseringsteknikker ([176]). Den anerkender den potentielle værdi af sådanne teknikker, men understreger, at visse teknikker ikke nødvendigvis fungerer i alle tilfælde. Den optimale løsning i en bestemt situation

([169]) EMD, *Von Hannover mod Tyskland*, nr. 59320/00, 24. juni 2004; EMD, *Sciacca mod Italien*, nr. 50774/99, 11. januar 2005; EU-Domstolen, C-212/13, *František Ryneš mod Úřad pro ochranu osobních údajů*, 11. december 2014.

([170]) EMD, *Peck mod Det Forenede Kongerige*, nr. 44647/98, 28. januar 2003; EMD, *Köpke mod Tyskland* (dec.), nr. 420/07, 5. oktober 2010; EDPS (2010), *The EDPS video-surveillance guidelines*, 17. marts 2010.

([171]) EMD, *P.G. og J.H. mod Det Forenede Kongerige*, nr. 44787/98, 25. september 2001, præmis 59-60; EMD, *Wisse mod Frankrig*, nr. 71611/01, 20. december 2005 (fransksproget udgave).

([172]) Se Artikel 29-Gruppen (2007), *Udtalelse 4/2007 om begrebet personoplysninger*, WP136, 20. juni 2007, s. 9; Europarådet, Henstilling nr. Rec(2006) 4 fra Ministerkomitéen til medlemsstaterne om forskning i biologiske materialer af menneskelig oprindelse, 15. marts 2006.

([173]) Generel forordning om databeskyttelse, artikel 4, stk. 13.

([174]) *Ibid.*, artikel 5, stk. 1, litra e); den moderniserede konvention 108, artikel 5, stk. 4, litra e).

([175]) Generel forordning om databeskyttelse, betragtning 26.

([176]) Artikel 29-Gruppen (2014), *Udtalelse 05/2014 om anonymiseringsteknikker*, WP 216, 10. april 2014.

findes ved at vælge den passende anonymiseringsproces ud fra den enkelte sag. Uanset den anvendte teknik skal identifikation uigenkaldeligt forhindres. Dette betyder, at der ikke må være noget element i oplysningerne, som med rimelige bestræbelser kan identificere den/de pågældende person/personer igen, for at data er anonyme ([177]). Risikoen for genidentifikation kan vurderes ved at tage hensyn til den tid, det arbejde eller de ressourcer, som er nødvendige grundet dataenes art, konteksten for deres brug, tilgængelige teknologier til genidentifikation og tilknyttede omkostninger ([178]).

Når data anonymiseres korrekt, er det ikke længere personoplysninger, og databeskyttelseslovgivningen finder ikke længere anvendelse.

GDPR fastsætter, at den person eller organisation, som kontrollerer behandlingen af personoplysninger, ikke er forpligtet til at beholde, indhente eller behandle yderligere oplysninger for at kunne identificere den registrerede alene med det formål at overholde forordningen. Denne regel har dog en væsentlig undtagelse: Når den registrerede med henblik på at udøve deres ret til indsigt, berigtigelse, sletning, begrænsning af behandling og dataportabilitet giver yderligere oplysninger til den dataansvarlige, der gør det muligt at identificere den pågældende, så bliver de oplysninger, som blev anonymiseret tidligere, til personoplysninger igen ([179]).

Pseudonymisering

Personoplysninger indeholder identifikatorer, som f.eks. navn, fødselsdato, køn, adresse eller andre elementer, der kan føre til identifikation. Processen med pseudonymisering af personoplysninger betyder, at disse identifikatorer erstattes af et pseudonym.

EU-retten definerer pseudonymisering som »behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en

([177]) Generel forordning om databeskyttelse, betragtning 26.

([178]) Europarådet, det rådgivende udvalg for konvention 108 (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. januar 2017, stk. 6.2.

([179]) Generel forordning om databeskyttelse, artikel 11.

identificeret eller identificerbar fysisk person« ([180]). I modsætning til anonymiserede oplysninger er pseudonymiserede oplysninger stadig personoplysninger og er derfor underlagt databeskyttelseslovgivningen. Selvom pseudonymisering kan reducere sikkerhedsrisici for de registrerede, er det stadig omfattet af GDPR.

GDPR anerkender forskellige anvendelser af pseudonymisering som en passende teknisk foranstaltning til at forstærke databeskyttelse, og den fremhæves især for designet og sikkerheden af dens databehandling ([181]). Det er også en passende foranstaltning, der kan benyttes til at behandle personoplysninger til andre formål end dem, som de oprindeligt blev indsamlet til ([182]).

Pseudonymisering er ikke udtrykkeligt nævnt i de juridiske definitioner i **Europarådets** moderniserede konvention 108. Den forklarende rapport til den moderniserede konvention 108 fastlægger dog tydeligt, at brugen af et pseudonym eller en anden digital identifikator/digital identitet ikke fører til anonymisering af oplysningerne, da den registrerede stadig kan identificeres eller individualiseres ([183]). Datakryptering er én måde at pseudonymisere oplysninger på. Når data er pseudonymiseret, findes forbindelsen til en identitet i form af pseudonymet plus en krypteringsnøgle. Uden en sådan nøgle er det vanskeligt at identificere pseudonymiserede oplysninger. Genidentifikation er let for alle, der har ret til at anvende krypteringsnøglen. Det skal især sikres, at krypteringsnøgler kun kan anvendes af bemyndigede personer. Pseudonymiserede oplysninger skal derfor anses som værende personoplysninger, der er underlagt den moderniserede konvention 108 ([184]).

Autentifikation

Dette er en procedure, hvorved en person kan dokumentere, at han eller hun har en bestemt identitet og/eller har bemyndigelse til at gøre bestemte ting, som f.eks. at gå ind i et sikkerhedsområde eller hæve penge fra en bankkonto. Autentifikation kan opnås ved at sammenligne biometriske data, f.eks. et foto eller fingeraftryk i et pas, med dataene for den person, der præsenterer sig, f.eks. ved immigrationskontrollen ([185]), ved at anmode om oplysninger, der kun bør kendes af personen med en bestemt identitet eller bemyndigelse, f.eks. et personligt identifikationsnummer

([180]) *Ibid.*, artikel 4, stk. 5.

([181]) *Ibid.*, artikel 25, stk. 1.

([182]) *Ibid.*, artikel 6, stk. 4.

([183]) Forklarende rapport til den moderniserede konvention 108, stk. 18.

([184]) *Ibid.*

([185]) *Ibid.*, stk. 56-57.

(PIN-kode) eller en adgangskode, eller ved at kræve, at der fremlægges en bestemt token, som kun personen med en bestemt identitet eller bemyndigelse bør være i besiddelse af, f.eks. et specielt chipkort eller nøglen til en bankboks. Bortset fra adgangskoder eller chipkort, evt. kombineret med PIN-koder, er elektroniske signaturer et instrument, der kan identificere og autentificere en person i forbindelse med elektronisk kommunikation.

2.1.2. Særlige kategorier af personoplysninger

I henhold til EU-retten samt **Europarådets retsorden** er der særlige kategorier af personoplysninger, som i sig selv kan udgøre en risiko for de registrerede, når de behandles, og derfor kræver øget beskyttelse. Sådanne oplysninger er underlagt et forbudsprincip, og behandling heraf tillades kun under et begrænset antal betingelser.

Inden for rammerne af den moderniserede konvention 108, artikel 6, og GDPR, artikel 9, betragtes følgende kategorier som følsomme oplysninger:

- personoplysninger om racemæssig eller etnisk baggrund
- personoplysninger om politisk, religiøs eller andre overbevisninger, herunder filosofiske overbevisninger
- personoplysninger, der afslører et medlemskab af en fagforening
- genetiske og biometriske oplysninger, der behandles med henblik på at identificere en person
- oplysninger om helbredsforhold og seksuelle forhold.

Eksempel: Sagen *Bodil Lindqvist* ([186]) omhandlede henvisninger til forskellige personer ud fra navn eller andet, såsom deres telefonnummer eller oplysninger om deres fritidsinteresser, på en internetside. EU-Domstolen tilkendegav, at »angivelsen af den omstændighed, at en person har beskadiget sin fod og er delvis sygemeldt, udgør en personoplysning om helbredsforhold« ([187]).

([186]) EU-Domstolen, C-101/01, *Straffesag mod Bodil Lindqvist*, 6. november 2003, præmis 51.

([187]) Det tidligere direktiv 95/46/EF, artikel 8, stk. 1, som nu er den generelle forordning om databeskyttelse, artikel 9, stk. 1.

Personoplysninger om straffedomme og lovovertrædelser

Den moderniserede konvention 108 omfatter personoplysninger, der omhandler lovovertrædelser, straffesager og -domme, og relaterede sikkerhedsforanstaltninger i listen over særlige kategorier for personoplysninger ([188]). Under GDPR's rammer er personoplysninger vedrørende straffedomme og lovovertrædelser eller relaterede sikkerhedsforanstaltninger ikke anført som sådan i listen over særlige kategorier af oplysninger, men de behandles i en særskilt artikel. Artikel 10 i GDPR fastlægger, at behandling af sådanne oplysninger kun må foretages »under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder«. Omfattende registre med oplysninger om straffedomme må på den anden side kun kontrolleres af særlige offentlige myndigheder ([189]). I EU reguleres behandling af personoplysninger i forbindelse med retshåndhævelse af et særligt retsligt instrument, direktiv (EU) 2016/680 ([190]). Direktivet fastlægger særlige regler for databeskyttelse, som er bindende for kompetente myndigheder, når de behandler personoplysninger navnlig for at forebygge, efterforske, afsløre og retsforfølge strafbare handlinger (se afsnit 8.2.1.).

2.2. Databehandling

Hovedpunkter

- »Databehandling« henviser til enhver behandling af personoplysninger.
- Udtrykket »behandling« omfatter automatisk og ikke-automatisk behandling.
- Under EU-retten henviser »behandling« desuden også til ikke-elektronisk behandling i strukturerede registre.
- I henhold til Europarådets retsorden kan betydningen af »behandling« ved national lovgivning udvides til også at omfatte ikke-elektronisk behandling.

([188]) Den moderniserede konvention 108, artikel 6, stk. 1.

([189]) Generel forordning om databeskyttelse, artikel 10.

([190]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA, EUT L 119 af 4. maj 2016.

2.2.1. Begrebet databehandling

Databehandling er et omfattende begreb **under både EU-retten og Europarådets retsorden**: Behandling af personoplysninger betyder »enhver aktivitet [...], f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse« ([191]) af personoplysninger. Den moderniserede konvention 108 tilføjer beskyttelse af personoplysninger til definitionen ([192]).

Eksempel: I sagen *František Ryneš* ([193]) optog František Ryneš video af to personer, som knuste vinduer i hans hjem, via hjemmets kameraovervågningssystem, som han havde monteret for at beskytte sin ejendom. EU-Domstolen fastslog, at videoovervågning, der omfatter optagelse og lagring af personoplysninger, er automatisk databehandling, som er underlagt EU's databeskyttelseslovgivning.

Eksempel: I sagen *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni* ([194]) anmodede Salvatore Manni om at få fjernet sine personoplysninger fra et kreditvurderingsselskabs register, som knyttede ham til likvidationen af et ejendomsselskab, hvilket havde en negativ virkning på hans omdømme. EU-Domstolen fastholdt, at »den myndighed, der har ansvaret for at føre selskabsregistret, ved at indføre og opbevare de nævnte oplysninger i registret og ved i givet fald efter anmodning at videregive disse til tredjemand, [foretager] en »behandling af personoplysninger«, som den er den »registeransvarlige« for«.

Eksempel: Arbejdsgivere indsamler og behandler oplysninger om deres medarbejdere, herunder information om deres løn. Retsgrundlaget for at gøre dette legitimt er ansættelseskontrakten.

([191]) Generel forordning om databeskyttelse, artikel 4, stk. 2. Se også den moderniserede konvention 108, artikel 2, litra b).

([192]) Den moderniserede konvention 108, artikel 2, litra b).

([193]) EU-Domstolen, C-212/13, *František Ryneš mod Úřad pro ochranu osobních údajů*, 11. december 2014, præmis 25.

([194]) EU-Domstolen, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 9. marts 2017, præmis 35.

Arbejdsgivere skal fremsende personalets lønoplysninger til skattemyndighederne. Denne fremsendelse af data udgør også »behandling«, således som dette udtryk er defineret i den moderniserede konvention 108 og GDPR. Retsgrundlaget for denne fremsendelse er dog ikke ansættelseskontrakten. Der skal være et yderligere retsgrundlag for behandling, der medfører overførsel af lønoplysninger fra arbejdsgiveren til skattemyndighederne. Dette retsgrundlag er normalt en del af bestemmelserne i de nationale skattelove. Uden sådanne bestemmelser og uden et legitimt grundlag for behandlingen ville videregivelsen af sådanne oplysninger udgøre ulovlig behandling.

2.2.2. Automatisk databehandling

Databeskyttelse i henhold til den moderniserede konvention 108 og GDPR er fuldt ud gældende for automatisk databehandling.

Under **EU-retten** omhandler automatisk databehandling aktiviteter, som udføres på »personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling« ([195]). Den moderniserede konvention 108 indeholder en lignende definition ([196]). Med andre ord betyder dette, at enhver behandling af personoplysninger via automatisk databehandling, f.eks. ved brug af en PC, mobilenhed eller en router, er både omfattet af EU's og Europarådets databeskyttelsesregler.

Eksempel: Sagen *Bodil Lindqvist* ([197]) omhandlede henvisninger til forskellige personer ud fra navn eller andet, såsom deres telefonnummer eller oplysninger om deres fritidsinteresser, på en internetside. EU-Domstolen fastholdt, at »en operation, der består i på en internetside at henvise til forskellige personer, og i at identificere dem ved navn eller på anden måde, f.eks. ved at oplyse deres telefonnummer eller ved at give oplysninger om deres arbejdsforhold og fritidsinteresser, udgør en »behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb« i den forstand, hvori udtrykket er anvendt i artikel 3, stk. 1, i direktiv 95/46/EF« ([198]).

([195]) Generel forordning om databeskyttelse, artikel 2, stk. 1, og artikel 4, stk. 2.

([196]) Den moderniserede konvention 108, artikel 2, litra b) og c), og forklarende rapport til den moderniserede konvention 108, stk. 21.

([197]) EU-Domstolen, C-101/01, *Straffesag mod Bodil Lindqvist*, 6. november 2003, præmis 27.

([198]) Generel forordning om databeskyttelse, artikel 2, stk. 1.

Eksempel: I sagen *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD), Mario Costeja González* ([199]) anmodede Mario Costeja González om at få et link mellem hans navn i Googles søgemaskine og to avisartikler, der annoncerede en tvangsauktion over fast ejendom på grund af gæld til den sociale sikringsordning, fjernet eller ændret. EU-Domstolen bemærkede, at »en søgemaskineudbyder, idet den automatisk, konstant og systematisk undersøger internettet for de oplysninger, der offentliggøres dér, »indsamler« sådanne oplysninger, som den dernæst »selektionerer«, »registrerer« og »systematiserer« inden for rammerne af sine indekseringsprogrammer, »opbevarer« på sine servere og i givet fald »videregiver« og »overlader« til sine brugere i form af resultatlister af brugernes søgninger« ([200]). EU-Domstolen konkluderede, at sådanne operationer skal kvalificeres som »behandling«, »uden at det herved har betydning, at søgemaskineudbyderen ligeledes anvender de samme operationer på andre typer oplysninger og ikke sondrer mellem disse og personoplysninger«.

2.2.3. Ikke-automatisk databehandling

Ikke-elektronisk databehandling kræver også databeskyttelse.

Databeskyttelse i henhold til **EU-retten** er på ingen måde begrænset til automatisk databehandling. Databeskyttelse gælder således i EU-retten for behandlingen af personoplysninger i et ikke-elektronisk register, dvs. et særligt struktureret papirregister ([201]). Et struktureret register er et, som kategoriserer et sæt personoplysninger og gør dem tilgængelige ud fra bestemte kriterier. Hvis en arbejdsgiver for eksempel forvalter et papirregister benævnt »medarbejderes orlov«, der indeholder alle detaljer om den orlov, som personalet har afholdt i det foregående år, og er sorteret alfabetisk, vil det register udgøre et ikke-elektronisk register, som er underlagt EU's databeskyttelsesregler. Databeskyttelse er her udvidet af følgende grunde:

- Papirregistre kan struktureres på en måde, som gør det let og hurtigt at finde information.

([199]) EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014.

([200]) *Ibid*., præmis 28.

([201]) Generel forordning om databeskyttelse, artikel 2, stk. 1.

- Opbevaring af personoplysninger i strukturerede papirregistre gør det nemt at omgå de begrænsninger, der ved lov er fastsat for automatisk databehandling ([202]).

I **Europarådets retsorden** anerkender definitionen af automatisk behandling, at det kan være nødvendigt med visse faser med ikke-elektronisk behandling af personoplysninger imellem automatiske operationer ([203]). Artikel 2, litra c), i den moderniserede konvention 108 fastlægger, at databehandling, når automatisk behandling ikke benyttes, betyder en operation eller række operationer foretaget på personoplysninger inden for et struktureret sæt af sådanne oplysninger, som er tilgængelige eller kan indhentes ud fra bestemte kriterier.

2.3. Brugere af personoplysninger

Hovedpunkter

- Enhver, der beslutter midlerne og formålet med behandlingen af andres personoplysninger, er en »dataansvarlig« i henhold til databeskyttelseslovgivningen. Hvis flere tager denne beslutning sammen, kan de være »fælles dataansvarlige«.
- En »databehandler« er en naturlig eller juridisk person, der behandler personoplysninger på den dataansvarliges vegne.
- En databehandler bliver en dataansvarlig, hvis denne bestemmer midlerne og formålene med selve databehandlingen.
- Alle, der modtager personoplysninger, er en »modtager«.
- En »tredjemand« er en fysisk eller juridisk person, som ikke er den registrerede, den dataansvarlige, databehandleren og personer, som under den dataansvarliges eller databehandlerens direkte myndighed er beføjet til at behandle personoplysninger.
- Samtykke som et juridisk grundlag for behandling af personoplysninger skal være en frit givet, informeret, specifik og utvetydig viljetilkendegivelse i form af en klar bekræftelse, der angiver accept af behandlingen.
- Behandling af særlige kategorier af oplysninger på baggrund af samtykke kræver udtrykkeligt samtykke.

([202]) Generel forordning om databeskyttelse, betragtning 15.

([203]) Den moderniserede konvention 108, artikel 2, litra b) og c).

2.3.1. Dataansvarlige og databehandlere

At være dataansvarlig eller databehandler medfører primært et juridisk ansvar for at overholde de respektive forpligtelser, der følger af databeskyttelseslovgivningen. I den private sektor er dette normalt en fysisk eller juridisk person. I den offentlige sektor er det normalt en myndighed. Der er en væsentlig forskel mellem en dataansvarlig og en databehandler: Førstnævnte er den fysiske eller juridiske person, som bestemmer behandlingens midler og formål, og sidstnævnte er den fysiske eller juridiske person, der behandler oplysningerne på den dataansvarliges vegne ud fra strenge instrukser. Principielt er det den dataansvarlige, som skal kontrollere behandlingen og er ansvarlig herfor, herunder juridisk ansvar. Med reformen af databeskyttelsesreglerne er databehandlere dog nu forpligtet til at overholde mange af kravene, som gælder for dataansvarlige. Under GDPR skal databehandlere for eksempel føre fortegnelser over alle kategorier af behandlingsaktiviteter for at påvise deres overholdelse af forordningens forpligtelser ([204]). Databehandlere skal også implementere passende tekniske og organisatoriske foranstaltninger til at sikre behandlingssikkerheden ([205]), til at udpege en databeskyttelsesrådgiver under særlige omstændigheder ([206]) og til at underrette den dataansvarlige om brud ([207]).

Hvorvidt en person har kapaciteten til at beslutte og bestemme behandlingens formål og midler afhænger af de pågældende faktiske elementer eller omstændigheder. I medfør af GDPR's definition kan fysiske personer, juridiske personer eller ethvert andet organ være en dataansvarlig. Artikel 29-Gruppen har dog understreget, at det med henblik på at give de registrerede en mere stabil referenceenhed i forbindelse med udøvelsen af deres rettigheder »bør [...] foretrækkes at anse selve virksomheden eller organet for at være den registeransvarlige snarere end en bestemt person i virksomheden eller organet« ([208]). For eksempel er det virksomheden, der sælger produkter til sundhedspleje til læger, som er den dataansvarlige for indsamling og vedligeholdelse af distributionslisten over alle læger i et bestemt område, og den salgsansvarlige, som faktisk bruger og forvalter listen, er dermed ikke dataansvarlig herfor.

([204]) Generel forordning om databeskyttelse, artikel 30, stk. 2.

([205]) *Ibid*., artikel 32.

([206]) *Ibid*., artikel 37.

([207]) *Ibid*., artikel 33, stk. 2.

([208]) Artikel 29-Gruppen (2010), *Udtalelse 1/2010 om begreberne »registeransvarlig« og »registerfører«*, WP 169, Bruxelles, 16. februar 2010.

Eksempel: Når markedsføringsdivisionen af selskabet Sunshine har planer om at behandle oplysninger til brug i en markedsundersøgelse, er selskabet Sunshine, og ikke markedsføringsdivisionen, den dataansvarlige for behandlingen. Markedsføringsdivisionen kan ikke være den dataansvarlige, da den ikke har en særskilt identitet.

Fysiske personer kan være dataansvarlige under både EU-retten og Europarådets retsorden. Ved behandling af oplysninger om andre som del af en rent personlig eller familiemæssig aktivitet er private enkeltpersoner dog ikke omfattet af reglerne i GDPR og den moderniserede konvention 108 og betragtes ikke som dataansvarlige ([209]). En enkeltperson, som fører korrespondance eller en personlig dagbog, der beskriver hændelser med venner og kolleger og familiemedlemmers patientjournaler, kan være fritaget fra databeskyttelsesreglerne, da disse aktiviteter kan være af en rent personlig eller familiemæssig art. GDPR angiver yderligere, at personlige eller familiemæssige aktiviteter også kan omfatte sociale netværksaktiviteter og onlineaktiviteter, der udøves som led i sådanne aktiviteter ([210]). På den anden side gælder databeskyttelsesregler fuldt ud for dataansvarlige og databehandlere, som tilvejebringer midlerne til behandling af personoplysninger til sådanne personlige eller familiemæssige aktiviteter (f.eks. platforme til sociale netværk) ([211]).

Borgeres internetadgang og muligheden for at benytte e-handelsplatforme, sociale netværk og blogs til at dele personlige oplysninger om sig selv og andre enkeltpersoner gør det i stigende grad mere vanskeligt at adskille behandling af personoplysninger fra behandling af oplysninger, som ikke er personlige ([212]). Om aktiviteter er rent personlige eller familiemæssige afhænger af omstændighederne ([213]). Aktiviteter, som har erhvervsmæssige eller kommercielle aspekter, er ikke omfattet af undtagelsen for familiemæssige aktiviteter ([214]). Når databehandlingens omfang og hyppighed tyder på, at der er tale om en erhvervsmæssig aktivitet eller fuldtidsbeskæftigelse, kan en privatperson dermed betragtes som en dataansvarlig. Udover

([209]) Generel forordning om databeskyttelse, betragtning 18, og artikel 2, stk. 2, litra c), og den moderniserede konvention 108, artikel 3, stk. 2.

([210]) Generel forordning om databeskyttelse, betragtning 18.

([211]) *Ibid.*, betragtning 18 og den forklarende rapport til den moderniserede konvention 108, stk. 29.

([212]) Se erklæringen i artikel 29-Gruppen vedrørende diskussioner omkring databeskyttelsesreformpakken (2013), *bilag 2: Proposals and Amendments regarding exemption for personal or household activities*, 27. februar 2013.

([213]) Forklarende rapport til den moderniserede konvention 108, stk. 28.

([214]) Se generel forordning om databeskyttelse, betragtning 18, og forklarende rapport til den moderniserede konvention 108, stk. 27.

den erhvervsmæssige eller kommercielle karakter af behandlingsaktiviteten er en anden faktor, der skal tages hensyn til, om personoplysninger gøres tilgængelige for et stort antal personer, som tydeligvis ligger uden for den private sfære for en enkeltperson. Retspraksis i henhold til databeskyttelsesdirektivet har konstateret, at databeskyttelseslovgivning finder anvendelse, når en privatperson i forbindelse med vedkommendes brug af internettet offentliggør oplysninger om andre på et offentligt websted. EU-Domstolen har endnu ikke afsagt dom om lignende fakta i medfør af GDPR, som indeholder mere vejledning om de emner, der kan vurderes som værende uden for anvendelsesområdet af databeskyttelseslovgivningen under »undtagelsen for familiemæssige aktiviteter«, såsom brugen af sociale medier i personligt øjemed.

Eksempel: Sagen *Bodil Lindqvist* ([215]) omhandlede henvisninger til forskellige personer ud fra navn eller andet, såsom deres telefonnummer eller oplysninger om deres fritidsinteresser, på en internetside. EU-Domstolen fastholdt, at »en operation, der består i på en internetside at henvise til forskellige personer, og i at identificere dem ved navn eller på anden måde [...] udgør en »behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb«« i den forstand, hvori udtrykket er anvendt i artikel 3, stk. 1, i databeskyttelsesdirektivet ([216]).

En sådan behandling af personoplysninger betragtes ikke som rent personlige eller familiemæssige aktiviteter, som er fritaget fra EU's databeskyttelsesregler, da denne undtagelse »skal [...] fortolkes således, at den udelukkende vedrører de aktiviteter, der indgår i den enkelte borgers privatliv eller familieliv, hvilket åbenbart ikke er tilfældet med hensyn til behandling af personoplysninger, som består i, at de offentliggøres på internettet, hvorved disse oplysninger bliver tilgængelige for et ubestemt antal personer« ([217]).

I henhold til EU-Domstolen kan videooptagelser fra et privat monteret sikkerhedskamera også være omfattet af EU's databeskyttelseslovgivning under visse omstændigheder.

([215]) EU-Domstolen, C-101/01, *Straffesag mod Bodil Lindqvist*, 6. november 2003.

([216]) *Ibid.*, præmis 27; det tidligere direktiv 95/46/EF, artikel 3, stk. 1, som nu er den generelle forordning om databeskyttelse, artikel 2, stk. 1.

([217]) EU-Domstolen, C-101/01, *Straffesag mod Bodil Lindqvist*, 6. november 2003, præmis 47.

Eksempel: I sagen *František Ryneš* ([218]) optog František Ryneš video af to personer, som knuste vinduer i hans hjem, via hjemmets kameraovervågningssystem, som han havde monteret for at beskytte sin ejendom. Optagelsen blev derefter overdraget til politiet og henvist til under straffesagen.

EU-Domstolen fastslog, at i det omfang, at videoovervågning dækker, selv hvis det er delvist, et offentligt område og derfor er rettet væk fra det private område tilhørende personen, som behandler oplysningerne på denne måde, kan det ikke betragtes som en aktivitet, der henhører under begrebet »rent personlige eller familiemæssige aktiviteter« ([219]).

Dataansvarlig

I EU-retten defineres en dataansvarlig som den, »der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger« ([220]). En dataansvarligs afgørelse fastlægger, hvorfor og hvordan oplysninger skal behandles.

I Europarådets retsorden definerer den moderniserede konvention 108 en »dataansvarlig« som en fysisk eller juridisk person, en offentlig myndighed, en tjeneste, en institution eller et andet organ, der alene eller sammen med andre har beslutningsbeføjelser vedrørende databehandling ([221]). Sådanne beslutningsbeføjelser omhandler behandlingens formål og hjælpemidler samt de kategorier af oplysninger, der behandles, og adgang til oplysningerne ([222]). Om denne beføjelse stammer fra en retlig udpegelse eller fra faktiske omstændigheder skal afgøres ud fra den enkelte sag ([223]).

([218]) EU-Domstolen, C-212/13, *František Ryneš mod Úřad pro ochranu osobních údajů*, 11. december 2014, præmis 33.

([219]) Det tidligere direktiv 95/46/EF, artikel 3, stk. 2, andet led, som nu er den generelle forordning om databeskyttelse, artikel 2, stk. 2, litra c).

([220]) Generel forordning om databeskyttelse, artikel 4, stk. 7.

([221]) Den moderniserede konvention 108, artikel 2, litra d).

([222]) Forklarende rapport til den moderniserede konvention 108, stk. 22.

([223]) *Ibid*.

Eksempel: Sagen *Google Spain* ([224]) blev anlagt af en spansk borger, som ønskede at få en gammel avisrapport om hans finansielle historik fjernet fra Google.

EU-Domstolen blev spurgt, om Google som søgemaskineudbyder var den »dataansvarlige« for dataene i medfør af artikel 2, litra d), i databeskyttelsesdirektivet ([225]). EU-Domstolen overvejede en bred definition af begrebet »ansvarlig« for at »sikre en effektiv og fuldstændig beskyttelse af de berørte personer« ([226]). EU-Domstolen konstaterede, at søgemaskineudbyderen bestemte formålet med aktiviteten og hjælpemidlerne hertil, og at den gjorde oplysninger lagt ud på internetsider af websideudgivere tilgængelige for enhver internetbruger, der foretager en søgning på den berørte persons navn ([227]). EU-Domstolen besluttede derfor, at Google kan betragtes som »registeransvarlig« ([228]).

Når en dataansvarlig eller databehandler ikke er etableret i Unionen, skal denne virksomhed skriftligt udpege en repræsentant i Unionen ([229]). GDPR understreger, at »repræsentanten skal være etableret i en af de medlemsstater, hvor de registrerede, hvis personoplysninger behandles i forbindelse med udbud af varer eller tjenesteydelser til dem, eller hvis adfærd overvåges, er« ([230]). Udpeges ingen repræsentant, kan der stadig indledes eventuelle retlige skridt mod den dataansvarlige eller databehandleren selv ([231]).

Fælles dataansvar

GDPR fastlægger, at hvis to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling, er de fælles dataansvarlige. Dette

([224]) EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014.

([225]) Generel forordning om databeskyttelse, artikel 4, stk. 7, og EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014, præmis 21.

([226]) EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014, præmis 34.

([227]) *Ibid.*, præmis 35-40.

([228]) *Ibid.*, præmis 41.

([229]) Generel forordning om databeskyttelse, artikel 27, stk. 1.

([230]) *Ibid.*, artikel 27, stk. 3.

([231]) *Ibid.*, artikel 27, stk. 5.

betyder, at de sammen beslutter at behandle oplysninger til et fælles formål ([232]). Den forklarende rapport til den moderniserede konvention 108 fastlægger, at flere dataansvarlige eller fælles udøvelse af dataansvar også er muligt under **Europarådets lovrammer** ([233]).

Artikel 29-Gruppen påpeger, at fælles kontrol kan antage forskellige former, og at de forskellige dataansvarlige kan deltage i forskellig grad i kontrolaktiviteterne ([234]). Denne fleksibilitet gør det muligt at imødekomme den øgede kompleksitet i forbindelse med databehandling i den aktuelle virkelighed ([235]). Fælles dataansvarlige skal derfor bestemme deres individuelle ansvar for at overholde forordningens forpligtelser i en specifik aftale ([236]).

Fælles udøvelse af dataansvar fører til fælles ansvar for en behandlingsaktivitet ([237]). Inden for **EU-rettens** rammer betyder det, at hver dataansvarlig eller databehandler kan hæfte solidarisk for hele skaden forvoldt af behandlingen under fælles dataansvar for at sikre fuld erstatning til den registrerede ([238]).

Eksempel: En database, der køres i fællesskab af flere kreditinstitutter med registrering af deres misligholdende kunder, er et almindeligt eksempel på fælles dataansvar. Når en person ansøger om et lån hos en bank, der er en af de fælles dataansvarlige, kontrollerer banken databasen, når den skal træffe en informeret beslutning om ansøgerens kreditværdighed.

Lovbestemmelserne fastlægger ikke udtrykkeligt, om fælles dataansvar kræver, at det fælles formål er det samme for hver af de dataansvarlige, eller om det er tilstrækkeligt, at deres formål kun overlapper delvist. Der findes dog endnu ingen relevant retspraksis på europæisk plan. I Artikel 29-Gruppens udtalelse fra 2010 om begreberne registeransvarlige og registerførere fastlægges det, at fælles dataansvarlige enten kan dele alle formål og hjælpemidler ved en behandling eller kun

([232]) *Ibid.*, artikel 4, stk. 7, og artikel 26.

([233]) Den moderniserede konvention 108, artikel 2, litra d), og forklarende rapport til den moderniserede konvention 108, stk. 22.

([234]) Artikel 29-Gruppen (2010), *Udtalelse 1/2010 om begreberne »registeransvarlig« og »registerfører«*, WP 169, Bruxelles, 16. februar 2010, s. 19.

([235]) *Ibid.*

([236]) Generel forordning om databeskyttelse, betragtning 79.

([237]) *Ibid.*, stk. 21.

([238]) *Ibid.*, artikel 82, stk. 4.

dele formål eller hjælpemidler eller en del heraf ([239]). Hvor førstnævnte antyder et meget tæt forhold mellem de forskellige aktører, antyder sidstnævnte et mere løst forhold.

Artikel 29-Gruppen anbefaler en bredere fortolkning af begrebet fælles kontrol, hvilket giver mulighed for større fleksibilitet med henblik på at imødekomme den øgede kompleksitet i forbindelse med databehandling i den aktuelle virkelighed ([240]). En sag med Society for Worldwide Interbank Financial Telecommunication (SWIFT) illustrerer Artikel 29-Gruppens holdning.

Eksempel: I den såkaldte SWIFT-sag gjorde europæiske pengeinstitutter indledningsvist brug af SWIFT som databehandler til forvaltning af dataoverførsler i forbindelse med banktransaktioner. SWIFT videresendte disse banktransaktionsoplysninger, som var lagret i et driftscenter i De Forenede Stater (USA), til det amerikanske finansministerium, uden at SWIFT udtrykkeligt var blevet bedt herom af de europæiske pengeinstitutter, som havde beskæftiget SWIFT. Artikel 29-Gruppen drog i løbet af evalueringen af situationens lovlighed den konklusion, at de europæiske pengeinstitutter, som havde beskæftiget SWIFT, samt SWIFT havde et fælles ansvar over for de europæiske kunder for overførslen af deres data til de amerikanske myndigheder ([241]).

Databehandler

En databehandler er **under EU-retten** defineret som én, der behandler personoplysninger på den dataansvarliges vegne ([242]). De aktiviteter, som overdrages til en databehandler, kan være begrænset til en meget specifik opgave eller sammenhæng eller kan være meget generel og omfattende.

I Europarådets retsorden defineres en databehandler på samme måde som i EU-retten ([243]).

([239]) Artikel 29-Gruppen (2010), Udtalelse 1/2010 om begreberne »registeransvarlig« og »registerfører«, WP 169, Bruxelles, 16. februar 2010, s. 19.

([240]) *Ibid*.

([241]) Artikel 29-Gruppen (2006), *Udtalelse 10/2006 om behandling af personoplysninger i Society for Worldwide Interbank Financial Telecommunication (SWIFT),* WP 128, Bruxelles, 22. november 2006.

([242]) Generel forordning om databeskyttelse, artikel 4, stk. 8.

([243]) Den moderniserede konvention 108, artikel 2, litra f).

Ud over at behandle oplysninger for andre er databehandlere også selv dataansvarlige i forhold til den behandling, de foretager til deres egne formål, f.eks. administrationen af deres egne medarbejdere, salg og regnskaber.

Eksempel: Virksomheden Everready er specialiseret i databehandling i forbindelse med administration af personaleoplysninger for andre virksomheder. I denne funktion er Everready databehandler. Når Everready behandler oplysninger om sine egne medarbejdere, er virksomheden dog den dataansvarlige for databehandling, der har til formål at opfylde virksomhedens forpligtelser som arbejdsgiver.

Forholdet mellem dataansvarlig og databehandler

Den dataansvarlige defineres således som den, der afgør, til hvilket formål og med hvilke hjælpemidler behandlingen må foretages. GDPR fastlægger udtrykkeligt, at databehandleren kun må behandle personoplysninger efter anvisning fra den dataansvarlige, medmindre EU's eller en medlemsstats lovgivning kræver, at databehandleren udfører behandlingen ([244]). Kontrakten mellem den dataansvarlige og databehandleren er et vigtigt element i deres forhold og et lovkrav ([245]).

Eksempel: Direktøren for virksomheden Sunshine beslutter, at virksomheden Cloudy, som har specialiseret sig i skybaseret datalagring, skal forvalte Sunshines kundedata. Virksomheden Sunshine forbliver den dataansvarlige, og Cloudy er kun databehandler, idet Cloudy i henhold til kontrakten kun må anvende Sunshines kundedata til de formål, som Sunshine fastlægger.

Hvis beføjelsen til at afgøre, med hvilke hjælpemidler behandlingen foretages, uddelegeres til en databehandler, skal den dataansvarlige stadig have en passende grad af kontrol over databehandlerens beslutninger med hensyn til hjælpemidler til behandling. Det overordnede ansvar ligger stadig hos den dataansvarlige, som skal føre tilsyn med databehandlerne for at sikre, at deres beslutninger er i overensstemmelse med databeskyttelseslovgivningen og de instrukser, de har modtaget.

([244]) Generel forordning om databeskyttelse, artikel 29.

([245]) *Ibid.*, artikel 28, stk. 3.

Hvis en databehandler ikke overholder de begrænsninger for databehandling, som den dataansvarlige har fastlagt, bliver databehandleren desuden dataansvarlig, for så vidt vedkommende overtræder den dataansvarliges instrukser. Dette vil sandsynligvis gøre databehandleren til en dataansvarlig, der handler ulovligt. Den oprindelige dataansvarlige skal til gengæld forklare, hvordan det var muligt for databehandleren at overtræde sit mandat ([246]). I henhold til Artikel 29-Gruppen er der ofte tale om fælles kontrol i sådanne tilfælde, da det sikrer den bedste beskyttelse af de registreredes interesser ([247]).

Der kan også være problemer i forbindelse med ansvarsfordelingen, når en dataansvarlig er en lille virksomhed, og databehandleren er et stort selskab, der har kapacitet til at diktere betingelserne for dets tjenesteydelser. Under sådanne omstændigheder fastholder Artikel 29-Gruppen dog, at standarden for ansvar ikke bør sænkes på grundlag af økonomisk skævhed, og at fortolkningen af begrebet »registeransvarlig« (dataansvarlig) skal fastholdes ([248]).

Af hensyn til klarheden og gennemsigtigheden bør detaljerne om forholdet mellem en dataansvarlig og en databehandler registreres i en skriftlig kontrakt ([249]). Kontrakten skal navnlig indeholde genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede. Den skal også angive den dataansvarliges og databehandlerens forpligtelser og rettigheder, såsom krav vedrørende tavshedspligt og sikkerhed. Hvis en sådan kontrakt ikke forefindes, er det et brud på den dataansvarliges forpligtelse til at fremlægge skriftlig dokumentation for parternes gensidige ansvar, og det kan medføre sanktioner. Når skader forårsages som følge af, at den pågældende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser, er det ikke kun den dataansvarlige men også databehandleren, som hæfter herfor ([250]). Databehandleren skal føre fortegnelser over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige ([251]). Disse

([246]) *Ibid*., artikel 82, stk. 2.

([247]) Artikel 29-Gruppen (2010), *Udtalelse 1/2010 om begreberne »registeransvarlig« og »registerfører«*, WP 169, Bruxelles, 16. februar 2010, s. 25, og Artikel 29-Gruppen (2006), *Udtalelse 10/2006 om behandling af personoplysninger i Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Bruxelles, 22. november 2006.

([248]) Artikel 29-Gruppen (2010), *Udtalelse 1/2010 om begreberne »registeransvarlig« og »registerfører«*, WP 169, Bruxelles, 16. februar 2010, s. 26.

([249]) Generel forordning om databeskyttelse, artikel 28, stk. 3 og 9.

([250]) *Ibid*., artikel 82, stk. 2.

([251]) *Ibid*., artikel 30, stk. 2.

fortegnelser skal efter anmodning stilles til rådighed for tilsynsmyndigheden, da den dataansvarlige og databehandleren begge skal samarbejde med denne myndighed i forbindelse med udførelsen af dens opgaver ([252]). Dataansvarlige og databehandlere har også mulighed for at overholde et godkendt adfærdskodeks eller en godkendt certificeringsmekanisme for at påvise deres overholdelse af GDPR's krav ([253]).

Databehandlere kan vælge at uddelegere visse opgaver til yderligere underkontraherede databehandlere. Dette er tilladt i henhold til lovgivningen og afhænger i detaljer af kontraktbestemmelserne mellem den dataansvarlige og databehandleren, herunder om den dataansvarliges godkendelse er nødvendig i hvert enkelt tilfælde, eller om underretning alene er tilstrækkelig. GDPR fastsætter, at den indledende databehandler forbliver fuldt ansvarlig over for den dataansvarlige for den underkontraherede databehandlers opfyldelse af sine databeskyttelsesforpligtelser ([254]).

I Europarådets retsorden gælder fortolkningen af begreberne dataansvarlig og databehandler (tidligere: registeransvarlig og registerfører), jf. ovennævnte, fuldt ud ([255]).

2.3.2. Modtagere og tredjemænd

Forskellen mellem disse to kategorier af personer eller enheder, som blev indført ved databeskyttelsesdirektivet, ligger primært i deres forhold til den dataansvarlige og dermed deres bemyndigelse til at få adgang til de personoplysninger, som den dataansvarlige ligger inde med.

En »tredjemand« er en part, som er adskilt fra den dataansvarlige og databehandleren. I henhold til artikel 4, stk. 10, i GDPR er en »tredjemand« en anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle personoplysninger«. Det betyder, at personer, der arbejder for en organisation, som er adskilt fra den registeransvarlige — selv om den

([252]) *Ibid.*, artikel 30, stk. 4 og 31.

([253]) *Ibid.*, artikel 28, stk. 5, og artikel 42, stk. 4.

([254]) *Ibid.*, artikel 28, stk. 4.

([255]) Se for eksempel: den moderniserede konvention 108, artikel 2, litra b) og f), og henstilling om profilering, artikel 1.

tilhører samme koncern eller holdingselskab – er (eller tilhører) en »tredjemand«. Filialer af en bank, som behandler en kundes konti under hovedkvarterets direkte bemyndigelse, betragtes på den anden side ikke som »tredjemænd« ([256]).

»Modtager« er et bredere begreb end »tredjemand«. I henhold til GDPR's artikel 4, stk. 9, er en modtager »en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, hvortil personoplysninger videregives, uanset om det er en tredjemand eller ej«. Modtageren kan være en person uden for den dataansvarliges eller databehandlerens organisation – og er så en tredjemand – eller en person inden for den registeransvarliges eller registerførerens organisation, som f.eks. en medarbejder eller en anden afdeling inden for samme virksomhed eller myndighed.

Sondringen mellem modtagere og tredjemænd er kun vigtig på grund af betingelserne for lovlig fremlæggelse af oplysninger. En dataansvarligs eller databehandlers medarbejdere kan uden yderligere juridiske krav være modtagere af personoplysninger, hvis de er involveret i den dataansvarliges eller databehandlerens behandlingsaktiviteter. En tredjemand, som er adskilt fra den dataansvarlige eller databehandleren, er på den anden side ikke beføjet til at anvende de personoplysninger, der besiddes af den dataansvarlige, medmindre der foreligger et særligt retsgrundlag i et konkret tilfælde.

Eksempel: En dataansvarligs medarbejder, som anvender personoplysninger til at udføre de opgaver, som arbejdsgiveren har pålagt ham eller hende, er en modtager af oplysninger, men ikke en tredjemand, da han eller hun bruger oplysningerne på vegne af og efter den dataansvarliges instrukser. Hvis en arbejdsgiver for eksempel videregiver personoplysninger om sine medarbejdere til sin personaleafdeling i forbindelse med fremkommende medarbejderevalueringer, er medarbejderne ved personaleafdelingen modtagere af personoplysninger, da oplysningerne er videresendt til dem i forbindelse med den dataansvarliges behandling.

Hvis organisationen derimod videregiver oplysninger om sine medarbejdere til en undervisningsvirksomhed, som bruger dem til at tilrettelægge et undervisningsprogram for medarbejderne, er undervisningsvirksomheden en tredjemand. Dette skyldes, at undervisningsvirksomheden ikke besidder en særlig berettigelse eller godkendelse (som i tilfældet med »personaleafdelingen«

([256]) Artikel 29-Gruppen (2010), Udtalelse 1/2010 om begreberne »registeransvarlig« og »registerfører«, WP 169, Bruxelles, 16. februar 2010, s. 31.

stammer fra ansættelsesforholdet til den dataansvarlige) til at behandle disse personoplysninger. Med andre ord har de ikke modtaget oplysningerne i forbindelse med deres ansættelse ved den dataansvarlige.

2.4. Samtykke

Hovedpunkter

- Samtykke som et juridisk grundlag for behandling af personoplysninger skal være en frit givet, informeret, specifik og utvetydig viljetilkendegivelse i form af en klar bekræftelse, der angiver accept af behandlingen.
- Behandling af særlige kategorier af oplysninger kræver udtrykkeligt samtykke.

Samtykke er som detaljeret i kapitel 4 én af de seks legitime grunde for behandling af personoplysninger. Samtykke betyder »enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede« ([257]).

EU-retten fastlægger flere kriterier for, at et samtykke er gyldigt. Dette har til formål at sikre, at registrerede virkelig havde til hensigt at acceptere en specifik anvendelse af deres oplysninger: ([258])

- Samtykke skal gives i form af en klar bekræftelse, der indebærer en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved vedkommende accepterer, at personoplysninger om vedkommende behandles. Dette kan foregå ved en erklæring eller handling.
- Den registrerede skal have ret til at trække samtykke tilbage på ethvert tidspunkt.
- I forbindelse med en skriftlig erklæring, som også omfatter andre forhold, såsom »servicevilkår«, skal en anmodning om samtykke forelægges på en måde, som klart kan skelnes fra de andre forhold, i en letforståelig og lettilgængelig form og

([257]) Generel forordning om databeskyttelse, artikel 4, stk. 11. Se også den moderniserede konvention 108, artikel 5, stk. 2.

([258]) Generel forordning om databeskyttelse, artikel 7.

i et klart og enkelt sprog. Enhver del af en sådan erklæring, som udgør en overtrædelse af GDPR, er ikke bindende.

Kun hvis alle disse krav er opfyldt, vil samtykket være gyldigt ifølge databeskyttelseslovgivningen. Det er den dataansvarliges ansvar at påvise, at den registrerede har givet samtykke til behandlingen af sine personoplysninger ([259]). Kriterierne for gyldigt samtykke diskuteres yderligere i afsnit 4.1.1. om lovlige grundlag for behandling af personoplysninger.

Konvention 108 indeholder ikke en definition af samtykke, men overlader dette til den nationale lovgivning. **I Europarådets retsorden** svarer kriterierne for et gyldigt samtykke dog til dem, der er nævnt ovenfor ([260]).

Yderligere civilretlige krav til et gyldigt samtykke, som f.eks. retsevne, gælder naturligvis også i forbindelse med databeskyttelse, da sådanne krav er grundlæggende juridiske forudsætninger. Ugyldigt samtykke fra personer, der ikke har retsevne, betyder, at der ikke er et retsgrundlag for at behandle oplysninger om sådanne personer. I forbindelse med mindreåriges retsevne til at indgå kontrakter fastlægger GDPR, at dens regler om mindstealderen for indhentning af gyldigt samtykke ikke påvirker medlemsstaternes generelle aftaleret ([261]).

Samtykke skal afgives på en tydelig måde, så der ikke er tvivl om den registreredes hensigt ([262]). Samtykke skal være udtrykkelig, når den vedrører behandling af følsomme oplysninger, og kan gives mundtligt eller skriftligt ([263]). Sidstnævnte kan foregå elektronisk ([264]). Inden for rammerne af både **EU-retten** og **Europarådets retsorden** skal en persons accept af behandlingen af vedkommendes oplysninger gives i en erklæring eller ved en klar bekræftelse ([265]). Samtykke kan dermed ikke gives ved tavshed, forudafkrydsede felter eller inaktivitet ([266]).

([259]) *Ibid.*, artikel 7, stk. 1.

([260]) Den moderniserede konvention 108, artikel 5, stk. 2, og forklarende rapport til den moderniserede konvention 108, stk. 42-45.

([261]) Generel forordning om databeskyttelse, artikel 8, stk. 3.

([262]) *Ibid.*, artikel 6, stk. 1, litra a), og artikel 9, stk. 2, litra a).

([263]) *Ibid.*, betragtning 32.

([264]) *Ibid.*

([265]) *Ibid.*, artikel 4, stk. 11, og den forklarende rapport til den moderniserede konvention 108, stk. 42.

([266]) Generel forordning om databeskyttelse, betragtning 32, og forklarende rapport til den moderniserede konvention 108, stk. 42.

3

De centrale principper i den europæiske databeskyttelseslovgivning

EU	Omhandlede emner	Europarådet
Generel forordning om databeskyttelse, artikel 5, stk. 1, litra a)	**Princippet om lovlighed**	Den moderniserede konvention 108, artikel 5, stk. 3
Generel forordning om databeskyttelse, artikel 5, stk. 1, litra a)	**Princippet om rimelighed**	Den moderniserede konvention 108, artikel 5, stk. 4, litra a) EMD, *K.H. m.fl. mod Slovakiet*, nr. 32881/04, 2009
Generel forordning om databeskyttelse, artikel 5, stk. 1, litra a) EU-Domstolen, C-201/14, *Smaranda Bara m.fl. mod Casa Națională de Asigurări de Sănătate m.fl.*, 2015	**Princippet om gennemsigtighed**	Den moderniserede konvention 108, artikel 5, stk. 4, litra a), og artikel 8 EMD, *Haralambie mod Rumænien*, nr. 21737/03, 2009
Generel forordning om databeskyttelse, artikel 5, stk. 1, litra b)	**Princippet om formålsbegrænsning**	Den moderniserede konvention 108, artikel 5, stk. 4, litra b)
Generel forordning om databeskyttelse, artikel 5, stk. 1, litra c) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 2014	**Princippet om dataminimering**	Den moderniserede konvention 108, artikel 5, stk. 4, litra c)

EU	Omhandlede emner	Europarådet
Generel forordning om databeskyttelse, artikel 5, stk. 1, litra d) EU-Domstolen, C-553/07, *College van burgemeester en wethouders van Rotterdam mod M. E. E. Rijkeboer*, 2009	**Princippet om rigtigheden af oplysninger**	Den moderniserede konvention 108, artikel 5, stk. 4, litra d)
Generel forordning om databeskyttelse, artikel 5, stk. 1, litra e) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 2014	**Princippet om opbevarings-begrænsning**	Den moderniserede konvention 108, artikel 5, stk. 4, litra e) EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 2008
Generel forordning om databeskyttelse, artikel 5, stk. 1, litra f), og artikel 32	**Princippet om datasikkerhed (integritet og fortrolighed)**	Den moderniserede konvention 108, artikel 7
Generel forordning om databeskyttelse, artikel 5, stk. 2	**Princippet om ansvarlighed**	Den moderniserede konvention 108, artikel 10

Artikel 5 i den generelle forordning om databeskyttelse fastlægger principperne for behandling af personoplysninger. Disse principper omfatter:

- lovlighed, rimelighed og gennemsigtighed
- formålsbegrænsning
- dataminimering
- rigtigheden af oplysninger
- opbevaringsbegrænsning
- integritet og fortrolighed.

Principperne fungerer som et udgangspunkt for de mere detaljerede bestemmelser i forordningens senere artikler. De optræder også i artikel 5, 7, 8 og 10 i den moderniserede konvention 108. Al senere lovgivning om databeskyttelse, der vedtages

af Europarådet eller på EU-plan, skal overholde disse principper, og der skal tages hensyn til dem ved enhver fortolkning af en sådan lovgivning. Under EU-retten tillades begrænsninger af behandlingsprincipperne kun i det omfang, at de svarer til rettigheder og forpligtelser fastlagt i artikel 12-22, og de skal overholde det væsentligste indhold af de grundlæggende rettigheder og friheder. Alle undtagelser fra og begrænsninger af disse centrale principper kan fastlægges på EU- eller nationalt plan ([267]). De skal være fastlagt ved lov, forfølge et legitimt formål og være nødvendige i et demokratisk samfund ([268]). Alle tre betingelser skal være opfyldt.

3.1. Principperne om lovlighed, rimelighed og gennemsigtighed

Hovedpunkter

- Principperne om lovlighed, rimelighed og gennemsigtighed gælder for enhver behandling af personoplysninger.
- Under GDPR kræver lovlighed enten:
  - den registreredes samtykke
  - krav om indgåelse af en kontrakt
  - en retlig forpligtelse
  - krav om at beskytte den registreredes eller en anden persons vitale interesser
  - krav om at udføre en opgave i offentlighedens interesse
  - krav om den dataansvarliges eller tredjemands legitime interesser, hvis de ikke tilsidesættes af den registreredes interesser og rettigheder.
- Behandling af personoplysninger skal udføres på en rimelig måde.
  - Den registrerede skal informeres omkring risikoen for at sikre, at behandling ikke har uforudsete negative konsekvenser.

([267]) Den moderniserede konvention 108, artikel 11, stk. 1, og generel forordning om databeskyttelse, artikel 23, stk. 1.

([268]) Generel forordning om databeskyttelse, artikel 23, stk. 1.

- Behandling af personoplysninger skal udføres på en gennemsigtig måde.
  - Dataansvarlige skal oplyse registrerede inden behandlingen af deres oplysninger om, bl.a., behandlingens formål og den dataansvarliges identitet og adresse.
  - Information om behandlingsaktiviteter skal leveres i et klart og tydeligt sprog, så registrerede let kan forstå de pågældende regler, risici, garantier og rettigheder.
  - Registrerede skal have ret til at få adgang til deres oplysninger, uanset hvor de behandles.

3.1.1. Lovlig behandling

EU's og Europarådets lovgivning om databeskyttelse kræver, at personoplysninger behandles lovligt ([269]). Lovlig behandling kræver den registreredes samtykke eller et andet legitimt grundlag fastlagt i databeskyttelseslovgivningen ([270]). Artikel 6, stk. 1, i GDPR indeholder fem lovlige grundlag for behandling udover samtykke, såsom af hensyn til opfyldelse af en kontrakt, af hensyn til udførelse af en opgave, som henhører under offentlig myndighedsudøvelse, for at overholde en retlig forpligtelse, for at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse eller for at beskytte den registreredes vitale interesser. Dette diskuteres i detaljer i afsnit 4.1.

3.1.2. Rimelig behandling

Ud over lovlig behandling kræver EU's og Europarådets lovgivning om databeskyttelse, at personoplysninger behandles rimeligt ([271]). Princippet om rimelig behandling omhandler primært forholdet mellem den dataansvarlige og den registrerede.

Dataansvarlige skal meddele registrerede og den brede offentlighed om, at de vil behandle oplysninger på en lovlig og gennemsigtig måde, og skal kunne påvise behandlingsaktiviteters overholdelse af GDPR. Behandlingsaktiviteter må ikke udføres i hemmelighed, og registrerede skal kende til potentielle risici. Desuden skal dataansvarlige så vidt muligt handle på en måde, der omgående efterkommer

([269]) Den moderniserede konvention 108, artikel 5, stk. 3, og generel forordning om databeskyttelse, artikel 5, stk. 1, litra a).

([270]) Den Europæiske Unions charter om grundlæggende rettigheder, artikel 8, stk. 2, generel forordning om databeskyttelse, betragtning 40, og artikel 6-9, den moderniserede konvention 108, artikel 5, stk. 2, og forklarende rapport til den moderniserede konvention 108, stk. 41.

([271]) Generel forordning om databeskyttelse, artikel 5, stk. 1, litra c), og den moderniserede konvention 108, artikel 5, stk. 4, litra a).

den registreredes ønsker, navnlig når dennes samtykke udgør retsgrundlaget for databehandlingen.

Eksempel: I *K.H. m.fl. mod Slovakiet* ([272]) var sagsøgerne kvinder af romaoprindelse, som var blevet behandlet på to hospitaler i det østlige Slovakiet under deres graviditet og fødsler. Efterfølgende kunne ingen af dem igen blive gravide trods gentagne forsøg. De nationale domstole gav hospitalerne påbud om at give sagsøgerne og deres repræsentanter tilladelse til at se og tage håndskrevne noter af patientjournalerne, men afviste deres anmodning om tilladelse til at fotokopiere dokumenterne angiveligt for at forhindre misbrug heraf. Staternes positive forpligtelser i medfør af artikel 8 i EMRK omfatter nødvendigvis en forpligtelse til at give registrerede adgang til kopier af deres egne sagsakter. Det var staten, der fastlagde procedurerne for kopiering af personlige sagsakter, eller som eventuelt skulle fremlægge overbevisende begrundelse for afvisningen heraf. I sagsøgernes tilfælde begrundede de nationale domstole forbuddet mod kopiering af patientjournaler med behovet for at beskytte de pågældende oplysninger mod misbrug. EMD kunne dog ikke se, hvordan ansøgerne, som under alle omstændigheder havde fået aktindsigt i deres fulde patientjournaler, kunne have misbrugt oplysninger om dem selv. Man kunne endvidere have forebygget risikoen for misbrug på anden måde end ved at forbyde sagsøgerne at kopiere patientjournalerne, f.eks. ved at begrænse den kreds af personer, der havde aktindsigt. Staten kunne ikke påvise, at der var tilstrækkeligt overbevisende grundlag til at nægte sagsøgerne effektiv aktindsigt i oplysninger vedrørende deres helbred. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

I forbindelse med internettjenester skal funktionerne i databehandlingssystemer give de registrerede reel mulighed for at forstå, hvad der sker med deres oplysninger. Under alle omstændigheder går princippet om rimelighed videre end gennemsigtighedsforpligtelser og kan også knyttes til behandling af personoplysninger på en etisk måde.

([272]) EMD, *K.H. m.fl. mod Slovakiet*, nr. 32881/04, 28. april 2009.

Eksempel: Et universitets forskningsafdeling udfører et eksperiment, hvor den analyserer humørskift hos 50 registrerede. Disse skal registrere deres tanker på et bestemt tidspunkt hver time i et elektronisk dokument. De 50 personer gav deres samtykke til dette bestemte projekt og universitetets specifikke brug af deres oplysninger. Forskningsafdelingen opdager snart, at elektronisk registrering af tanker ville være nyttigt til et andet projekt, som er fokuseret på mental sundhed og ledes af et andet hold. Selvom universitetet som dataansvarlig kunne have brugt de samme oplysninger til det andet holds arbejde uden yderligere trin til at sikre lovligheden af behandlingen af disse oplysninger, oplyste universitet de registrerede herom, da formålene med de to projekter er forenelige, og spurgte om nyt samtykke i medfør af dets kodeks for etisk forskning og princippet for rimelig behandling.

3.1.3. Gennemsigtighed ved behandling

EU's og Europarådets databeskyttelseslovgivning kræver, at behandling af personoplysninger udføres »på en gennemsigtig måde i forhold til den registrerede« ([273]).

Dette princip fastlægger, at den dataansvarlige er forpligtet til at træffe alle passende foranstaltninger til at holde registrerede – som kan være brugere, kunder eller klienter — informeret om, hvordan deres oplysninger anvendes ([274]). Gennemsigtighed kan henvise til oplysningerne givet til den enkelte person inden behandlingen starter ([275]), de oplysninger, som skal være let tilgængelige for registrerede i løbet af behandlingen ([276]), men også til information givet til registrerede efter en anmodning om indsigtsret i deres egne oplysninger ([277]).

Eksempel: I sagen *Haralambie mod Rumænien* ([278]) fik sagsøgeren først adgang til de oplysninger, som det hemmelige politi havde lagret om ham, fem år efter sin anmodning. EMD gentog, at personer, der var genstand for offentlige myndigheders sagsakter, havde en afgørende interesse i at kunne få aktindsigt i dem. Myndighederne havde pligt til at fastlægge en effektiv

([273]) Generel forordning om databeskyttelse, artikel 5, stk. 1, litra a), og den moderniserede konvention 108, artikel 5, stk. 4, litra a), og artikel 8.

([274]) Generel forordning om databeskyttelse, artikel 12.

([275]) *Ibid.*, artikel 13 og 14.

([276]) Artikel 29-Gruppen, *Udtalelse 2/2017 om databehandling på arbejdspladsen*, s. 23.

([277]) Generel forordning om databeskyttelse, artikel 15.

([278]) EMD, *Haralambie mod Rumænien*, nr. 21737/03, 27. oktober 2009.

procedure for aktindsigt i sådanne oplysninger. EMD fandt, at hverken mængden af overførte sagsakter eller mangler i arkivsystemet kunne begrunde, at sagsøgerens anmodning om aktindsigt først blev imødekommet med fem års forsinkelse. Myndighederne havde ikke givet sagsøgeren en effektiv og brugbar procedure for aktindsigt i vedkommendes personlige sagsakter inden for en rimelig periode. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Behandlingsaktiviteter skal forklares for de registrerede på en lettilgængelig måde, som sikrer, at de forstår, hvad der sker med deres oplysninger. Dette betyder, at den registrerede skal kende til det specifikke formål med behandlingen af personoplysninger ved tidspunktet for indsamlingen af personoplysninger ([279]). Gennemsigtighed i behandlingen kræver, at der bruges et klart og forståeligt sprog ([280]). De berørte personer skal være klar over, hvilke risici, regler, garantier og rettigheder der er i forbindelse med behandlingen af deres personoplysninger ([281]).

Europarådets retsorden fastsætter også, at det er obligatorisk, at den dataansvarlige meddeler visse væsentlige oplysninger på en proaktiv måde til de registrerede. Oplysninger om den dataansvarliges (eller de fælles dataansvarliges) navn og adresse, retsgrundlaget og formålet med databehandlingen, kategorierne for de behandlede oplysninger og modtagere samt midler til udøvelse af rettighederne kan tilvejebringes i et vilkårligt passende format (gennem et websted, teknologiske værktøjer på personlige enheder osv.), så længe oplysningerne fremføres for den registrerede på en rimelig og effektiv måde. De fremførte oplysninger skal være lettilgængelige, læsbare, forståelige og tilpasset til de relevante registrerede (for eksempel i et børnevenligt sprog, hvis det er nødvendigt). Alle yderligere oplysninger, som er nødvendige til at sikre rimelig databehandling eller er brugbare til et sådant formål, såsom opbevaringsperioden, viden om årsagen bag databehandlingen eller oplysninger om dataoverførsler til en modtager, som er part eller ikke-part (herunder om den pågældende tredjemand sikrer et passende beskyttelsesniveau eller de foranstaltninger, som den dataansvarlige har truffet for at garantere et sådant passende databeskyttelsesniveau), skal også frembringes ([282]).

([279]) Generel forordning om databeskyttelse, betragtning 39.

([280]) *Ibid*.

([281]) *Ibid*.

([282]) Forklarende rapport til den moderniserede konvention 108, stk. 68.

I medfør af indsigtsretten ([283]) har en registreret efter indgivelse af en anmodning til en dataansvarlig ret til at få at vide, om vedkommendes oplysninger behandles og, i så fald, hvilke oplysninger som behandles ([284]). Derudover skal de personer, hvis oplysninger behandles, i medfør af oplysningspligten ([285]) principielt informeres proaktivt af dataansvarlige eller databehandlere om, bl.a., formål, varighed og behandlingsmidler, inden behandlingsaktiviteten begynder.

Eksempel: Sagen *Smaranda Bara m.fl. mod Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate og Agenția Națională de Administrare Fiscală (ANAF)* II([286]) omhandlede overførsel af personlige skatteoplysninger omkring selvstændiges indkomst fra skattestyrelsen til det nationale sygeforsikringsinstitut i Rumænien, på baggrund af hvilket sygeforsikringsinstituttet krævede efterbetaling af bidrag til sygeforsikringsordningen. EU-Domstolen blev bedt om at afgøre, om den registrerede forudgående skulle være blevet oplyst om identiteten på den dataansvarlige og formålet med videregivelsen af oplysningerne, inden oplysningerne blev behandlet af det nationale sygeforsikringsinstitut. EU-Domstolen fastholdt, at registrerede skal oplyses omkring overførsler eller behandling, når en offentlig myndighed i en medlemsstat videregiver personoplysninger til en anden offentlig myndighed, som efterfølgende behandler disse oplysninger.

Under visse omstændigheder tillades undtagelser fra pligten om at oplyse registrerede om databehandling, og disse diskuteres i detaljer i afsnit 6.1. om den registreredes rettigheder.

([283]) Generel forordning om databeskyttelse, artikel 15.

([284]) Den moderniserede konvention 108, artikel 8 og 9, stk. 1, litra b).

([285]) Generel forordning om databeskyttelse, artikel 13 og 14.

([286]) EU-Domstolen, C-201/14, *Smaranda Bara m.fl. mod Casa Națională de Asigurări de Sănătate m.fl.*, 1. oktober 2015, præmis 28-46.

3.2. Princippet om formålsbegrænsning

Hovedpunkter

- Formålet med databehandlingen skal defineres, inden behandlingen påbegyndes.
- Oplysninger må ikke viderebehandles på en måde, som er i strid med det oprindelige formål, selvom den generelle forordning om databeskyttelse forventer undtagelser til denne regel på baggrund af arkivformål i samfundets interesse, videnskabelige eller historiske forskningsformål og statistiske formål.
- Grundlæggende betyder princippet om formålsbegrænsning, at enhver behandling af personoplysninger skal have et bestemt, veldefineret formål og må kun have yderligere, specificerede formål, der er forenelige med det oprindelige.

Princippet om formålsbegrænsning er et af de grundlæggende principper i europæisk databeskyttelseslovgivning. Det er stærkt knyttet til gennemsigtighed, forudsigelighed og brugerkontrol: Hvis formålet med behandlingen er tilstrækkelig specifikt og klart, så ved enkeltpersoner, hvad de kan forvente, og gennemsigtigheden og retssikkerheden forbedres. Det er ligeledes vigtigt med en tydelig afgrænsning af formålet, for at registrerede effektivt kan udøve deres rettigheder, såsom retten til at gøre indsigelse mod behandling ([287]).

Princippet kræver, at enhver behandling af personoplysninger skal have et bestemt, veldefineret formål og må kun have yderligere formål, der er forenelige med det oprindelige ([288]). Behandlingen af personoplysninger til udefinerede og/eller ubegrænsede formål er derfor ulovligt. Behandlingen af personoplysninger uden et bestemt formål, som bare er baseret på en begrundelse af, at de kan være praktiske i fremtiden, er også ulovligt. Berettigelsen af behandlingen af personoplysninger afhænger af behandlingens formål, som skal være udtrykkeligt, specificeret og legitimt.

Ethvert nyt formål med behandling af oplysninger, som ikke er foreneligt med det oprindelige, skal have sit eget særlige retsgrundlag og kan ikke støtte sig til, at oplysningerne oprindeligt blev indhentet eller behandlet til et andet legitimt formål. Legitim behandling er derfor begrænset til det oprindeligt specificerede formål, og ethvert nyt behandlingsformål kræver et særskilt, nyt retsgrundlag. For eksempel skal videregivelse af personoplysninger til tredjemænd til et nyt formål overvejes

([287]) Artikel 29-Gruppen (2013), Udtalelse 3/2013 om formålsbegrænsning, WP 203, 2. april 2013.

([288]) Generel forordning om databeskyttelse, artikel 5, stk. 1, litra b).

nøje, da denne overdragelse sandsynligvis kræver et yderligere retsgrundlag, som adskiller sig fra det for indsamlingen af oplysningerne.

Eksempel: Et flyselskab indsamler oplysninger fra passagererne ved booking for at kunne operere flyvningen korrekt. Flyselskabet skal have oplysninger om: passagerernes flysæder, særlige fysiske begrænsninger, f.eks. kørestolsbehov, og særlige krav til maden, f.eks. kosher- eller halalmad. Hvis flyselskaber anmodes om at overføre disse oplysninger, som er en del af passagerlisteoplysningerne, til immigrationsmyndighederne i ankomstlufthavnen, anvendes disse oplysninger til immigrationskontrol, som er et andet formål end det oprindelige med dataindsamlingen. Overførsel af disse oplysninger til en immigrationsmyndighed kræver derfor et nyt og særskilt retsgrundlag.

For at fastlægge omfanget af og begrænsningerne for et bestemt formål benytter den moderniserede konvention 108 og den generelle forordning om databeskyttelse begrebet forenelighed: Det er tilladt at anvende oplysninger til forenelige formål på grundlag af det oprindelige retsgrundlag. Viderebehandling af oplysningerne må derfor ikke udføres på en måde, som er uventet, upassende eller betænkeligt for den registrerede ([289]). Ved vurdering af, om viderebehandlingen er forenelig, skal den dataansvarlige (blandt andet) tage hensyn til følgende:

- enhver forbindelse mellem disse formål og formålet med den påtænkte viderebehandling
- den sammenhæng, som personoplysningerne er blevet indsamlet i, navnlig de registreredes rimelige forventninger til den videre anvendelse heraf på grundlag af deres forhold til den dataansvarlige
- personoplysningernes art
- konsekvenserne af den påtænkte viderebehandling for de registrerede

([289]) Forklarende rapport til den moderniserede konvention 108, stk. 49.

- tilstedeværelsen af fornødne garantier i forbindelse med både de oprindelige og de påtænkte yderligere behandlingsaktiviteter([290]). Dette kunne for eksempel gennemføres via kryptering eller pseudonymisering.

Eksempel: Virksomheden Sunshine har indsamlet og lagret CRM-oplysninger (oplysninger om forvaltning af kunderelationer) om sine kunder. Den overfører derefter disse oplysninger til en markedsføringsvirksomhed, Moonlight, som ønsker at bruge disse oplysninger i andre virksomheders markedsføringskampagner. Sunshines overførsel af oplysninger til brug i andre virksomheders markedsføring er en viderebehandling af oplysninger til et nyt formål, som er uforeneligt med CRM, der var virksomheden Sunshines oprindelige formål med indsamlingen af kundedataene. Overførslen af oplysninger til virksomheden Moonlight skal derfor have et særskilt retsgrundlag.

I modsætning dertil accepteres virksomheden Sunshines brug af CRM-dataene til egne markedsføringsformål, dvs. udsendelsen af markedsføringsbudskaber til virksomhedens egne kunder vedrørende dens egne produkter, generelt som et foreneligt formål.

Den generelle forordning om databeskyttelse og den moderniserede konvention 108 erklærer, at »viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål« anses *a priori* som værende foreneligt med det oprindelige formål ([291]). Der skal dog være fastlagt passende garantier, såsom anonymisering, kryptering eller pseudonymisering af oplysningerne samt begrænsning af adgang hertil, ved viderebehandling af personoplysninger ([292]). Den generelle forordning om databeskyttelse tilføjer, at når »den registrerede har givet samtykke, eller behandlingen er baseret på EU-retten eller medlemsstaternes nationale ret, som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund med henblik på at beskytte navnlig vigtige målsætninger af generel samfundsinteresse, bør den dataansvarlige kunne

([290]) Generel forordning om databeskyttelse, betragtning 50, og artikel 6, stk. 4, og forklarende rapport til den moderniserede konvention 108, stk. 49.

([291]) Generel forordning om databeskyttelse, artikel 5, stk. 1, litra b), og den moderniserede konvention 108, artikel 5, stk. 4, litra b). Et eksempel på sådanne nationale bestemmelser er den østrigske lov om databeskyttelse (*Datenschutzgesetz*), Østrigs lovtidende I nr. 165/1999, stk. 46.

([292]) Generel forordning om databeskyttelse, artikel 6, stk. 4, den moderniserede konvention 108, artikel 5, stk. 4, litra b), og forklarende rapport til den moderniserede konvention 108, stk. 50.

viderebehandle personoplysningerne uafhængigt af formålenes forenelighed« ([293]). Ved udførelse af viderebehandling skal den registrerede derfor oplyses om formålene samt vedkommendes rettigheder, såsom retten til at gøre indsigelse ([294]).

Eksempel: Virksomheden Sunshine har indsamlet og lagret CRM-oplysninger (oplysninger om forvaltning af kunderelationer) om sine kunder. Sunshines senere brug af disse oplysninger i en statistisk analyse af kundernes indkøbsmønstre vil kunne tillades, da statistiske analyser er et foreneligt formål. Det er ikke nødvendigt med yderligere retsgrundlag, såsom de registreredes samtykke. Ved viderebehandling af personoplysningerne til statistiske formål skal Sunshine dog sikre de fornødne garantier for den registreredes rettigheder og friheder. De tekniske og organisatoriske foranstaltninger, som Sunshine skal implementere, kan omfatte pseudonymisering.

3.3. Princippet om dataminimering

Hovedpunkter

- Databehandling skal begrænses til det, der er nødvendigt til at opfylde et legitimt formål.
- Behandlingen af personoplysninger skal kun finde sted, når behandlingens formål ikke kan opfyldes via andre midler på rimelig vis.
- Behandling af oplysninger må ikke være et uforholdsmæssigt indgreb i de foreliggende interesser, rettigheder og friheder.

Der må kun behandles oplysninger i et omfang, som er tilpas, relevant og ikke overdrevet i forhold til det formål, de indsamles og/eller viderebehandles til ([295]). Kategorierne af oplysninger, som er valgt til behandling, skal være nødvendige til at opnå det erklærede overordnede mål med behandlingsaktiviteterne, og en dataansvarlig skal strengt begrænse indsamlingen af oplysninger til det, som er direkte relevant for behandlingens specifikke formål.

([293]) Generel forordning om databeskyttelse, betragtning 50.

([294]) *Ibid.*

([295]) Den moderniserede konvention 108, artikel 5, stk. 4, litra c), og generel forordning om databeskyttelse, artikel 5, stk. 1, litra c).

Eksempel: I *Digital Rights Ireland*-sagen ([296]) overvejede EU-Domstolen gyldigheden af datalagringsdirektivet, som var rettet mod at harmonisere nationale bestemmelser om lagring af personoplysninger, der var genereret eller behandlet af offentligt tilgængelige elektroniske kommunikationstjenester eller -netværk, for deres eventuelle overførsel til kompetente myndigheder med henblik på bekæmpelse af grov kriminalitet, såsom organiseret kriminalitet og terrorisme. Selvom dette var et formål, der faktisk forfølger et mål af almen interesse, vurderede man, at den måde, som direktivet omfattede »alle personer og alle elektroniske kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om at bekæmpe grov kriminalitet«, var problematisk ([297]).

Derudover er det ved anvendelse af særlig privatlivsfremmende teknologi nogle gange muligt helt at undgå brugen af personoplysninger eller at bruge foranstaltninger til at reducere muligheden for at henføre oplysninger til en registreret (for eksempel gennem pseudonymisering), hvilket resulterer i en privatlivsvenlig løsning. Dette er især hensigtsmæssigt i mere omfattende behandlingssystemer.

Eksempel: Et byråd tilbyder borgere, der regelmæssigt benytter byens offentlige transportsystem, et chipkort mod et gebyr. På kortet er borgerens navn skrevet på kortets overflade, og det er også registreret i elektronisk form i chippen. Når en bus eller sporvogn benyttes, skal chipkortet føres gennem en kortlæser, der f.eks. er anbragt i bussen eller sporvognen. De oplysninger, der aflæses af kortlæseren, kontrolleres i forhold til en database, der indeholder navnene på alle de borgere, der har købt rejsekortet.

Dette system overholder ikke princippet om dataminimering på en optimal måde: Det kan kontrolleres, om en person har lov til at bruge transportsystemet, uden at sammenligne personoplysninger på kortchippen med en database. Det ville f.eks. være tilstrækkeligt at have et særligt elektronisk billede, som f.eks. en stregkode, i kortchippen, som ved aflæsning i kortlæseren ville bekræfte, om kortet er gyldigt eller ej. Et sådant system ville ikke registrere, hvem der benyttede hvilket transportmiddel på hvilket

([296]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014.

([297]) *Ibid.*, præmis 44 og 57.

tidspunkt. Dette ville være den optimale løsning med hensyn til princippet om dataminimering, da dette princip medfører en forpligtelse til at minimere indsamlingen af personoplysninger.

Artikel 5, stk. 1, i den moderniserede konvention 108 indeholder et proportionalitetskrav ved behandling af personoplysninger i forbindelse med det forfulgte legitime mål. Der skal være en rimelig afvejning af alle berørte interesser under alle behandlingens faser. Dette betyder, at personoplysninger, som er passende og relevante, men ville medføre et uforholdsmæssigt indgreb i de foreliggende grundlæggende rettigheder og frihedsrettigheder, skal betragtes som unødvendige ([298]).

3.4. Princippet om oplysningernes rigtighed

Hovedpunkter

- Princippet om oplysningernes rigtighed skal implementeres af den dataansvarlige i alle behandlingsaktiviteter.
- Ukorrekte oplysninger skal omgående slettes eller berigtiges.
- Det kan være nødvendigt at kontrollere oplysninger regelmæssigt og holde dem ajourført for at sikre nøjagtighed.

En dataansvarlig, som besidder personoplysninger, skal ikke benytte disse oplysninger uden at tage skridt mod at med rimelig sikkerhed kunne sikre, at oplysningerne er nøjagtige og ajourført ([299]).

Forpligtelsen om at sikre oplysningers nøjagtighed skal forstås sammen med databehandlingens formål.

([298]) Forklarende rapport til den moderniserede konvention 108, stk. 52, og generel forordning om databeskyttelse, artikel 5, stk. 1, litra c).

([299]) Generel forordning om databeskyttelse, artikel 5, stk. 1, litra d), og den moderniserede konvention 108, artikel 5, stk. 4, litra d).

Eksempel: I *Rijkeboer*-sagen ([300]) undersøgte EU-Domstolen en anmodning fra en nederlandsk statsborger, der ville indhente oplysninger fra den lokale myndighed i Amsterdam omkring identiteten af de personer, som havde fået meddelt fortegnelser omkring statsborgeren, som den lokale myndighed opbevarede, i de to foregående år, og omkring indholdet af de meddelte oplysninger. EU-Domstolen fastslog, at retten »til respekt for privatlivets fred indebærer, at den registrerede skal kunne have sikkerhed for, at hans personoplysninger behandles korrekt og lovligt, dvs. navnlig, at basisoplysningerne om den pågældende er korrekte og videregives til nogen, som er berettiget til at modtage dem«. EU-Domstolen henviste derefter til præamblen i databeskyttelsesdirektivet, som fastlægger, at registrerede skal have ret til indsigt i deres personoplysninger for at kunne efterprøve dem ([301]).

Der kan også være tilfælde, hvor ajourføring af lagrede oplysninger forbydes ved lov, da formålet med oplysningernes opbevaring primært er at dokumentere hændelser som »historiske øjebliksbilleder«.

Eksempel: Patientjournalen for en operation må ikke ændres, eller ajourføres, selv hvis oplysninger deri senere viser sig at være forkerte. Under sådanne omstændigheder må der kun laves tilføjelser til journalens bemærkninger, hvis de tydeligt markeres som bidrag, der er foretaget på et senere tidspunkt.

På den anden side er der situationer, hvor det er absolut nødvendigt at ajourføre og regelmæssigt kontrollere oplysningernes nøjagtighed grundet de potentielle skader, som den registrerede måtte lide, hvis oplysningerne forbliver ukorrekte.

Eksempel: Hvis nogen gerne vil indgå en kreditaftale med en bank, undersøger banken normalt den potentielle kundes kreditværdighed. Der findes specielle databaser til dette formål, som indeholder oplysninger om privatpersoners kredithistorik. Hvis en sådan database indeholder ukorrekte eller forældede oplysninger om en enkeltperson, kan det have negative følger for denne person. Dataansvarlige for sådanne databaser skal derfor gøre en særlig indsats for at følge princippet om oplysningernes rigtighed.

([300]) EU-Domstolen, C-553/07, *College van burgemeester en wethouders van Rotterdam mod M. E. E. Rijkeboer*, 7. maj 2009.

([301]) Tidligere betragtning 41, præamblen til direktiv 95/46/EF.

3.5. Princippet om opbevaringsbegrænsning

Hovedpunkter

- Princippet om opbevaringsbegrænsning betyder, at personoplysninger skal slettes eller anonymiseres, så snart de ikke længere er nødvendige til de formål, de blev indsamlet til.

Artikel 5, stk. 1, litra e), i GDPR samt artikel 5, stk. 4, litra e), i den moderniserede konvention 108 kræver, at personoplysninger »opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles«. Oplysningerne skal derfor slettes eller anonymiseres, når disse formål er opfyldt. Til dette formål »bør den dataansvarlige indføre tidsfrister for sletning eller periodisk gennemgang«, således at oplysningerne ikke opbevares i længere tid end nødvendigt ([302]).

I *S. og Marper* konkluderede EMD, at de centrale principper i Europarådets relevante instrumenter og de andre kontraherende parters lov og praksis kræver, at opbevaringen af oplysninger er proportionel med indsamlingens formål og er tidsmæssigt begrænset, især på politiområdet ([303]).

Eksempel: I *S. og Marper* ([304]) fastslog EMD, at opbevaring af de to sagsøgeres fingeraftryk, celleprøver og DNA-profiler på ubestemt tid var uforholdsmæssigt og unødvendigt i et demokratisk samfund, siden straffesagerne mod begge sagsøgere var blevet afsluttet med henholdsvist en frikendelse og en ophævelse.

Tidsbegrænsningen for opbevaring af personoplysninger gælder kun for oplysninger lagret i en form, som tillader identifikation af registrerede. Lovlig opbevaring af oplysninger, som ikke længere er nødvendige, kunne derfor opnås ved at anonymisere oplysninger.

([302]) Generel forordning om databeskyttelse, betragtning 39.

([303]) EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 4. december 2008. Se for eksempel også: EMD, *M.M. mod Det Forenede Kongerige*, nr. 24029/07, 13. november 2012.

([304]) EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 4. december 2008.

Arkiver med oplysninger i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål må opbevares i længere perioder, hvis disse oplysninger udelukkende anvendes til ovennævnte formål ([305]). Der skal gennemføres passende tekniske og organisatoriske foranstaltninger til den løbende opbevaring og brug af personoplysninger til at garantere den registreredes rettigheder og friheder.

Den moderniserede konvention 108 tillader også undtagelser fra princippet om opbevaringsbegrænsning på den betingelse, at de er fastlagt ved lov, overholder det væsentligste indhold af de grundlæggende rettigheder og friheder og er nødvendige og proportionale til at forfølge et begrænset antal legitime mål ([306]). Disse omfatter bl.a. beskyttelse af den nationale sikkerhed, efterforskning og retsforfølgning af strafbare handlinger, fuldbyrdelse af strafferetlige sanktioner, beskyttelse af den registrerede og af andres rettigheder og grundlæggende friheder.

Eksempel: I *Digital Rights Ireland*-sagen ([307]) overvejede EU-Domstolen gyldigheden af datalagringsdirektivet, som var rettet mod at harmonisere nationale bestemmelser om lagring af personoplysninger, der var genereret eller behandlet af offentligt tilgængelige elektroniske kommunikationstjenester eller -netværk, med henblik på bekæmpelse af grov kriminalitet, såsom organiseret kriminalitet og terrorisme. Datalagringsdirektivet foreskriver en datalagringsperiode på »mindst seks måneder, uden at der på nogen måde foretages en sondring mellem de kategorier af data, som er fastsat i dette direktivs artikel 5, efter deres relevans for det mål, som forfølges, eller afhængigt af, hvilke personer der er berørt« ([308]). EU-Domstolen fremhævede også manglen af objektive kriterier i datalagringsdirektivet, på baggrund af hvilken den eksakte datalagringsperiode – som kan variere mellem mindst seks måneder og maksimalt 24 måneder –skal fastlægges for at sikre, at denne periode er begrænset til det strengt nødvendige ([309]).

([305]) Generel forordning om databeskyttelse, artikel 5, stk. 1, litra e), og den moderniserede konvention 108, artikel 5, stk. 4, litra b), og artikel 11, stk. 2.

([306]) Den moderniserede konvention 108, artikel 11, stk. 1, og forklarende rapport til den moderniserede konvention 108, stk. 91-98.

([307]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014.

([308]) *Ibid.*, præmis 63.

([309]) *Ibid.*, præmis 64.

3.6. Princippet om datasikkerhed

Hovedpunkter

- Det er nødvendigt, at personoplysninger er sikre og fortrolige for at forhindre negative virkninger for den registrerede.
- Sikkerhedsforanstaltninger kan være af en teknisk og/eller organisatorisk karakter.
- Pseudonymisering er en proces, der kan beskytte personoplysninger.
- Sikkerhedsforanstaltningers hensigtsmæssighed skal vurderes ud fra den enkelte sag og gennemgås regelmæssigt.

Princippet om datasikkerhed kræver, at passende tekniske eller organisatoriske foranstaltninger gennemføres ved behandling af personoplysninger for at beskytte oplysningerne mod uhensigtsmæssig, uautoriseret eller ulovlig adgang, brug, modifikation, videregivelse, tab, destruktion eller skade ([310]). GDPR fastlægger, at den dataansvarlige og databehandleren skal tage hensyn til »det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder« ved gennemførelsen af sådanne foranstaltninger ([311]). På baggrund af den enkelte sags omstændigheder kan passende tekniske og organisatoriske foranstaltninger for eksempel omfatte pseudonymisering og kryptering af personoplysninger og/eller regelmæssig afprøvning og evaluering af foranstaltningernes effektivitet for at sikre, at databehandlingen er sikker ([312]).

Som forklaret i afsnit 2.1.1. betyder pseudonymisering af oplysninger, at personoplysningernes identifikatorer – som gør det muligt at identificere den registrerede – erstattes med et pseudonym, og disse identifikatorer holdes adskilt, ved brug af tekniske eller organisatoriske foranstaltninger. Processen for pseudonymisering må ikke forveksles med processen for anonymisering, hvor alle henvisninger, der kan identificere personen, fjernes.

([310]) Generel forordning om databeskyttelse, betragtning 39, og artikel 5, stk. 1, litra f), og den moderniserede konvention 108, artikel 7.

([311]) Generel forordning om databeskyttelse, artikel 32, stk. 1.

([312]) *Ibid.*

Eksempel: Sætningen »Charles Spencer, født den 3. april 1967, er far i en familie på fire børn, to drenge og to piger« kan for eksempel pseudonymiseres som følger:

»C.S. 1967 er far i en familie på fire børn, to drenge og to piger«

»324 er far i en familie på fire børn, to drenge og to piger« eller

»YESz320l er far i en familie på fire børn, to drenge og to piger«.

Brugere, som tilgår pseudonymiserede oplysninger, har normalt ikke mulighed for at identificere »Charles Spencer, født den 3. april 1967« ud fra »324« eller »YESz3201«. Der er derfor en større sandsynlighed for, at sådanne oplysninger er sikret mod misbrug.

Det første eksempel er dog mindre sikkert. Hvis sætningen »C.S. 1967 er far i en familie på fire børn, to drenge og to piger« benyttes i den lille landsby, hvor Charles Spencer bor, så ville han være let at identificere. Pseudonymiseringsmetoden kan påvirke databeskyttelsens effektivitet.

Personoplysninger med krypterede identifikatorer eller identifikatorer, der er lagret særskilt, benyttes i mange sammenhænge til at hemmeligholde personers identitet. Dette er særligt praktisk, når dataansvarlige skal sikre, at de har med de samme registrerede at gøre, men ikke kræver, eller ikke burde have, de registreredes rigtige identiteter. Dette er for eksempel tilfældet, når en forsker undersøger en sygdoms forløb i patienter, hvis identitet kun kendes af hospitalet, hvor de behandles, og hvorfra forskeren indhenter de pseudonymiserede patientjournaler. Pseudonymisering er derfor et stærkt led i kæden med privatlivsfremmende teknologier. Det kan fungere som et vigtigt element ved gennemførelse af indbygget privatlivsbeskyttelse. Dette betyder, at databeskyttelse er indbygget i databehandlingssystemers struktur.

Artikel 25 i GDPR, som omhandler databeskyttelse gennem design, henviser udtrykkeligt til pseudonymisering som et eksempel på en passende teknisk og organisatorisk foranstaltning, som dataansvarlige bør gennemføre for at overholde databeskyttelsesprincipperne og integrere de fornødne garantier. Herved opfylder dataansvarlige forordningens krav og vil beskytte registreredes rettigheder ved behandling af deres personoplysninger.

Overholdelse af et godkendt adfærdskodeks eller en godkendt certificeringsmekanisme kan bruges til at påvise overholdelse af kravene til behandlingssikkerhed ([313]). I sin udtalelse om konsekvenser for databeskyttelse som følge af behandlingen af passagerlisteoplysninger giver Europarådet andre eksempler på passende sikkerhedsforanstaltninger til at beskytte personoplysninger i systemer med passagerlisteoplysninger. Disse omfatter opbevaring af oplysninger i et sikkert fysisk miljø, begrænsning af adgangskontrol via lagdelte login og beskyttelse af dataoverførsler med stærk kryptografi ([314]).

Eksempel: Sociale netværkssider og e-mailudbydere gør det muligt for brugere at tilføje et ekstra lag af datasikkerhed til de tjenester, de udbyder, ved indførelsen af totrinsbekræftelse. Brugere skal indtaste et personligt kodeord og udføre en yderligere registrering for at få adgang til deres personlige konto. Sidstnævnte kan for eksempel være indtastning af en sikkerhedskode, som er sendt til mobiltelefonnummeret knyttet til den personlige konto. På denne måde giver totrinsbekræftelse en bedre beskyttelse mod uautoriseret adgang og hacking af personlige konto og de personlige oplysninger deri.

Den forklarende rapport til den moderniserede konvention 108 indeholder flere eksempler på passende garantier, såsom gennemførelse af en tavshedspligt eller vedtagelse af kvalificerede tekniske sikkerhedsforanstaltninger, såsom datakryptering ([315]). Ved fastlæggelse af specifikke sikkerhedsforanstaltninger skal den dataansvarlige – eller, om relevant, databehandleren – tage hensyn til flere elementer, såsom karakteren og mængden af de behandlede personoplysninger, potentielle skadelige konsekvenser for registrerede og behovet for at begrænse dataadgang ([316]). De aktuelle datasikkerhedsmetoder og teknikker for databehandling skal overvejes ved implementering af passende sikkerhedsforanstaltninger. Omkostningerne til sådanne foranstaltninger skal være proportionale med alvorligheden af og sandsynligheden for potentielle risici. Det er nødvendigt med en regelmæssig gennemgang af sikkerhedsforanstaltningerne, så de kan ajourføres som nødvendigt ([317]).

([313]) *Ibid.*, artikel 32, stk. 3.

([314]) Europarådet, det rådgivende udvalg for konvention 108, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19. august 2016, s. 9.

([315]) Forklarende rapport til den moderniserede konvention 108, stk. 56.

([316]) *Ibid.*, stk. 62.

([317]) *Ibid.*, præmis 63.

I tilfælde, hvor et brud på persondatasikkerheden finder sted, kræver både den moderniserede konvention 108 og GDPR, at den dataansvarlige meddeler den kompetente tilsynsmyndighed om bruddet, som truer enkeltpersoners rettigheder og friheder, uden unødig forsinkelse ([318]). Der findes en lignende kommunikationsforpligtelse for den registrerede, når bruddet på persondatasikkerheden med sandsynlighed udgør en stor risiko for vedkommendes rettigheder og friheder ([319]). Meddelelse af sådanne brud til registrerede skal være udformet i et klart og almindeligt sprog ([320]). Hvis databehandleren bliver opmærksom på et brud på persondatasikkerheden, skal den dataansvarlige omgående meddeles ([321]). I visse situationer kan undtagelser fra underretningsforpligtelsen være gældende. For eksempel er det ikke et krav, at den dataansvarlige meddeler tilsynsmyndigheden, når »bruddet på persondatasikkerheden sandsynligvis ikke indebærer risiko for fysiske personers rettigheder eller frihedsrettigheder« ([322]). Det er heller ikke nødvendigt at meddele den registrerede, når gennemførte sikkerhedsforanstaltninger gør oplysningerne uforståelige for ikke-autoriserede personer, eller når efterfølgende foranstaltninger sikrer, at den høje risiko sandsynligvis ikke længere er reel ([323]). Hvis meddelelse af et brud på persondatasikkerheden til de registrerede ville omfatte en uforholdsmæssig indsats fra den dataansvarlige, kan en offentlig meddelelse eller tilsvarende foranstaltning sikre, at »de registrerede underrettes på en tilsvarende effektiv måde« ([324]).

3.7. Princippet om ansvarlighed

Hovedpunkter

- Ansvarlighed kræver, at dataansvarlige og databehandlere aktivt og løbende gennemfører foranstaltninger til at fremme og sikre databeskyttelse i forbindelse med deres behandlingsaktiviteter.

([318]) Den moderniserede konvention 108, artikel 7, stk. 2, og generel forordning om databeskyttelse, artikel 33, stk. 1.

([319]) Den moderniserede konvention 108, artikel 7, stk. 2, og generel forordning om databeskyttelse, artikel 34, stk. 1.

([320]) Generel forordning om databeskyttelse, artikel 34, stk. 2.

([321]) *Ibid.*, artikel 33, stk. 1.

([322]) *Ibid.*, artikel 32, stk. 1.

([323]) *Ibid.*, artikel 34, stk. 3, litra a) og b).

([324]) *Ibid.*, artikel 34, stk. 3, litra c).

- Dataansvarlige og databehandlere er ansvarlige for, at deres behandlingsaktiviteter overholder databeskyttelseslovgivningen, og for at overholde deres gældende forpligtelser.
- Dataansvarlige skal kunne påvise overholdelse af bestemmelserne om databeskyttelse for registrerede, den brede offentlighed og tilsynsmyndigheder på ethvert tidspunkt. Databehandlere skal også overholde visse forpligtelser, som udelukkende er knyttet til ansvarlighed (såsom føring af fortegnelser over behandlingsaktiviteter og udpegelse af en databeskyttelsesrådgiver).

GDPR og den moderniserede konvention 108 fastlægger, at den dataansvarlige er ansvarlig for og skal kunne påvise overholdelse af principperne for behandling af personoplysninger, som er beskrevet i dette kapitel ([325]). Til dette formål skal den dataansvarlige implementere passende tekniske og organisatoriske foranstaltninger ([326]). Selvom princippet om ansvarlighed i artikel 5, stk. 2, i GDPR kun er rettet mod dataansvarlige, forventes det også, at databehandlere er ansvarlige, siden de skal overholde flere forpligtelser, og de er tæt knyttet til ansvarlighed.

EU's og Europarådets databeskyttelseslovgivning fastlægger også, at den dataansvarlige er ansvarlig for og skal sikre overholdelse af principperne for databeskyttelse diskuteret i afsnit 3.1 til 3.6. ([327]). Artikel 29-Gruppen påpeger, at »typerne af procedurer og mekanismer [vil] variere, alt efter risiciene ved at behandle de pågældende oplysninger og arten af disse oplysninger« ([328]).

Dataansvarlige kan fremme overholdelse af dette krav på forskellige måder, som omfatter:

- registrering af behandlingsaktiviteter og videregivelse heraf til tilsynsmyndigheden efter anmodning ([329])
- udpegelse af en databeskyttelsesrådgiver, som er indblandet i alle spørgsmål vedrørende beskyttelse af personoplysninger, under visse omstændigheder ([330])

([325]) *Ibid.*, artikel 5, stk. 2, og den moderniserede konvention 108, artikel 10, stk. 1.

([326]) Generel forordning om databeskyttelse, artikel 24.

([327]) *Ibid.*, artikel 5, stk. 2, og den moderniserede konvention 108, artikel 10, stk. 1.

([328]) Artikel 29-Gruppen (2010), Udtalelse 3/2010 om princippet om ansvarlighed, WP 173, Bruxelles, 13. juli 2010, stk. 12.

([329]) Generel forordning om databeskyttelse, artikel 30.

([330]) *Ibid.*, artikel 37-39.

- udførelse af konsekvensanalyser vedrørende databeskyttelse for behandlingstyper, som med sandsynlighed medfører en høj risiko for fysiske personers rettigheder og friheder ([331])

- sikring af databeskyttelse gennem design og gennem standardindstillinger ([332])

- implementering af modaliteter og procedurer for registreredes udøvelse af deres rettigheder ([333])

- overholdelse af godkendte adfærdskodekser eller certificeringsmekanismer ([334]).

Selvom princippet om ansvarlighed i GDPR's artikel 5, stk. 2, ikke er rettet mod databehandlere som sådan, er der bestemmelser vedrørende ansvarlighed, som også indeholder forpligtelser for dem, såsom føring af fortegnelser over behandlingsaktiviteter og udpegelse af en databeskyttelsesrådgiver for alle behandlingsaktiviteter, der kræver en sådan ([335]). Databehandlere skal også sikre, at alle foranstaltninger, som er nødvendige til at sikre oplysningernes sikkerhed, er implementeret ([336]). Den retsligt bindende kontrakt mellem den dataansvarlige og databehandleren skal fastsætte, at databehandleren skal bistå den dataansvarlige med nogle af kravene til overholdelse, såsom ved udførelse af en konsekvensanalyse vedrørende databeskyttelse eller underretning af den dataansvarlige om et brud på persondatasikkerheden, så snart de gøres opmærksom herpå ([337]).

Organisationen for Økonomisk Samarbejde og Udvikling (OECD) vedtog retningslinjer for beskyttelse af privatlivets fred i 2013, hvori man fremhævede, at registeransvarlige har et stort ansvar for at få databeskyttelse til at fungere i praksis. Retningslinjerne udgør et ansvarlighedsprincip, som fastlægger, at en dataansvarlig er ansvarlig for at overholde foranstaltninger, som gennemfører de væsentlige principper, der er nævnt i retningslinjerne ([338]).

([331]) *Ibid*., artikel 35, og den moderniserede konvention 108, artikel 10, stk. 2.

([332]) Generel forordning om databeskyttelse, artikel 25, og den moderniserede konvention 108, artikel 10, stk. 2 og 3.

([333]) *Ibid*., artikel 12 og 24.

([334]) *Ibid*., artikel 40 og 42.

([335]) *Ibid*., artikel 5, stk. 2, artikel 30 og 37.

([336]) *Ibid*., artikel 28, stk. 3, litra c).

([337]) *Ibid*., artikel 28, stk. 3, litra d).

([338]) OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, Artikel 14.

Eksempel: Et eksempel på lovgivning, som understreger princippet om ansvarlighed, er ændringen ([339]) af e-databeskyttelsesdirektivet 2002/58/EF fra 2009. I henhold til artikel 4 som ændret pålægges dataansvarlige en forpligtelse til at »gennemføre en sikkerhedspolitik for behandling af personoplysninger«. For så vidt angår sikkerhedsbestemmelserne i nævnte direktiv, besluttede lovgiveren, at det var nødvendigt at indføre et udtrykkeligt krav om at fastlægge og indføre en sikkerhedspolitik.

I henhold til Artikel 29-Gruppens udtalelse ([340]) er essensen af ansvarlighed den dataansvarliges forpligtelse til:

- at gennemføre foranstaltninger, der — under normale omstændigheder — garanterer, at databeskyttelsesreglerne overholdes i forbindelse med behandlingsaktiviteter

- over for registrerede og tilsynsmyndigheder at kunne dokumentere, hvilke foranstaltninger der er iværksat for at overholde databeskyttelsesreglerne.

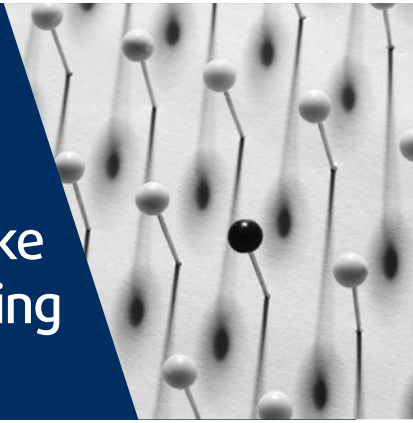
Princippet om ansvarlighed kræver således, at de dataansvarlige aktivt påviser overensstemmelse og ikke blot afventer, at registrerede eller tilsynsmyndigheder påpeger mangler.

([339]) Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse, EUT L 337 af 18. december 2009, s. 11.

([340]) Artikel 29-Gruppen (2010), *Udtalelse 3/2010 om princippet om ansvarlighed*, WP 173, Bruxelles, 13. juli 2010.

4

Reglerne i den europæiske databeskyttelseslovgivning



EU	Omhandlede emner	Europarådet
Regler om lovlig behandling af oplysninger		
Generel forordning om databeskyttelse, artikel 6, stk. 1, litra a) EU-Domstolen, C-543/09, *Deutsche Telekom AG mod Bundesrepublik Deutschland*, 2011 EU-Domstolen, C-536/15, *Tele2 (Netherlands) BV m.fl. mod Autoriteit Consument en Markt (ACM)*, 2017	**Samtykke**	Henstilling om profilering, artikel 3.4, litra b), og artikel 3.6 Den moderniserede konvention 108, artikel 5, stk. 2
Generel forordning om databeskyttelse, artikel 6, stk. 1, litra b)	**(Præ-)kontraktligt forhold**	Henstilling om profilering, artikel 3.4, litra b)
Generel forordning om databeskyttelse, artikel 6, stk. 1, litra c)	**Den dataansvarliges retlige forpligtelser**	Henstilling om profilering, artikel 3.4, litra a)
Generel forordning om databeskyttelse, artikel 6, stk. 1, litra d)	**Den registreredes vitale interesser**	Henstilling om profilering, artikel 3.4, litra b)
Generel forordning om databeskyttelse, artikel 6, stk. 1, litra e) EU-Domstolen, C-524/06, *Heinz Huber mod Bundesrepublik Deutschland* [GC], 2008	**Samfundsinteresser og offentlig myndigheds-udøvelse**	Henstilling om profilering, artikel 3.4, litra b)

EU	Omhandlede emner	Europarådet
Generel forordning om databeskyttelse, artikel 6, stk. 1, litra f) EU-Domstolen, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde mod Rīgas pašvaldības SIA »Rīgas satiksme«*, 2017 EU-Domstolen, forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado*, 2011	**Andres legitime interesser**	Henstilling om profilering, artikel 3.4, litra b) EMD, *Y mod Tyrkiet*, nr. 648/10, 2015
Generel forordning om databeskyttelse, artikel 6, stk. 4	**Undtagelser fra formåls-begrænsning: yderligere behandling til andre formål**	Den moderniserede konvention 108, artikel 5, stk. 4, litra b)
Regler om lovlig behandling af følsomme oplysninger		
Generel forordning om databeskyttelse, artikel 9, stk. 1	**Generelt forbud mod behandling**	Den moderniserede konvention 108, artikel 6
Generel forordning om databeskyttelse, artikel 9, stk. 2	**Undtagelser fra det generelle forbud**	Den moderniserede konvention 108, artikel 6
Regler om sikker behandling		
Generel forordning om databeskyttelse, artikel 32	**Forpligtelse om at sikre sikker behandling**	Den moderniserede konvention 108, artikel 7, stk. 1 EMD, *I mod Finland*, nr. 20511/03, 2008
Generel forordning om databeskyttelse, artikel 28 og 32, stk. 1, litra b)	**Forpligtelse om fortrolighed**	Den moderniserede konvention 108, artikel 7, stk. 1
Generel forordning om databeskyttelse, artikel 34 Direktiv om databeskyttelse inden for elektronisk kommunikation, artikel 4, stk. 2	**Meddelelser om brud på person-datasikkerheden**	Den moderniserede konvention 108, artikel 7, stk. 2
Regler om ansvarlighed og fremme af overholdelse		
Generel forordning om databeskyttelse, artikel 12, 13 og 14	**Gennemsigtighed generelt**	Den moderniserede konvention 108, artikel 8

EU	Omhandlede emner	Europarådet
Generel forordning om databeskyttelse, artikel 37, 38 og 39	Databeskyttelses-rådgivere	Den moderniserede konvention 108, artikel 10, stk. 1
Generel forordning om databeskyttelse, artikel 30	Fortegnelser over behandlings-aktiviteter	
Generel forordning om databeskyttelse, artikel 35 og 36	Konsekvensanalyse og forudgående høring	Den moderniserede konvention 108, artikel 10, stk. 2
Generel forordning om databeskyttelse, artikel 33 og 34	Meddelelser om brud på person-datasikkerheden	Den moderniserede konvention 108, artikel 7, stk. 2
Generel forordning om databeskyttelse, artikel 40 og 41	Adfærdskodekser	
Generel forordning om databeskyttelse, artikel 42 og 43	Certificering	
Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger		
Generel forordning om databeskyttelse, artikel 25, stk. 1, litra a)	Databeskyttelse gennem design	Den moderniserede konvention 108, artikel 10, stk. 2
Generel forordning om databeskyttelse, artikel 25, stk. 1, litra b)	Databeskyttelse gennem standardindstillinger	Den moderniserede konvention 108, artikel 10, stk. 3

Principper er nødvendigvis af generel karakter. Deres anvendelse i konkrete situationer giver mulighed for fortolkning og valg af hjælpemidler. **Europarådets retsorden** overlader det til parterne i den moderniserede konvention 108 at præcisere disse muligheder for fortolkning i deres nationale lovgivning. I **EU-retten** er situationen en anden. For at sikre databeskyttelse i det indre marked fandt man det nødvendigt at fastlægge detaljerede regler allerede på EU-plan for at harmonisere niveauet af databeskyttelse i medlemsstaternes nationale ret. Den generelle forordning om databeskyttelse fastlægger et lag af detaljerede regler under principperne fastlagt i artikel 5, som finder direkte anvendelse i den nationale retsorden. De følgende bemærkninger vedrørende de detaljerede databeskyttelsesregler på europæisk plan vedrører derfor primært EU-retten.

4.1. Regler om lovlig behandling

Hovedpunkter

- Behandlingen af personoplysninger er lovlig, hvis den opfylder ét af følgende kriterier:
  - behandlingen er baseret på den registreredes samtykke
  - et kontraktforhold kræver behandlingen af personoplysninger
  - behandlingen er nødvendig for, at den dataansvarlige kan overholde en retlig forpligtelse
  - de registreredes eller anden persons vitale interesser kræver, at deres oplysninger behandles
  - behandlingen er nødvendig af hensyn til udførelse af en opgave, der udføres i samfundets interesse
  - dataansvarliges eller tredjemænds legitime interesser er grundlaget for behandlingen, men kun for så vidt de ikke tilsidesætter de registreredes interesser eller grundlæggende rettigheder.
- Lovlig behandling af følsomme personoplysninger er underlagt særlige og strengere regler.

4.1.1. Lovlige grundlag for behandling af personoplysninger

Kapitel II i den generelle forordning om databeskyttelse, benævnt »principper«, fastlægger, at al behandling af personoplysninger skal først og fremmest overholde principperne vedrørende datakvalitet fastsat i artikel 5 i GDPR. Ét af principperne er, at personoplysninger skal »behandles lovligt, rimeligt og på en gennemsigtig måde«. For det andet skal behandlingen, for at oplysninger behandles lovligt, overholde ét af de lovlige grundlag for legitim databehandling, som er angivet i artikel 6 ([341]) for ikke-følsomme personoplysninger og i artikel 9 for særlige kategorier af personoplysninger (eller følsomme oplysninger). Kapitel II i den moderniserede

([341]) EU-Domstolen, forenede sager C-465/00, C-138/01 og C-139/01, *Rechnungshof mod Österreichischer Rundfunk m.fl.* og *Christa Neukomm og Jospeh Lauermann mod Österreichischer Rundfunk*, 20. maj 2003, præmis 65; EU-Domstolen, C-524/06, *Heinz Huber mod Bundesrepublik Deutschland* [GC], 16. december 2008, præmis 48; EU-Domstolen, forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado*, 24. november 2011, præmis 26.

konvention 108, som fastlægger de grundlæggende principper for beskyttelse af personoplysninger, fastsætter ligeledes, at databehandling skal være proportional med det forfulgte legitime mål for at være lovlig.

Uanset det lovlige grundlag for behandling, som en dataansvarlig støtter sig til for at indlede en aktivitet med behandling af personoplysninger, skal den dataansvarlige også benytte garantierne fastlagt i den generelle retsorden for databeskyttelse.

Samtykke

I Europarådets retsorden nævnes samtykke i artikel 5, stk. 2, i den moderniserede konvention 108. Det henvises også til i EMD's retspraksis og flere af Europarådets henstillinger ([342]). **I EU-retten** er samtykke som grundlag for lovlig databehandling klart fastlagt ved GDPR's artikel 6, og det nævnes også udtrykkeligt i chartrets artikel 8. Karakteristika for gyldigt samtykke er forklaret i definitionen af samtykke i artikel 4, betingelserne for at indhente gyldigt samtykke er detaljeret i artikel 7, og de særlige regler for børns samtykke i forbindelse med informationssamfundstjenester er fastlagt i artikel 8 i GDPR.

Som forklaret i afsnit 2.4. skal samtykke gives frit og være informeret, specifik og utvetydig. Samtykke skal være en erklæring eller klar bekræftelse, som angiver accept af behandlingen, og personen har ret til at trække deres samtykke tilbage på ethvert tidspunkt. Dataansvarlige er forpligtede til at føre en verificerbar fortegnelse over samtykket.

Frivilligt samtykke

Inden for **Europarådets** rammer i den moderniserede konvention 108 skal den registreredes samtykke udgøre et bevidst valg truffet frivilligt ([343]). Et frivilligt samtykke er kun gyldigt, »hvis den registrerede er i stand til at foretage et reelt valg, og der ikke er nogen risiko for vildledning, intimidering, tvang eller væsentlige negative konsekvenser, hvis han/hun ikke samtykker« ([344]). I denne sammenhæng fastlægger **EU-retten**, at samtykke ikke betragtes som at være givet frivilligt, »hvis den

([342]) Se for eksempel: Europarådet, Ministerudvalget (2010), Henstilling CM/Rec(2010)13 til medlemsstaterne om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, for så vidt angår profilering, 23. november 2010, artikel 3.4, litra b).

([343]) Forklarende rapport til den moderniserede konvention 108, stk. 42.

([344]) Se også Artikel 29-Gruppen (2011), *Udtalelse 15/2011 om definitionen af samtykke* , WP 187, Bruxelles, 13. juli 2011, s. 12.

registrerede ikke har et reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende« ([345]). GDPR understreger, at ved »vurderingen af, om samtykke er givet frit, tages der størst muligt hensyn til, bl.a. om opfyldelsen af en kontrakt, herunder om en tjenesteydelse, er gjort betinget af samtykke til behandling af personoplysninger, som ikke er nødvendig for opfyldelse af denne kontrakt« ([346]). Den forklarende rapport til den moderniserede konvention 108 fastlægger, at den registrerede ikke må udsættes for unødige påvirkninger eller pres (der kan have en økonomisk eller anden karakter), uanset om det er direkte eller indirekte, og samtykke skal ikke betragtes som at være givet frivilligt, hvis den registrerede ikke har noget reelt valg eller ikke er i stand til at afvise eller tilbagetrække samtykke uden forbehold ([347]).

Eksempel: Nogle kommuner i stat A besluttede at udvikle opholdskort med en indbygget chip. Det er ikke obligatorisk for borgere at anskaffe disse elektroniske kort. Borgere, som ikke besidder kortet, har dog ikke adgang til en række vigtige administrative tjenesteydelser, såsom muligheden for at betale skat online, indsende klager elektronisk, hvor vedkommende drager nytte af, at myndigheden har tre dage til at svare, og endda muligheden for at undgå køer, købe nedsatte billetter ved besøg i den kommunale koncertsal og bruge skannere i indgangen.

Kommunernes behandling af personoplysninger i dette eksempel kan ikke baseres på samtykke. Da der er et indirekte pres for, at borgere anskaffer sig det elektroniske kort og godkender behandlingen, er samtykke ikke givet frivilligt. Kommunernes udvikling af et system for elektroniske kort skal derfor baseres på et andet legitimt grundlag, som begrunder behandlingen. De kunne for eksempel henvise til, at behandling er nødvendig af hensyn til udførelse af en opgave, der udføres i samfundets interesse, hvilket er et retsgrundlag for behandling i medfør af artikel 6, stk. 1, litra e), i GDPR ([348]).

([345]) Generel forordning om databeskyttelse, betragtning 42.

([346]) *Ibid.*, artikel 7, stk. 4.

([347]) Forklarende rapport til den moderniserede konvention 108, stk. 42.

([348]) Artikel 29-Gruppen (2011), *Udtalelse 15/2011 om definitionen af samtykke* , WP 187, Bruxelles, 13. juli 2011, s. 16. Yderligere eksempler på tilfælde, hvor databehandling ikke kan baseres på samtykke, men kræver et andet retsgrundlag til at legitimere behandlingen, kan findes på side 14 og 17 i udtalelsen.

Der kan også være tvivl om frivilligt samtykke i situationer med underordnede forhold, hvor der er en væsentlig økonomisk eller anden skævhed mellem den dataansvarlige, som vil sikre samtykke, og den registrerede, der afgiver samtykke ([349]). Et typisk eksempel på sådan en skævhed og underordning er en arbejdsgivers behandling af personoplysninger i forbindelse med et ansættelsesforhold. I henhold til artikel 29-Gruppen er arbejdstagere næsten aldrig i en position, hvor de frivilligt kan afgive, afvise eller tilbagetrække samtykke grundet det afhængighedsforhold, findes mellem arbejdsgiver/arbejdstager. Grundet denne skævhed i magtbalancen kan arbejdstagere kun afgive frivilligt samtykke under usædvanlige omstændigheder, hvor der ikke er nogen konsekvenser overhovedet ved at acceptere eller afvise et tilbud ([350]).

Eksempel: En stor virksomhed har planer om at oprette en medarbejderfortegnelse over alle virksomhedens medarbejdere, deres funktion i virksomheden og deres arbejdsadresse alene for at forbedre den interne kommunikation i virksomheden. Personalechefen foreslår, at der indsættes et foto af hver medarbejder i fortegnelsen, så det f.eks. bliver nemmere at genkende kolleger på møder. Medarbejderrepræsentanterne kræver, at dette kun sker, hvis den enkelte medarbejder giver sit samtykke.

I en sådan situation bør en medarbejders samtykke anerkendes som retsgrundlag for behandling af fotos i fortegnelsen, fordi det er troværdigt, at medarbejderen ikke vil opleve nogen negative følger, hvis han eller hun ønsker eller ikke ønsker at få sit foto offentliggjort i medarbejderfortegnelsen.

Eksempel: Virksomhed A planlægger et møde mellem tre af sine medarbejdere og ledelsen for virksomhed B for at diskutere et potentielt fremtidigt samarbejde på et projekt. Mødet vil finde sted i virksomheds B's lokaler, og virksomhed B kræver, at virksomhed A sender dem en mail med navne, CV'er og fotos for mødets deltagere. Virksomhed B argumenterer, at den skal bruge navne og fotos for deltagerne, så sikkerhedspersonalet ved bygningens indgang kan kontrollere, at de er de rigtige personer, og CV'erne vil give

([349]) Se også Artikel 29-Gruppen (2001), *Udtalelse 8/2001 om behandling af personoplysninger i ansættelsesforhold*, WP 48, Bruxelles, 13. september 2001; Artikel 29-Gruppen (2005), Arbejdsdokument om en ensartet fortolkning af artikel 26, stk. 1, i direktiv 95/46/EF af 24. oktober 1995, WP 114, Bruxelles, 25. november 2005; Artikel 29-Gruppen (2017), *Udtalelse 2/2017 om databehandling på arbejdspladsen*, WP 249, Bruxelles, 8. juni 2017.

([350]) Artikel 29-Gruppen, *Udtalelse 2/2017 om databehandling på arbejdspladsen*, WP 249, Bruxelles, 8. juni 2017.

ledelsen mulighed for at forberede sig bedre til mødet. I dette tilfælde kan virksomhed A's overførsel af personoplysningerne for dets medarbejdere ikke være baseret på samtykke. Samtykke kan ikke betragtes som at være givet frivilligt, da medarbejderne potentielt kan opleve negative følger, hvis de afviser kravet (de kan for eksempel blive erstattet af en anden kollega ikke bare i forbindelse med mødet, men også under samarbejdet med virksomhed B og bidrag til projektet generelt). Behandlingen skal derfor baseres på et andet lovligt behandlingsgrundlag.

Dette betyder dog ikke, at samtykke aldrig kan være gyldigt under omstændigheder, hvor mangel på samtykke ville have visse negative følger. Hvis en mangel på samtykke til at modtage et kundekort til et supermarked kun resulterer i, at vedkommende ikke modtager en mindre prisnedsættelse for visse varer, kan samtykke være et gyldigt retsgrundlag for behandling af personoplysningerne for de kunder, som gav deres samtykke til at modtage et sådant kort. Der er intet underordnet forhold mellem virksomhed og kunde, og konsekvenserne ved at afvise samtykket er ikke alvorlige nok til at forhindre den registreredes frie valg (såfremt prisreduktionen er lille nok til ikke at påvirke deres frie valg).

I tilfælde hvor varer eller tjenester kun kan opnås, hvis bestemte personoplysninger videregives til den dataansvarlige eller til tredjeparter, kan den registreredes samtykke til at videregive dennes oplysninger, som ikke er nødvendige for kontrakten, ikke anses som en frivillig beslutning, og samtykket er derfor ikke gyldigt efter databeskyttelseslovgivningen ([351]). GDPR har meget strenge regler, der forbyder sammenkobling af samtykke med levering af varer og tjenester ([352]).

Eksempel: Passagerers accept af, at et flyselskab overfører såkaldte PNR-oplysninger (Passenger Name Records), dvs. oplysninger om deres identitet, spisevaner eller sundhedsproblemer, til immigrationsmyndighederne i et bestemt fremmed land, kan ikke betragtes som et gyldigt samtykke i henhold til databeskyttelseslovgivningen, da de rejsende passagerer ikke har noget valg, hvis de ønsker at besøge det pågældende land. Hvis sådanne oplysninger skal overføres lovligt, kræves der et andet retsgrundlag end samtykke, sandsynligvis en særskilt lov.

([351]) Generel forordning om databeskyttelse, artikel 7, stk. 4.

([352]) *Ibid.*

Informeret samtykke

Den registrerede skal have tilstrækkelig information, inden vedkommende træffer sit valg. Normalt omfatter et informeret samtykke en præcis og letforståelig beskrivelse af det forhold, der kræver samtykke. Som Artikel 29-Gruppen forklarer, skal samtykke baseres på en respekt for og forståelse af de fakta og konsekvenser, som den registreredes accept af behandlingen har. Derfor skal den »pågældende patient [...] på en klar og forståelig måde gives korrekte og fuldstændige oplysninger om alle relevante spørgsmål [...] såsom arten af de behandlede oplysninger, formålet med behandlingen, modtagerne af oplysningerne ved eventuelle overførsler og den registreredes rettigheder« ([353]). For at samtykke er informeret, skal enkeltpersoner også være klar over konsekvenserne ved ikke at give deres samtykke til behandlingen.

På baggrund af vigtigheden af informeret samtykke forsøgte GDPR og den forklarende rapport til den moderniserede konvention 108 at forklare begrebet. Betragtningerne i GDPR fastlægger, at informeret samtykke betyder, at »den registrerede som minimum [bør] være bekendt med den dataansvarliges identitet og formålene med den behandling, som personoplysningerne skal bruges til« ([354]).

I den usædvanlige situation, hvor samtykke bruges som en undtagelse til at sikre et retsgrundlag for international dataoverførsel, skal den dataansvarlige informere den registrerede om de mulige risici, som sådanne overførsler kan medføre på grund af den manglende afgørelse om tilstrækkeligheden af beskyttelsesniveauet og fornødne garantier, for at dette samtykke kan anses som gyldigt ([355]).

Den forklarende rapport til den moderniserede konvention 108 fastlægger, at der skal oplyses omkring konsekvenserne af den registreredes beslutning, navnlig hvad samtykke faktisk medfører, og i hvilket omfang samtykke gives ([356]).

Informationens kvalitet er vigtig. Informationskvalitet betyder, at sprogbrugen i denne information bør tilpasses den forventede målgruppe. Information skal gives uden brug af fagtermer, i et klart og almindeligt sprog, som en almindelig bruger bør

([353]) Artikel 29-Gruppen (2007), Arbejdsdokument vedrørende behandling af personlige sundhedsoplysninger i elektroniske patientjournaler (EPJ), WP 131, Bruxelles, 15. februar 2007.

([354]) Generel forordning om databeskyttelse, betragtning 42.

([355]) *Ibid*., artikel 49, stk. 1, litra a).

([356]) Forklarende rapport til den moderniserede konvention 108, stk. 42.

kunne forstå ([357]). Informationer skal også være lettilgængelige for den registrerede og kan gives mundtligt eller skriftligt. Det er vigtigt, at informationen er tilgængelig og synlig: Informationen skal tydeligt kunne ses og være fremtrædende. I et onlinemiljø kan lagdelte informationsmeddelelser være en god løsning, da det giver den registrerede mulighed for at vælge, om denne vil have adgang til kortfattede eller omfattende informationer.

Specifikt samtykke

For at være gyldigt skal et samtykke også være specifikt for behandlingens formål, hvilket skal beskrives klart og med utvetydige begreber. Dette går hånd i hånd med kvaliteten af den information, der gives om genstanden for samtykket. I denne sammenhæng er de rimelige forventninger, som en gennemsnitlig registreret person måtte have, relevante. Den registrerede skal igen anmodes om samtykke, hvis behandlingen udvides eller ændres på en måde, som den registrerede ikke med rimelighed kunne forvente, da det oprindelige samtykke blev givet, og derfor har fået et nyt formål. Når behandling tjener flere formål, bør der gives samtykke til dem alle ([358]).

Eksempler: I sagen *Deutsche Telekom AG* ([359]) behandlede EU-Domstolen spørgsmålet om, hvorvidt en telekommunikationsudbyder, der skulle videregive personoplysninger om abonnenter, skulle indhente nyt samtykke fra de registrerede ([360]), da oplysningernes modtagere ikke var nævnt, da samtykket blev givet.

EU-Domstolen fastslog, at nyt samtykke inden videregivelse af personoplysninger ikke var påkrævet i henhold til artikel 12 i direktivet om databeskyttelse inden for elektronisk kommunikation. Siden de registrerede kun havde mulighed for at give samtykke til formålet med behandlingen, dvs. offentliggørelsen af deres oplysninger, kunne de ikke vælge mellem forskellige fortegnelser, hvori disse oplysninger eventuelt ville blive offentliggjort.

([357]) Artikel 29-Gruppen (2011), Udtalelse 15/2011 om definitionen af samtykke , WP 187, Bruxelles, 13. juli 2011, s. 19.

([358]) Generel forordning om databeskyttelse, betragtning 32.

([359]) EU-Domstolen, C-543/09, *Deutsche Telekom AG mod Bundesrepublik Deutschland*, 5. maj 2011. Se navnlig præmis 53 og 54.

([360]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor, EFT L 201 af 31. juli 2002 (direktiv om databeskyttelse inden for elektronisk kommunikation).

Som Domstolen understregede, »følger det af en fortolkning ud fra den lovgivningsmæssige sammenhæng og af en systematisk fortolkning af artikel 12 i direktivet om databeskyttelse inden for elektronisk kommunikation, at samtykket i henhold til artikel 12, stk. 2, vedrører formålet med offentliggørelsen af personoplysningerne i en offentlig nummerfortegnelse, og ikke identiteten på udbyderen af en bestemt fortegnelse« ([361]). Desuden er det »selve offentliggørelsen af personoplysninger i en nummerfortegnelse med et særligt formål, der kan være til ugunst for en abonnent« ([362]), og ikke identiteten af den, som offentliggør oplysningerne.

Sagen *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV mod Autoriteit Consument en Markt (AMC)* ([363]) omhandlede en belgisk virksomheds anmodning om, at nummeroplysningstjenester og abonnentfortegnelser for virksomheder, der tildeler telefonnumre i Nederlandene, skulle give virksomheden adgang til oplysninger vedrørende dennes abonnenter. Den belgiske virksomhed henviste til en forpligtelse i forsyningspligtdirektivet ([364]). Denne kræver, at virksomheder, der tildeler telefonnumre, gør disse numre tilgængelige for abonnentfortegnelser, som anmoder om disse, hvis abonnenterne gav deres samtykke til offentliggørelsen af deres numre. De nederlandske virksomheder afviste anmodningen og meddelte, at det ikke var et krav, at de skulle videregive de pågældende oplysninger til en virksomhed, som var etableret i en anden medlemsstat. De argumenterede, at brugerne havde afgivet samtykke til offentliggørelse af deres numre under forudsætning af, at de ville blive offentliggjort i en nederlandsk abonnentfortegnelse. EU-Domstolen fastholdt, at forsyningspligtdirektivet omfatter alle anmodninger fra nummeroplysningstjenester, uanset hvilken medlemsstat de er etableret i. EU-Domstolen fastholdt desuden, at overdragelse af de samme oplysninger til et andet foretagende, som planlægger at offentliggøre en offentlig nummerfortegnelse uden at indhente fornyet samtykke fra abonnenterne, ikke berører det egentlige indhold i retten til beskyttelse af

([361]) EU-Domstolen, C-543/09, *Deutsche Telekom AG mod Bundesrepublik Deutschland*, 5. maj 2011, præmis 61.

([362]) *Ibid.*, stk. 62.

([363]) EU-Domstolen, C-536/15, *Tele2 (Netherlands) BV m.fl. mod Autoriteit Consument en Markt (ACM)*, 15. marts 2017.

([364]) Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), EFT L 108 af 24. april 2002, s. 51, som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (forsyningspligtdirektivet), EUT L 337 af 18. december 2009, s. 11.

personoplysninger ([365]). På baggrund heraf kan den virksomhed, der tildeler telefonnumre til sine abonnenter, ikke fremsætte anmodningen om samtykke til abonnenten på en måde, hvorefter abonnenten skal give dette samtykke specifikt i forhold til den medlemsstat, som abonnentens personoplysninger videregives til ([366]).

Utvetydigt samtykke

Al samtykke skal være utvetydig ([367]). Dette betyder, at der ikke bør herske nogen rimelig tvivl om, at den registrerede ønskede at give sin accept af behandlingen af sine oplysninger. For eksempel udgør en registrerets inaktivitet ikke utvetydigt samtykke.

Dette er tilfældet for dataansvarlige, som indhenter samtykke med erklæringer i deres privatlivspolitikker, såsom »ved at benytte vores tjeneste giver du dit samtykke til behandlingen af dine personoplysninger«. I så tilfælde kan dataansvarlige være nødt til at sikre, at brugere manuelt og individuelt giver deres samtykke til sådanne politikker.

Hvis samtykke er givet skriftligt som en del af en kontrakt, skal samtykke til behandling af personoplysninger individualiseres, og under alle omstændigheder »bør garantier sikre, at den registrerede er bekendt med, at og i hvilket omfang der er givet samtykke« ([368]).

Krav om samtykke ved børn

GDPR beskytter særligt børn i forbindelse med udbud af informationssamfundstjenester, »eftersom de ofte er mindre bevidste om de pågældende risici, konsekvenser og garantier og deres rettigheder for så vidt angår behandling af personoplysninger« ([369]). I medfør af **EU-retten** vil udbydere af informationssamfundstjenesters behandling af personoplysninger for børn under 16 år på baggrund af samtykke kun være lovlig, »hvis og i det omfang samtykke gives eller godkendes af indehaveren

([365]) EU-Domstolen, C-536/15, *Tele2 (Netherlands) BV m.fl. mod Autoriteit Consument en Markt (ACM)*, 15. marts 2017, præmis 36.

([366]) *Ibid.*, præmis 40-41.

([367]) Generel forordning om databeskyttelse, artikel 4, stk. 11.

([368]) *Ibid.*, betragtning 42.

([369]) *Ibid.*, betragtning 38.

af forældremyndigheden over barnet« ([370]). Medlemsstater kan fastlægge en lavere alder i national lovgivning, dog ikke lavere end 13 år ([371]). Samtykke fra indehaveren af forældremyndigheden er ikke nødvendigt, »når det drejer sig om forebyggende eller rådgivende tjenester, der tilbydes direkte til et barn« ([372]). Oplysninger og meddelelser, hvis behandling er rettet mod et barn, bør være i et så klart og enkelt sprog, at et barn let kan forstå dem ([373]).

Retten til at trække samtykke tilbage på ethvert tidspunkt

GDPR indeholder en generel rettighed til at trække samtykke tilbage på ethvert tidspunkt ([374]). Den registrerede skal informeres om en sådan rettighed, inden denne afgiver samtykke, og vedkommende kan udøve denne ret efter eget skøn. Der må ikke være nogle krav om at begrunde tilbagetrækningen og ingen risiko for negative følger ud over ophøret af eventuelle fordele som følge af den tidligere aftale om brug af oplysninger. Det skal være lige så let at trække sit samtykke tilbage som at give det ([375]). Samtykke anses ikke for at være givet frivilligt, hvis den registrerede ikke kan tilbagetrække sit samtykke uden skadelige følger, eller hvis tilbagetrækningen af samtykket er mere besværligt end at afgive det ([376]).

Eksempel: En kunde accepterer at modtage reklamepost på en adresse, som han eller hun oplyser en dataansvarlig. Hvis kunden trækker sit samtykke tilbage, skal den dataansvarlige straks holde op med at sende reklamepost. Det må ikke medføre negative følger for kunden, som f.eks. gebyrer. Tilbagetrækningen finder dog sted engang i fremtiden og har ingen tilbagevirkende effekt. Perioden, hvori kundens personoplysninger blev lovligt behandlet grundet kundens samtykke, har været legitim. Tilbagetrækningen forhindrer enhver videre behandling af disse oplysninger, medmindre en sådan behandling er i medfør af retten til sletning ([377]).

([370]) *Ibid*. Artikel 8, stk. 1, første led. Begrebet informationssamfundstjenester er defineret i artikel 4, stk. 25, i GDPR.

([371]) Generel forordning om databeskyttelse, artikel 8, stk. 1, andet led.

([372]) *Ibid*., betragtning 38.

([373]) *Ibid*., betragtning 58. Se også den moderniserede konvention 108, artikel 15, stk. 2, litra e). Forklarende rapport til den moderniserede konvention 108, stk. 68 og 125.

([374]) Generel forordning om databeskyttelse, artikel 7, stk. 3. Forklarende rapport til den moderniserede konvention 108, stk. 45.

([375]) Generel forordning om databeskyttelse, artikel 7, stk. 3.

([376]) Generel forordning om databeskyttelse, betragtning 42, og forklarende rapport til den moderniserede konvention 108, stk. 42.

([377]) Generel forordning om databeskyttelse, artikel 17, stk. 1, litra b).

Nødvendig af hensyn til opfyldelse af en kontrakt

I EU-retten fastlægger artikel 6, stk. 1, litra b), i GDPR et andet grundlag for legitim behandling, navnlig hvis det er »nødvendigt af hensyn til opfyldelse af en kontrakt, som den registrerede er part i«. Denne bestemmelse omfatter også aftaler forud for kontraktindgåelse. For eksempel i tilfælde, hvor en part ønsker at indgå en kontrakt, men ikke har gjort det endnu, muligvis fordi nogle kontroller mangler at blive udført. Hvis én part har brug for at behandle oplysninger til dette formål, er en sådan behandling legitim, sålænge den er nødvendig »af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt« ([378]).

Opfattelsen af databehandling som et legitimt grundlag fastlagt i lovgivningen angivet i artikel 5, stk. 2, i den moderniserede konvention 108 omfatter også databehandling til opfyldelse af en kontrakt (eller prækontraktuelle foranstaltninger efter anmodning fra den registrerede), som den registrerede er part i ([379]).

Den dataansvarliges retlige forpligtelser

EU-retten fastlægger et andet grundlag for legitimering af databehandling, nemlig hvis den »er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige« (artikel 6, stk. 1, litra c), i GDPR). Denne bestemmelse henviser til dataansvarlige, som både er aktører inden for den private og offentlige sektor. De retslige forpligtelser for dataansvarlige inden for den offentlige sektor kan også høre under artikel 6, stk. 1, litra e), i GDPR. Der er mange eksempler på situationer, hvor loven forpligter dataansvarlige inden for den private sektor til at behandle oplysninger om konkrete registrerede. For eksempel skal arbejdsgivere behandle oplysninger om deres arbejdstagere grundet socialsikring og beskatning, og virksomheder skal behandle oplysninger om deres kunder af skattemæssige grunde.

Den retslige forpligtelse kan stamme fra Unionens eller medlemsstaters lovgivning, hvilket kan være grundlaget for én eller flere behandlingsaktiviteter. Lovgivningen bør bestemme formålet med behandlingen, fastlægge specifikationer til at præcisere, hvem den dataansvarlige er, hvilken type oplysninger der skal behandles,

([378]) *Ibid.*, artikel 6, stk. 1, litra b).

([379]) Forklarende rapport til den moderniserede konvention 108, stk. 46 og Europarådet, Ministerudvalget (2010), henstilling CM/Rec(2010)13 til medlemsstaterne om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, for så vidt angår profilering, 23. november 2010, artikel 3.4, litra b).

berørte registrerede, hvilke enheder der eventuelt får kendskab til oplysningerne, formålsbegrænsningerne, opbevaringsperioden og andre foranstaltninger, der sikrer en lovlig og rimelig behandling ([380]). Enhver sådan lov, som er grundlaget for behandling af personoplysninger, skal både overholde artikel 7 og 8 i chartret og artikel 8 i EMRK.

Den dataansvarliges retslige forpligtelser fungerer også som et grundlag for legitim databehandling **under Europarådets retsorden** ([381]). Som tidligere angivet er de retslige forpligtelser for en dataansvarlig i den private sektor bare et bestemt tilfælde af andres legitime interesser som anført i artikel 8, stk. 2, i EMRK. Eksemplet med arbejdsgivere, som behandler oplysninger om deres medarbejdere, er derfor også relevant for Europarådets retsorden.

Den registreredes eller en anden fysisk persons vitale interesser

I EU-retten fastlægger artikel 6, stk. 1, litra d), i GDPR, at behandling af personoplysninger er lovlig, hvis det er »nødvendigt for at beskytte den registreredes eller en anden fysisk persons vitale interesser«. Dette legitime grundlag må kun påberåbes for behandling af personoplysninger på baggrund af en anden fysisk persons vitale interesser, hvis denne behandling »tydeligvis ikke kan baseres på et andet retsgrundlag« ([382]). Nogle gange kan en form for behandling være baseret på flere grundlag: offentlig interesse og den registreredes eller en anden persons vitale interesser. Dette er for eksempel tilfældet ved overvågning af epidemier og deres udvikling, eller når der er en humanitær nødsituation.

I Europarådets retsorden nævnes den registreredes vitale interesser ikke i artikel 8 i EMRK. Begrebet »legitimt grundlag« i artikel 5, stk. 2, i den moderniserede konvention 108, som omhandler legitimiteten af behandling af personoplysninger, anses dog som at omfatte den registreredes vitale interesser ([383]).

Samfundsinteresser og offentlig myndighedsudøvelse

Som følge af de mange mulige måder at tilrettelægge offentlige anliggender på fastlægges det i GDPR's artikel 6, stk. 1, litra e), at behandling af personoplysninger

([380]) Generel forordning om databeskyttelse, betragtning 45.

([381]) Europarådet, Ministerudvalget (2010), henstilling CM/Rec(2010)13 til medlemsstaterne om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger så vidt angår profilering, 23. november 2010, artikel 3.4, litra a).

([382]) Generel forordning om databeskyttelse, betragtning 46.

([383]) Forklarende rapport til den moderniserede konvention 108, stk. 46.

er lovlig, hvis den »er nødvendig for at udføre en opgave i samfundets interesse eller henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt [...]« ([384]).

Eksempel: I sagen *Huber mod Bundesrepublik Deutschland* ([385]) anmodede Heniz Huber, østrigsk statsborger bosat i Tyskland, forbundskontoret for migration og flygtninge om at få slettet nogle oplysninger om ham, som er registreret i det centrale udlændingeregister (AZR). Registret, som indeholder personoplysninger om ikketyske EU-statsborgere, der opholder sig i Tyskland i mere end tre måneder, anvendes til statistiske formål og til brug for politi- og justitsmyndighedernes efterforskning og retsforfølgelse af kriminelle handlinger eller handlinger, som bringer den offentlige sikkerhed i fare. Den forelæggende domstol spurgte, om behandlingen af personoplysninger i et register som AZR — hvilket andre offentlige myndigheder har adgang til — er forenelig med EU-retten, idet det bemærkes, at et sådant register ikke findes for tyske statsborgere.

EU-Domstolen fastslog, at behandling af personoplysninger i henhold til direktiv 95/46/EF ([386]), artikel 7, litra e), er lovlig, hvis den er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse.

EU-Domstolen udtalte, at »af hensynet til at sikre et ensartet beskyttelsesniveau i alle medlemsstater må nødvendighedsbegrebet i artikel 7, litra e), i direktiv 95/46/EF ([387]) [...] følgelig ikke tillægges forskelligt indhold i medlemsstaterne. Dermed er det et selvstændigt fællesskabsretligt begreb, som skal fortolkes i fuld overensstemmelse med direktivets formål, som det er formuleret i dets artikel 1, stk. 1« ([388]).

([384]) Se generel forordning om databeskyttelse, betragtning 45.

([385]) EU-Domstolen, C-524/06, *Heinz Huber mod Bundesrepublik Deutschland* [GC], 16. december 2008.

([386]) Det tidligere databeskyttelsesdirektiv, artikel 7, litra e), som nu er den generelle forordning om databeskyttelse, artikel 6, stk. 1, litra e).

([387]) *Ibid.*

([388]) EU-Domstolen, C-524/06, *Heinz Huber mod Bundesrepublik Deutschland* [GC], 16. december 2008, præmis 52.

Domstolen bemærkede, at en unionsborgers ret til fri bevægelighed i en medlemsstats territorium, hvor vedkommende ikke er statsborger, ikke er ubetinget, idet den kan være undergivet de begrænsninger og betingelser, der er fastsat i traktaten om Den Europæiske Unions funktionsmåde og gennemførelsesbestemmelserne hertil. Hvis en medlemsstats anvendelse af et register som AZR til at støtte myndigheder med ansvar for forvaltningen af lovgivningen om opholdsret dermed principielt er lovlig, må et sådant register ikke indeholde andre oplysninger end dem, der er nødvendige til det formål. Domstolen konkluderede, at et sådant system til behandling af personoplysninger er foreneligt med EU-retten, hvis det udelukkende indeholder oplysninger, som er nødvendige for at gennemføre denne lovgivning, og hvis dets centraliserede karakter muliggør en mere effektiv forvaltning af denne lovgivning. Den nationale ret skal efterprøve, at disse betingelser opfyldtes i den pågældende sag. Hvis ikke, kan opbevaring og behandling af personoplysninger i et register som AZR til statistisk brug ikke på noget grundlag anses for nødvendig i den forstand, hvori udtrykket er anvendt i artikel 7, litra e) ([389]), i direktiv 95/46/EF ([390]).

Endelig fastholdt EU-Domstolen, for så vidt angår spørgsmålet om brugen af oplysninger i registret med henblik på kriminalitetsbekæmpelse, at dette mål nødvendigvis tilsigter »retsforfølgning af forbrydelser og begåede lovovertrædelser uafhængigt af gerningsmændenes nationalitet«. Det omhandlede register indeholder ikke personoplysninger vedrørende medlemsstatens egne statsborgere, og denne forskellige behandling udgør en forskelsbehandling omfattet af forbuddet i artikel 18 i TEUF. EU-Domstolen konstaterede således, at denne bestemmelse er »til hinder for, at en medlemsstat med henblik på kriminalitetsbekæmpelse indfører et system til behandling af personoplysninger, som kun omfatter unionsborgere, der ikke er statsborgere i denne medlemsstat« ([391]).

([389]) Det tidligere databeskyttelsesdirektiv, artikel 7, litra e), som nu er den generelle forordning om databeskyttelse, artikel 6, stk. 1, litra e).

([390]) EU-Domstolen, C-524/06, *Heinz Huber mod Bundesrepublik Deutschland* [GC], 16. december 2008, præmis 54, 58-59 og 66-68.

([391]) *Ibid*., præmis 78 og 81.

Offentlige myndigheders anvendelse af personoplysninger er også omfattet af artikel 8 i **EMRK** og, hvor det er passende, er det hensigten, at den er omfattet af artikel 5, stk. 2, i den moderniserede konvention 108 ([392]).

Legitime interesser, der forfølges af den dataansvarlige eller en tredjemand

Under **EU-retten** er den registrerede er ikke den eneste med legitime interesser. Artikel 6, stk. 1, litra f), i GDPR fastlægger, at det er lovligt at behandle personoplysninger, hvis det »er nødvendig for, at den dataansvarlige eller en tredjemand [undtagen offentlige myndigheder, når de udfører deres arbejdsopgaver] kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse, går forud herfor [...]« ([393]).

Eksistensen af en legitim interesse skal vurderes nøje i hvert enkelt tilfælde ([394]). Hvis den dataansvarliges legitime interesser identificeres, så skal en afvejning af de interesser og den registreredes interesser eller grundlæggende rettigheder og friheder gennemføres ([395]). Der skal tages hensyn til den registreredes rimelige forventninger under en sådan vurdering for at bestemme, om den dataansvarliges interesser går forud for den registreredes interesser eller grundlæggende rettigheder ([396]). Hvis den registreredes rettigheder går forud for den dataansvarliges legitime interesser, så kan den dataansvarlige træffe foranstaltninger og implementere garantier til at sikre, at konsekvenserne for den registreredes rettigheder minimeres (såsom ved pseudonymisering af oplysninger), og derved »rette op på balancen«, inden denne lovligt er i stand til anvende dette som et legitimt behandlingsgrundlag. I sin udtalelse om begrebet om den dataansvarliges legitime interesser understregede Artikel 29-Gruppen den vigtige rolle, som ansvarlighed og gennemsigtighed spiller, og den registreredes rettigheder til at gøre indsigelse mod behandlingen af deres oplysninger eller til at de tilgås, ændres, slettes eller overføres, når den dataansvarliges legitime interesser afvejes mod interesserne for den registreredes grundlæggende rettigheder ([397]).

([392]) Forklarende rapport til den moderniserede konvention 108, stk. 46 og 47.

([393]) Sammenlignet med direktiv 95/46/EF angiver den generelle forordning om databeskyttelse flere eksempler, som anses for at udgøre en legitim interesse.

([394]) Generel forordning om databeskyttelse, præambel, betragtning 47.

([395]) Artikel 29-Gruppen (2014), *Udtalelse 06/2014 om begrebet om den dataansvarliges legitime interesser i henhold til artikel 7 i direktiv 95/46/EF*, 4. april 2014.

([396]) *Ibid.*

([397]) *Ibid.*

Der gives eksempler i GDPR's betragtninger på, hvad der udgør en legitim interesse for en berørt dataansvarlig. For eksempel tillades behandlingen af personoplysninger uden den registreredes samtykke, når det udføres med henblik på direkte markedsføring, eller når en sådan behandling »er strengt nødvendig for at forebygge svig« ([398]).

I sin retspraksis har EU-Domstolen udvidet testen for at vurdere, hvad der udgør en legitim interesse.

Eksempel: Sagen *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* ([399]) omhandlede skader på en trolleybus tilhørende transportvirksomheden Rīgas, der blev forårsaget ved, at en passager pludseligt åbnede en taxadør. Rīgas satiksme ønskede at anlægge en erstatningssag mod passageren. Politiet ville dog kun afsløre passagerens navn og ikke vedkommendes ID-nummer og adresse, da de argumenterede, at denne offentliggørelse ville være ulovlig under national databeskyttelseslovgivning.

Den forelæggende domstol i Letland bad EU-Domstolen om at afgive en præjudiciel afgørelse om, hvorvidt EU's databeskyttelseslovgivning pålægger en forpligtelse om at afsløre alle de personoplysninger, der er nødvendige til at indlede et civilt søgsmål mod personen, der angiveligt er skyldig i en administrativ forseelse ([400]).

EU-Domstolen præciserede, at EU's databeskyttelseslovgivning indeholder muligheden — og ikke en forpligtelse — for at videregive oplysninger til tredjemand med henblik på de legitime interesser, som den part forfølger ([401]). EU-Domstolen fastlægger tre kumulative betingelser, som skal opfyldes, for at behandling af personoplysninger er lovligt på grundlag af »legitime interesser« ([402]). For det første skal de tredjemænd, til hvem oplysningerne videregives, forfølge en legitim interesse. I dette tilfælde betyder det, at en anmodning om personoplysninger til at anlægge en erstatningssag mod en person for skader forvoldt på ejendom udgør en tredjemands

([398]) Generel forordning om databeskyttelse, præambel, betragtning 47.

([399]) EU-Domstolen, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde mod Rīgas pašvaldības SIA »Rīgas satiksme«*, 4. maj 2017.

([400]) *Ibid.*, præmis 23.

([401]) *Ibid.*, præmis 26.

([402]) *Ibid.*, præmis 28-34.

legitime interesse. For det andet skal behandlingen af personoplysninger være nødvendig for at forfølge de legitime interesser. I dette tilfælde er det strengt nødvendigt at indhente personoplysninger, såsom adresse og/eller ID-nummer, for at identificere personen. For det tredje må de grundlæggende rettigheder og frihedsrettigheder, der tilkommer den registrerede, ikke gå forud for den dataansvarliges eller tredjemænds legitime interesser. Interesseafvejningen skal vurderes ud fra den enkelte sag under hensyntagen til elementer, såsom omfanget af overtrædelsen af den registreredes rettigheder eller sågar den registreredes alder i visse situationer. I denne sag mente EU-Domstolen dog ikke, at afvisningen af videregivelsen udelukkende var begrundet ved, at den registrerede var en mindreårig.

I sagen *ASNEF og FECEMD* afsagde EU-Domstolen udtrykkeligt dom omkring behandling af oplysninger ud fra retsgrundlaget »legitime interesser«, hvilket på det tidspunkt var fastlagt i databeskyttelsesdirektivets artikel 7, litra f) ([403]).

Eksempel: I sagen *ASNEF og FECEMD* ([404]) præciserede EU-Domstolen, at nationale lovgivninger ikke kan fastsætte supplerende krav til dem, der er nævnt i direktivet om lovlig behandling af personoplysninger, artikel 7, litra f) ([405]). Sagen vedrørte en situation, hvor private parter i henhold til den spanske databeskyttelseslov kun kunne påstå at have en legitim interesse i behandlingen af personoplysninger, hvis oplysningerne allerede var opført i offentligt tilgængelige kilder.

EU-Domstolen bemærkede først, at direktiv 95/46/EF ([406]) har til formål at gøre niveauet for beskyttelsen af det enkelte menneskes rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger ensartet i alle medlemsstater. Endvidere må tilnærmelsen af de nationale lovgivninger, der finder anvendelse på området, ikke medføre en forringelse af den beskyttelse, disse yder. Den skal tværtimod have til formål at sikre et

([403]) Det tidligere databeskyttelsesdirektiv, artikel 7, litra f), som nu er den generelle forordning om databeskyttelse, artikel 6, stk. 1, litra f).

([404]) EU-Domstolen, forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado*, 24. november 2011.

([405]) Det tidligere databeskyttelsesdirektiv, artikel 7, litra f), som nu er den generelle forordning om databeskyttelse, artikel 6, stk. 1, litra f).

([406]) Det tidligere databeskyttelsesdirektiv, som nu er den generelle forordning om databeskyttelse.

højt beskyttelsesniveau inden for EU ([407]). EU-Domstolen fastslog derfor, at det følger af »formålet, som består i at sikre et ensartet beskyttelsesniveau i alle medlemsstaterne, at artikel 7 i direktiv 95/46/EF ([408]) fastsætter en udtømmende og fuldstændig liste over de tilfælde, hvor behandling af personoplysninger kan anses for at være lovlig«. Det følger endvidere, at »medlemsstaterne hverken kan tilføje nye principper vedrørende grundlaget for behandling af oplysninger i artikel 7 i direktiv 95/46/EF ([409]) eller fastsætte supplerende krav, som ændrer rækkevidden af et af de seks principper, der er fastsat i« artikel 7 ([410]). Hvad angår den nødvendige afvejning i henhold til artikel 7, litra f), i direktiv 95/46/EF, erkendte EU-Domstolen endvidere, at det er »muligt at tage hensyn til, at grovheden af den krænkelse af den registreredes grundlæggende rettigheder, der er sket ved nævnte behandling, kan variere alt efter, om de pågældende oplysninger allerede fremgår af offentligt tilgængelige kilder, eller om dette ikke er tilfældet«.

Direktivets artikel 7, litra f), er dog »til hinder for, at en medlemsstat kategorisk og generelt udelukker muligheden for behandling af visse kategorier af personoplysninger uden at tillade en afvejning af de i en konkret sag foreliggende modstående rettigheder og interesser«.

På baggrund af disse overvejelser konkluderede Domstolen, »at artikel 7, litra f), i direktiv 95/46/EF ([411]) skal fortolkes således, at den er til hinder for en national lovgivning, som, i tilfælde af at den registrerede ikke har givet sit samtykke, og for at muliggøre behandlingen af den pågældendes personoplysninger, som er nødvendig for, at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, kræver, ud over at den registreredes grundlæggende rettigheder og frihedsrettigheder ikke krænkes, at nævnte oplysninger

([407]) EU-Domstolen, forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado*, 24. november 2011, præmis 28. Se databeskyttelsesdirektivet, betragtning 8 og 10.

([408]) Det tidligere databeskyttelsesdirektiv, artikel 7, som nu er den generelle forordning om databeskyttelse, artikel 6, stk. 1, litra f).

([409]) Det tidligere databeskyttelsesdirektiv, artikel 7, som nu er den generelle forordning om databeskyttelse, artikel 6.

([410]) *Ibid.*

([411]) Det tidligere databeskyttelsesdirektiv, artikel 7, litra f), som nu er den generelle forordning om databeskyttelse, artikel 6, stk. 1, litra f).

er opført i offentligt tilgængelige kilder, og således kategorisk og generelt udelukker enhver behandling af oplysninger, som ikke er opført i sådanne kilder« ([412]).

Når personoplysninger behandles på grundlag af »legitime interesser«, har den enkelte person ret til at gøre indsigelse mod behandlingen på ethvert tidspunkt på baggrund af vedkommendes særlige situation i medfør af artikel 21, stk. 1, i GDPR. Den dataansvarlige skal standse behandlingen, medmindre den kan fremvise overbevisende, legitime grundlag til at fortsætte den.

I forbindelse med **Europarådets retsorden** findes lignende formuleringer i den moderniserede konvention 108 ([413]) og i Europarådets henstillinger. I henhold til henstillingen om profilering er behandling af personoplysninger med henblik på profilering lovlig, hvis den er nødvendig af hensyn til andres legitime interesser, medmindre den registreredes grundlæggende rettigheder og frihedsrettigheder går forud herfor ([414]). Derudover er »for at beskytte andres ret og frihed« anført i EMRK's artikel 8, stk. 2, som et af de legitime grundlag for at begrænse retten til databeskyttelse.

Eksempel: I sagen *Y mod Tyrkiet* ([415]) var sagsøgeren HIV-positiv. Da han var bevidstløs ved ankomsten til hospitalet, informerede ambulancemandskabet hospitalets personale om, at han var HIV-positiv. Sagsøgeren hævdede for EMD, at videregivelsen af disse oplysninger havde overtrådt hans ret til respekt for privatliv. Videregivelsen af oplysningerne blev dog ikke betragtet som et brud på hans rettigheder grundet behovet for at beskytte hospitalspersonalets sikkerhed.

([412]) EU-Domstolen, forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado*, 24. november 2011, præmis 40, 44 og 48-49.

([413]) Forklarende rapport til den moderniserede konvention 108, stk. 46.

([414]) Europarådet, Ministerudvalget (2010), Henstilling CM/Rec(2010)13 til medlemsstaterne om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger så vidt angår profilering, 23. november 2010, artikel 3.4, litra b), (henstilling om profilering) samt dennes begrundelse.

([415]) EMD, *Y mod Tyrkiet*, nr. 648/10, 17. februar 2015.

4.1.2. Behandling af særlige kategorier af oplysninger (følsomme oplysninger)

Europarådets retsorden overlader det til de nationale lovgivninger at sikre hensigtsmæssig beskyttelse i forbindelse med behandlingen af følsomme oplysninger, hvis betingelserne i artikel 6 i den moderniserede konvention 108 er opfyldt, navnlig at passende garantier, som supplerer konventionens andre bestemmelser, er fastlagt i lovgivningen. **EU-retten**, navnlig artikel 9 i GDPR, indeholder en detaljeret ordning for behandling af særlige kategorier af oplysninger (også kaldet »følsomme oplysninger«). Disse oplysninger afslører racemæssig eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger og medlemskab af en fagforening. Det er også oplysninger, som afslører en persons sexliv eller seksuelle orientering i forbindelse med behandling af genetiske og biometriske oplysninger med henblik på at identificere én bestemt fysisk person og i forbindelse med sundhedsoplysninger. Behandling af følsomme oplysninger er principielt forbudt ([416]).

Der er dog opstillet en udtømmende liste over undtagelser til dette forbud, som findes i forordningens artikel 9, stk. 2, og udgør retsgrundlag for behandling af følsomme oplysninger. Disse undtagelser omfatter situationer, hvor:

- den registrerede har givet udtrykkeligt samtykke til behandlingen
- behandlingen foretages af et organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i dets legitime aktiviteter og alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed
- behandlingen vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede
- behandlingen er nødvendig:
    - for at overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser

([416]) Det tidligere databeskyttelsesdirektiv, artikel 7, litra f), som nu er den generelle forordning om databeskyttelse, artikel 9, stk. 1.

- for at beskytte den registreredes eller en anden fysisk persons vitale interesser (i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke)

- for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol

- med henblik på forebyggende medicin eller arbejdsmedicin: »til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson«

- til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål

- af hensyn til samfundsinteresser på folkesundhedsområdet, eller

- af hensyn til væsentlige samfundsinteresser.

I forbindelse med behandling af særlige kategorier af oplysninger betragtes et kontraktligt forhold med den registrerede dermed ikke som et retsgrundlag for den legitime behandling af følsomme oplysninger, undtagen ved en kontrakt med en sundhedsperson, som er underlagt tavshedspligt ([417]).

Den registreredes udtrykkelige samtykke

I **EU-retten** er den registreredes samtykke det første mulige grundlag for lovlig behandling af oplysninger, uanset om der er tale om følsomme oplysninger eller ej. Ved behandling af følsomme oplysninger skal et sådant samtykke være udtrykkeligt. EU-retten eller medlemsstaters nationale ret kan dog fastsætte, at forbuddet mod behandling af særlige kategorier af oplysninger ikke kan hæves ved den registreredes samtykke ([418]). Dette kan for eksempel være tilfældet, når behandling indebærer usædvanlige risici for den registrerede.

([417]) Generel forordning om databeskyttelse, artikel 9, stk. 2, litra h) og i).

([418]) *Ibid.*, artikel 9, stk. 2, litra a).

Ansættelsesret eller social sikkerhed og socialret

Under **EU-retten** kan forbuddet i artikel 9, stk. 1, ophæves, hvis behandlingen er nødvendig for at overholde den dataansvarliges eller den registreredes arbejds- eller socialretlige forpligtelser og rettigheder. Behandlingen skal dog godkendes i EU-retten eller den nationale ret eller en kollektiv overenskomst i medfør af den nationale ret, som giver fornødne garantier for den registreredes grundlæggende rettigheder og interesser ([419]). Beskæftigelsesregistre, som en organisation besidder, kan indeholde følsomme personoplysninger under visse betingelser anført i GDPR og relevant national lovgivning. Eksempler på følsomme oplysninger kan omfatte medlemskab af en fagforening eller sundhedsmæssige oplysninger.

Den registreredes eller andre personers vitale interesser

I **EU-retten** må følsomme oplysninger, ligesom ikke-følsomme oplysninger, behandles på baggrund af den registreredes eller andre fysiske personers vitale interesser ([420]). Når behandling er baseret på en anden persons vitale interesser, må dette legitime grundlag kun påberåbes, hvis denne behandling »tydeligvis ikke kan baseres på et andet retsgrundlag« ([421]). I nogle tilfælde kan behandling af personoplysninger tjene både enkeltpersoners og samfundsmæssige interesser, for eksempel når behandling er nødvendig af humanitære årsager ([422]).

For at behandlingen af følsomme oplysninger kan legitimeres af dette grundlag, skal det være umuligt at bede den registrerede om vedkommendes samtykke, for eksempel fordi den registrerede er bevidstløs, ikke er tilstede eller ikke kan kontaktes. Med andre ord er personen fysisk eller juridisk ikke i stand til at afgive samtykke.

Velgørenhedsorganisationer eller organer, som ikke arbejder med gevinst for øje

Behandling af personoplysninger tillades kun i forbindelse med legitime aktiviteter for stiftelser, sammenslutninger eller andre organer, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art. Behandlingen skal dog alene vedrøre organets medlemmer, tidligere medlemmer

([419]) Generel forordning om databeskyttelse, artikel 9, stk. 2, litra b).

([420]) *Ibid*., artikel 9, stk. 2, litra c).

([421]) *Ibid*., betragtning 46.

([422]) *Ibid.*

eller personer, der på grund af organets formål er i regelmæssig kontakt hermed ([423]). De følsomme oplysninger må ikke videregives uden for organet uden den registreredes samtykke.

Oplysninger, som tydeligvis er offentliggjort af den registrerede

Artikel 9, stk. 2, litra e), i GDPR fastsætter, at behandling ikke forbydes, hvis det vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede. Selvom betydningen af »som tydeligvis er offentliggjort af den registrerede« ikke defineres i forordningen, skal den, da det er en undtagelse fra at forbyde behandling af følsomme oplysninger, tolkes strengt og som, at ordlyden kræver, at den registrerede bevidst offentliggør sine personoplysninger. Når en fjernsynsudsendelse taget fra et videoovervågningskamera blandt andet viser en brandmand, som bliver såret under evakuering fra en bygning, kan det dermed ikke betragtes som, at brandmanden tydeligvis har offentliggjort oplysningerne. Hvis brandmanden på den anden side beslutter at beskrive hændelsen og offentliggøre videoen og fotografierne på en offentlig internetside, har vedkommende foretaget en bevidst, bekræftende handling om at offentliggøre personoplysningerne. Det er vigtigt at bemærke, at offentliggørelse af ens egne oplysninger ikke udgør samtykke, men det er en anden tilladelse for behandling af særlige kategorier af oplysninger.

Det faktum, at den registrerede offentliggjorde de behandlede personoplysninger, fritager ikke dataansvarlige fra deres forpligtelser under databeskyttelseslovgivningen. For eksempel gælder princippet om formålsbegrænsning fortsat for personoplysninger, selv hvis disse oplysninger er blevet offentliggjort ([424]).

Retskrav

Behandlingen af særlige kategorier af oplysninger, som »er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares«, om det er i forbindelse med en retssag eller en administrativ eller udenretslig procedure ([425]), er også tilladt under GDPR ([426]). I dette tilfælde skal behandlingen være relevant for et bestemt

([423]) *Ibid.*, artikel 9, stk. 2, litra d).

([424]) Artikel 29-Gruppen (2013), Udtalelse 3/13 om formålsbegrænsning, WP 203, Bruxelles, 2. april 2013, s. 14.

([425]) Generel forordning om databeskyttelse, præambel, betragtning 52.

([426]) *Ibid.*, artikel 9, stk. 2, litra f).

retskrav, og at dette krav gøres gældende eller forsvares, og en af parterne i tvisten kan anmode herom.

Når domstole handler i deres egenskab af domstol, må de behandle særlige kategorier af oplysninger i forbindelse med bilæggelsen af en tvist ([427]). Eksempler på disse særlige kategorier af oplysninger, som behandles i denne sammenhæng, kan for eksempel omfatte genetiske oplysninger ved påvisning af slægtskab eller sundhedsstatus, når en del af dokumentationen omhandler en skade, der er påført et offer for en forbrydelse.

Af hensyn til væsentlige samfundsinteresser

I medfør af GDPR's artikel 9, stk. 2, litra g), kan medlemsstater introducere yderligere omstændigheder, hvorunder følsomme oplysninger må behandles, så længe:

- behandling af oplysninger er nødvendig af hensyn til væsentlige samfundsinteresser
- det er fastlagt i EU-retten
- EU-retten eller medlemsstaternes nationale ret er proportional, respekterer retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og interesser ([428]).

Et fremtrædende eksempel er elektroniske patientjournalsystemer. Sådanne systemer tillader, at helbredsoplysninger, der indsamles af sundhedsmedarbejdere under behandlingen af en patient, stilles til rådighed for andre sundhedsmedarbejdere, der kommer i kontakt med denne patient, på overordnet plan, oftest nationalt.

Artikel 29-Gruppen har konkluderet, at indførelsen af sådanne systemer ikke kan ske i henhold til de nuværende regler for behandling af patientoplysninger ([429]). Det er dog muligt at benytte elektroniske patientjournalsystemer, hvis de er baseret på »hensyn til væsentlige samfundsinteresser« ([430]). Dette ville kræve et udtrykkeligt

([427]) *Ibid.*

([428]) *Ibid.*, artikel 9, stk. 2, litra g).

([429]) Artikel 29-Gruppen (2007), Arbejdsdokument vedrørende behandling af personlige sundhedsoplysninger i elektroniske patientjournaler (EPJ), WP 131, Bruxelles, 15. februar 2007. Se også generel forordning om databeskyttelse, artikel 9, stk. 3.

([430]) Generel forordning om databeskyttelse, artikel 9, stk. 2, litra g).

retsgrundlag for deres indførelse, herunder de nødvendige garantier til at sikre, at systemet køres sikkert ([431]).

Andre grundlag til behandling af følsomme oplysninger

GDPR fastsætter, at følsomme oplysninger kan behandles, når behandling er nødvendig ([432]):

- med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson

- af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr på grundlag af EU-retten eller medlemsstaternes nationale ret. Loven skal fastlægge egnede og specifikke foranstaltninger til at sikre den registreredes rettigheder

- til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål på grundlag af EU-retten eller medlemsstaternes nationale ret. Loven skal være proportionel med det forfulgte mål, respektere det væsentligste indhold i retten til databeskyttelse og sikre passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og interesser.

Yderligere betingelser i national lovgivning

GDPR gør det også muligt for medlemsstater at indføre eller forvalte yderligere betingelser, herunder begrænsninger for behandling af genetiske, biometriske og sundhedsrelaterede oplysninger ([433]).

([431]) Artikel 29-Gruppen (2007), *Arbejdsdokument vedrørende behandling af personlige sundhedsoplysninger i elektroniske patientjournaler (EPJ)*, WP 131, Bruxelles, 15. februar 2007.

([432]) Generel forordning om databeskyttelse, artikel 9, stk. 2, litra h), i) og j).

([433]) *Ibid.*, artikel 9, stk. 2, litra h), og artikel 9, stk. 4.

4.2. Regler om behandlingssikkerhed

Hovedpunkter

- Reglerne om behandlingssikkerhed pålægger den dataansvarlige og databehandleren at gennemføre passende tekniske og organisatoriske foranstaltninger med det formål at forhindre uautoriseret indgriben i databehandlingsaktiviteter.
- Det nødvendige niveau af datasikkerhed fastlægges på baggrund af:
  - de sikkerhedsfunktioner, der findes på markedet til en bestemt type behandling
  - omkostningerne
  - databehandlingens risici for registreredes grundlæggende rettigheder og frihedsrettigheder.
- Sikring af personoplysningers fortrolighed er en del af et generelt princip, som er anerkendt i den generelle forordning om databeskyttelse.

Under både **EU-retten og Europarådets retsorden** har dataansvarlige en generel forpligtelse til at være gennemsigtige og ansvarlige ved behandling af personoplysninger og navnlig ved databrud, hvis sådanne brud finder sted. I tilfælde af databrud skal dataansvarlige meddele tilsynsmyndighederne, medmindre bruddet sandsynligvis ikke indebærer risiko for fysiske personers rettigheder og frihedsrettigheder. Registrerede skal også informeres om bruddet på persondatasikkerheden, når det med sandsynlighed indebærer en stor risiko for fysiske personers rettigheder og frihedsrettigheder.

4.2.1. Elementer af datasikkerhed

I **EU-rettens** relevante bestemmelser anføres følgende:

> *»Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici [...]«* ([434]).

([434]) *Ibid.*, artikel 32, stk. 1.

Disse foranstaltninger omfatter bl.a.:

- pseudonymisering og kryptering af personoplysninger ([435])
- sikring af den vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester ([436])
- rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af datatab ([437])
- en procedure for afprøvning, vurdering og evaluering af effektiviteten af foranstaltningerne til sikring af behandlingssikkerheden ([438]).

En lignende bestemmelse findes i **Europarådets retsorden**:

> *Alle parter skal sørge for, at den dataansvarlige og, om relevant, databehandleren gennemfører relevante sikkerhedsforanstaltninger mod risici, såsom hændelig eller ikke-autoriseret adgang til, destruktion, tab, brug, ændring eller videregivelse af personoplysninger* ([439]).

Under **EU-retten og Europarådets retsorden** forpligter et databrud, som kan have en virkning for enkeltpersoners rettigheder og frihedsrettigheder, den dataansvarlige til at meddele tilsynsmyndigheden omkring bruddet (se afsnit 4.2.3.).

Der er i mange tilfælde også udviklet industrielle, nationale og internationale normer for sikker behandling af personoplysninger. EuroPriSe (europæisk datasikkerhedsmærkning) er f.eks. et eTEN-projekt (Trans-European Telecommunications Networks), som EU gennemfører for at undersøge mulighederne for at certificere produkter, især software, som værende i overensstemmelse med den europæiske databeskyttelseslovgivning. ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) blev oprettet for at styrke EU's, medlemsstaternes og erhvervslivets evne

([435]) *Ibid.*, artikel 32, stk. 1, litra a).

([436]) *Ibid.*, artikel 32, stk. 1, litra b).

([437]) *Ibid.*, artikel 32, stk. 1, litra c).

([438]) *Ibid.*, artikel 32, stk. 1, litra d).

([439]) Den moderniserede konvention 108, artikel 7, stk. 1.

til at forhindre, løse og reagere på netværks- og informationssikkerhedsproblemer ([440]). ENISA offentliggør regelmæssigt analyser af aktuelle sikkerhedstrusler og rådgiver om, hvordan de kan afhjælpes ([441]).

Datasikkerhed opnås ikke kun ved at have det rigtige udstyr, dvs. hardware og software. Det kræver også passende interne organisatoriske regler. Sådanne interne regler bør ideelt set omfatte følgende:

- regelmæssig underretning af alle medarbejdere om datasikkerhedsregler og deres forpligtelser i henhold til databeskyttelseslovgivningen, især vedrørende deres tavshedspligt
- klar ansvarsfordeling og klar oversigt over kompetencerne i forhold vedrørende databehandling, navnlig vedrørende beslutninger om at behandle personoplysninger og overføre oplysninger til tredjemand eller registrerede
- anvendelse af personoplysninger alene i henhold til den kompetente persons instrukser eller i henhold til generelt fastlagte regler
- beskyttelse af adgang til lokaler og til den dataansvarliges eller databehandlerens hardware og software, herunder kontrol af adgangstilladelser
- kontrol af, at tilladelser til adgang til personoplysninger gives af den kompetente person og er betinget af relevant dokumentation
- automatiske protokoller over elektronisk adgang til personoplysninger og regelmæssig kontrol af disse protokoller gennemført af den interne tilsynsfunktion (hvilket dermed kræver registrering af alle databehandlingsaktiviteter)
- omhyggelig dokumentation af andre former for videregivelse end automatisk adgang til oplysninger med henblik på at påvise, at ulovlig dataoverførsel ikke har fundet sted.

([440]) Europa-Parlamentets og Rådets forordning (EU) nr. 526/2013 af 21. maj 2013 om Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og om ophævelse af forordning (EF) nr. 460/2004 (EUT L 165 af 18. juni 2013).

([441]) For eksempel, ENISA, (2016), Cyber Security and Resilience of smart cars. Good practices and recommendations; ENISA (2016), Security of Mobile Payments and Digital Wallets.

Tilbud om tilstrækkelig uddannelse og undervisning i datasikkerhed til personalet er også et vigtigt element i en effektiv sikkerhedsindsats. Der skal indføres bekræftelsesprocedurer for at sikre, at de passende foranstaltninger ikke kun findes på papiret, men også gennemføres og fungerer i praksis (f.eks. ved interne eller eksterne revisioner).

Foranstaltninger vedrørende forbedring af en dataansvarligs eller databehandlers sikkerhedsniveau omfatter instrumenter, som f.eks. databeskyttelsesansvarlige, sikkerhedsuddannelse af medarbejdere, regelmæssige revisioner, gennemtrængningstests og kvalitetsmærker.

Eksempel: I sagen *I mod Finland* ([442]) kunne sagsøgeren ikke bevise, at andre medarbejdere på det hospital, hvor hun arbejdede, ulovligt havde haft adgang til hendes patientjournal. Hendes påstand om overtrædelsen af hendes ret til databeskyttelse blev derfor afvist af de nationale domstole. EMD konkluderede, at artikel 8 i EMRK var blevet overtrådt, da hospitalets patientjournalsystem var af en sådan karakter, at det ikke efterfølgende var muligt at afklare anvendelsen af patientjournaler, da det kun viste de fem seneste opslag, og at denne information blev slettet, når journalen blev returneret til arkivet. For Domstolen var det afgørende, at hospitalets patientjournalsystem tydeligvis ikke opfyldte kravene i den nationale lovgivning, en kendsgerning, som de nationale domstole ikke tillagde den fornødne vægt.

EU har indført direktivet om sikkerhed for net- og informationssystemer (NIS-direktivet) ([443]), som er det første retslige instrument om cybersikkerhed for hele EU. Direktivet er rettet mod at forbedre cybersikkerhed på nationalt plan samt øge samarbejdsniveauet på EU-plan. Det pålægger også forpligtelser for udbydere af væsentlige tjenesteydelser (herunder udbydere inden for sektorerne for energi, sundhed, bankvirksomhed, transport, digital infrastruktur osv.) og digitale tjenesteydelser om at håndtere risici, sikre deres net- og informationssystemer og rapportere omkring sikkerhedshændelser.

([442]) EMD, *I mod Finland*, nr. 20511/03, 17. juli 2008.

([443]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EUT L 194 af 19. juli 2016.

Fremtidsudsigter

I september 2017 fremsatte Europa-Kommissionen et forslag til forordning, som var rettet mod at reformere ENISA's mandat for at tage hensyn til agenturets nye kompetencer og ansvarsområder i medfør af NIS-direktivet. Målet med den foreslåede lovgivning var at udvikle ENISA's opgaver og forstærke dets rolle som referencepunktet for EU's økosystem for cybersikkerhed ([444]). Den foreslåede forordning skal være uden forbehold for GDPR's principper og vil også forstærke sikkerheden for personoplysninger ved at afklare de væsentligste elementer af de europæiske ordninger for cybersikkerhedscertificering. I september 2017 foreslog Europa-Kommissionen på samme tid et udkast til en gennemførelsesforordning, der angav de elementer, som udbydere af digitale tjenesteydelser skal tage hensyn til for at sikre, at deres net- og informationssystemer er sikre, hvilket blev anmodet om i artikel 16, stk. 8, i NIS-direktivet. Ved tidspunktet for håndbogens udarbejdelse var diskussionerne om disse to forslag endnu ikke afsluttet.

4.2.2. Fortrolighed

I EU-retten anerkender GDPR personoplysningers fortrolighed som en del af et generelt princip ([445]). Udbydere af offentlige elektroniske kommunikationstjenester skal sikre fortrolighed. De er også forpligtede til at garantere sikkerheden af deres tjenesteydelser ([446]).

Eksempel: En medarbejder i et forsikringsselskab modtager et telefonopkald på arbejdspladsen fra en person, der siger, at han er kunde hos forsikringsselskabet og ønsker oplysninger om sine forsikringspolicer.

Forpligtelsen til at holde kundernes data fortrolige kræver, at medarbejderen anvender minimumssikkerhedsforanstaltninger, inden personoplysninger videregives. Det kan f.eks. ske ved at tilbyde at ringe tilbage til kunden på et telefonnummer, der er registreret for kunden.

([444]) Proposal for a Regulation of the European Parliament and of the Council on ENISA, the »EU Cybersecurity Agency«, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (Cybersecurity Act), COM(2017)477, 13. september 2017, s. 6.

([445]) Generel forordning om databeskyttelse, artikel 5, stk. 1, litra f).

([446]) Direktiv om databeskyttelse inden for elektronisk kommunikation, artikel 5, stk. 1.

I henhold til artikel 5, stk. 1, litra f), skal personoplysninger behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

I medfør af artikel 32 skal den dataansvarlige og databehandleren implementere tekniske og organisatoriske foranstaltninger til at sikre et højt sikkerhedsniveau. Sådanne foranstaltninger omfatter, blandt andet, pseudonymisering og kryptering af personoplysninger, evnen til at sikre behandlingens løbende fortrolighed, integritet, tilgængelighed og robusthed, evaluering og prøvning af foranstaltningernes effektivitet og evnen til at genoprette behandlingen i tilfælde af en fysisk eller teknisk hændelse. Derudover kan overholdelse af en godkendt adfærdskodeks eller en godkendt certificeringsmekanisme bruges som et element til at påvise overholdelse af princippet om integritet og fortrolighed. Desuden skal kontrakten, som binder den dataansvarlige til databehandleren, i henhold til artikel 28 i GDPR fastlægge, at databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

Tavshedspligten omfatter ikke situationer, hvor en person bliver bekendt med oplysninger på baggrund af dennes kapacitet som privatperson og ikke som en medarbejder hos en dataansvarlig eller databehandler. I dette tilfælde finder artikel 28 og 32 i GDPR ikke anvendelse, da privatpersoners brug af personoplysninger på ingen måde er omfattet af forordningens anvendelsesområde, når en sådan brug opfylder kriterierne til den såkaldte familiemæssige undtagelse ([447]). Denne familiemæssige undtagelse er brugen af personoplysninger »af en fysisk person som led i rent personlige eller familiemæssige aktiviteter« ([448]). Siden EU-Domstolens afgørelse i sagen med *Bodil Lindqvist* ([449]) skal denne undtagelse dog fortolkes snævert, især med hensyn til videregivelse af oplysninger. Den familiemæssige undtagelse gælder f.eks. ikke for offentliggørelse af personoplysninger til et ubegrænset antal modtagere på internettet eller for databehandling, som har erhvervsmæssige eller kommercielle aspekter (flere oplysninger om denne sag findes i afsnit 2.1.2., 2.2.2. og 2.3.1.).

([447]) Generel forordning om databeskyttelse, artikel 2, stk. 2, litra c).

([448]) *Ibid.*

([449]) EU-Domstolen, C-101/01, *Straffesag mod Bodil Lindqvist*, 6. november 2003.

»Fortroligheden af juridiske personers kommunikationer« er et andet aspekt af fortrolighed, som er underlagt *lex specialis*. De særlige regler for at sikre fortroligheden af elektroniske kommunikationer under e-databeskyttelsesdirektivet kræver, at medlemsstater forbyder, at andre personer end brugere, eller personer uden brugeres samtykke, lytter til, aflytter, lagrer eller på anden måde opfanger eller overvåger kommunikationer og tilhørende metadata ([450]). National lovgivning kan tillade undtagelser fra dette princip udelukkende på baggrund af national sikkerhed, forsvar, forebyggelse eller opdagelse af kriminalitet, og kun hvis sådanne foranstaltninger er nødvendige til og proportionale med de forfulgte mål ([451]). De samme regler vil finde anvendelse under det fremtidige e-databeskyttelsesdirektiv, dog vil retsaktens omfang udvides fra offentlige elektroniske kommunikationstjenester til også at dække kommunikationer, der foretages igennem OTT-tjenester (såsom mobile applikationer).

I Europarådets retsorden er tavshedspligten underforstået i begrebet datasikkerhed i artikel 7, stk. 1, i den moderniserede konvention 108, som omhandler datasikkerhed.

For databehandlere betyder tavshedspligten, at de ikke må videregive personoplysninger til tredjemænd eller andre modtagere uden tilladelse. For en dataansvarligs eller databehandlers medarbejdere kræver tavshedspligten, at de kun anvender personoplysninger i overensstemmelse med instrukserne fra deres kompetente overordnede.

Tavshedspligten skal medtages i enhver kontrakt mellem dataansvarlige og deres databehandlere. Dataansvarlige og databehandlere skal endvidere iværksætte specifikke foranstaltninger for at pålægge deres medarbejdere en juridisk tavshedspligt, hvilket normalt sker ved at medtage fortrolighedsklausuler i medarbejdernes ansættelseskontrakter.

Brud på tavshedspligten er en strafbar handling i mange EU-medlemsstater og parter til konvention 108.

([450]) Direktiv om databeskyttelse inden for elektronisk kommunikation, artikel 5, stk. 1.

([451]) *Ibid*., artikel 15, stk. 1.

4.2.3. Meddelelser vedrørende brud på persondatasikkerheden

Brud på persondatasikkerheden henviser til et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, som er behandlet ([452]). Selvom nye teknologier, såsom kryptering, giver flere muligheder for at sikre behandlingssikkerheden, er databrud stadig et almindeligt fænomen. Årsagerne til databrud kan spænde fra fejl begået af personer, der arbejder ved en organisation, og eksterne trusler, såsom hackere og cyberkriminelle organisationer.

Databrud kan have negative konsekvenser for enkeltpersoners privatliv og databeskyttelsesrettigheder, der på grund af bruddet mister kontrollen over deres personoplysninger. Brud kan føre til identitetstyveri eller svindel, økonomiske tab eller materielle skader, tab af fortrolighed for personoplysninger beskyttet af tavshedspligt og negative konsekvenser for den registreredes omdømme. I dennes retningslinjer om anmeldelse af brud på persondatasikkerheden i henhold til forordning 2016/679 forklarer Artikel 29-Gruppen, at brud kan have tre forskellige typer af skadevirkninger på personoplysninger: videregivelse, tab og/eller ændring ([453]). Udover forpligtelsen om at træffe foranstaltninger til at sikre behandlingens sikkerhed som forklaret i afsnit 4.2. er det ligeså vigtigt at sikre, at dataansvarlige håndterer brud, når de opstår, på en passende og rettidig måde.

Tilsynsmyndigheder og enkeltpersoner ved ofte ikke, at et databrud har fundet sted, og dette forhindrer enkeltpersoner i at tage skridt til at beskytte sig selv mod bruddets negative konsekvenser. **EU og Europarådet** pålægger et meddelelseskrav for dataansvarlige under visse omstændigheder til at bekræfte enkeltpersoners rettigheder og begrænse konsekvenserne af databrud.

Under **Europarådets** moderniserede konvention 108 skal kontraherende parter som minimum kræve, at dataansvarlige meddeler den kompetente tilsynsmyndighed om databrud, der kan udgøre et alvorligt indgreb i de registreredes rettigheder. En sådan meddelelse skal sendes omgående ([454]).

([452]) Generel forordning om databeskyttelse, artikel 4, stk. 12. Se også Artikel 29-Gruppen (2017), *Retningslinjer om anmeldelse af brud på persondatasikkerheden i henhold til forordning 2016/679*, WP250, 3. oktober 2017, s. 8.

([453]) Artikel 29-Gruppen (2017), *Retningslinjer om anmeldelse af brud på persondatasikkerheden i henhold til forordning 2016/679*, WP250, 3. oktober 2017, s. 6.

([454]) Den moderniserede konvention 108, artikel 7, stk. 2, og forklarende rapport til den moderniserede konvention 108, stk. 64-66.

EU-retten fastlægger en detaljeret ordning, som regulerer meddelelsernes timing og indhold ([455]). Som følge heraf skal dataansvarlige meddele visse databrud til tilsynsmyndighederne uden unødig forsinkelse og, hvis det er muligt, inden for 72 timer fra det tidspunkt, hvor de gøres opmærksom herom. Hvis tidsperioden på 72 timer overskrides, skal meddelelsen ledsages af en forklaring af forsinkelsen. Dataansvarlige er kun fritaget fra meddelelseskravet, hvis de er i stand til dokumentere, at databruddet sandsynligvis ikke indebærer en risiko for de pågældende fysiske personers rettigheder og frihedsrettigheder.

Forordningen angiver de minimale oplysninger, der skal medtages i meddelelsen, så tilsynsmyndigheden kan træffe den nødvendige foranstaltning ([456]). Meddelelsen skal som minimum indeholde en beskrivelse af databruddets karakter og kategorierne og det omtrentlige antal berørte registrerede, en beskrivelse af de sandsynlige konsekvenser af databruddet og de foranstaltninger, som den dataansvarlige har truffet for at begrænse bruddets skadevirkninger. Derudover skal navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt angives, så den kompetente tilsynsmyndighed kan indhente yderligere oplysninger, om nødvendigt.

Hvis et databrud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige uden unødig forsinkelse underrette disse personer (de registrerede) om bruddet ([457]). Informationen til de registrerede, herunder beskrivelsen af databruddet, skal være udformet i et klart og forståeligt sprog og indeholde de samme oplysninger, som er krævet til meddelelse af tilsynsmyndigheder. Under visse omstændigheder kan dataansvarlige være undtaget fra forpligtelsen om at underrette registrerede om sådanne brud. Den dataansvarlige er undtaget, hvis denne har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering. Foranstaltninger, som den dataansvarlige har truffet for at sikre, at indgrebet i de registreredes rettigheder ikke længere finder sted, kan også fritage den dataansvarlige fra forpligtelsen om at underrette de registrerede. Endelig, hvis meddelelse medfører en uforholdsmæssig indsats for den dataansvarlige, kan

([455]) Generel forordning om databeskyttelse, artikel 33 og 34.

([456]) *Ibid.*, artikel 33, stk. 3.

([457]) *Ibid.*, artikel 34.

registrerede underrettes om bruddet på anden vis, såsom offentlig meddelelse eller tilsvarende foranstaltninger ([458]).

Forpligtelsen om at meddele databrud til tilsynsmyndighederne og registrerede er rettet mod dataansvarlige. Databrud kan dog finde sted, uanset om behandling udføres af en dataansvarlig eller databehandler. Det er derfor vigtigt at sikre, at databehandlere også skal rapportere om databrud. I dette tilfælde skal databehandlere underrette databrud til den dataansvarlige uden unødig forsinkelse ([459]). Den dataansvarlige er derefter ansvarlig for at underrette tilsynsmyndighederne og berørte registrerede underlagt de tidligere nævnte regler og tidsrammer.

4.3. Regler om ansvarlighed og fremme af overholdelse

Hovedpunkter

- For at sikre ansvarlighed ved behandling af personoplysninger skal dataansvarlige og databehandlere føre fortegnelser over de behandlingsaktiviteter, som er udført under deres ansvarsområde, og videregive dem til tilsynsmyndighederne efter anmodning.
- Den generelle forordning om databeskyttelse fastsætter flere instrumenter til at fremme overholdelse:
  - udpegelse af databeskyttelsesrådgivere i visse situationer
  - udførelse af en konsekvensanalyse inden påbegyndelse af behandlingsaktiviteter, som sandsynligvis vil medføre store risici for enkeltpersoners rettigheder og frihedsrettigheder
  - forudgående høring ved den relevante tilsynsmyndighed, hvis konsekvensanalysen angiver, at behandlingen udgør risici, som ikke kan begrænses
  - adfærdskodeks for dataansvarlige og databehandlere, der angiver forordningens anvendelse inden for forskellige behandlingssektorer
  - certificeringsmekanismer, mærkninger og mærker.
- Europarådets lovgivning foreslår lignende instrumenter til fremme af overholdelse i den moderniserede konvention 108.

([458]) *Ibid.*, artikel 34, stk. 3, litra c).

([459]) *Ibid.*, artikel 33, stk. 2.

Princippet om ansvarlighed er særligt vigtigt til at garantere håndhævelsen af databeskyttelsesreglerne i Europa. Den dataansvarlige er ansvarlig for og skal kunne påvise overholdelse af databeskyttelsesregler. Ansvarlighed er ikke kun relevant, efter en overtrædelse har fundet sted. Dataansvarlige har nærmere en proaktiv forpligtelse om at følge passende dataforvaltningspolitikker under alle databehandlingsfaser. Europæisk databeskyttelseslovgivning kræver, at dataansvarlige implementerer tekniske og organisatoriske foranstaltninger for at sikre og være i stand til at påvise, at behandlingen udføres i medfør af loven. Disse foranstaltninger er blandt andet udpegelse af databeskyttelsesrådgivere, føring af registre og dokumentation vedrørende behandlingen samt udførelse af konsekvensanalyser om privatliv.

4.3.1. Databeskyttelsesrådgivere

Databeskyttelsesrådgivere (DPO) er personer, som rådgiver organisationer, der udfører databehandling, omkring overholdelse af databeskyttelsesregler. De er en »hjørnesten for ansvarlighed«, da de fremmer overholdelse, mens de fungerer som mellemled mellem tilsynsmyndigheder, registrerede og organisationen, som har udpeget dem.

Under Europarådets retsorden placerer artikel 10, stk. 1, i den moderniserede konvention 108 en generel forpligtelse om ansvarlighed på dataansvarlige og databehandlere. Denne kræver, at dataansvarlige og databehandlere skal træffe alle passende foranstaltninger til at overholde databeskyttelsesreglerne angivet i konventionen, og at de kan påvise, at databehandlingen, de forvalter, overholder konventionens bestemmelser. Selvom konventionen ikke angiver de konkrete foranstaltninger, som dataansvarlige og databehandlere skal vedtage, indikerer den forklarende rapport til den moderniserede konvention 108, at udpegelse af en DPO ville være én mulig foranstaltning, som kan hjælpe med at påvise overholdelse. DPO'er skal tildeles alle nødvendige midler til at opfylde deres mandater ([460]).

I modsætning til Europarådets retsorden er udpegelse af en DPO **under EU-retten** ikke altid overladt til dataansvarliges og databehandleres skøn, men er obligatorisk under visse omstændigheder. GDPR anerkender, at DPO'en spiller en vigtig rolle i det nye forvaltningssystem og indeholder detaljerede bestemmelser vedrørende rådgiverens udpegelse, stilling, pligter og opgaver ([461]).

([460]) Forklarende rapport til den moderniserede konvention 108, stk. 87.

([461]) Generel forordning om databeskyttelse, artikel 37-39.

GDPR gør det obligatorisk at udpege en DPO i tre specifikke tilfælde: når behandling foretages af en offentlig myndighed eller et offentligt organ; når den dataansvarliges eller databehandlerens kerneaktiviteter består af behandlingsaktiviteter, der kræver regelmæssig og systematisk overvågning af registrerede i stort omfang, eller når den dataansvarliges eller databehandlerens kerneaktiviteter består af behandling i stort omfang af særlige kategorier af oplysninger eller personoplysninger vedrørende straffedomme og lovovertrædelser ([462]). Selvom begreber som »systematisk overvågning i stort omfang« og »kerneaktiviteter« ikke er defineret i forordningen, har Artikel 29-Gruppen udstedt retningslinjer om, hvordan de skal fortolkes ([463]).

Eksempel: Sociale medievirksomheder og søgemaskiner anses sandsynligvis som dataansvarlige, hvis behandlingsaktiviteter kræver regelmæssig og systematisk overvågning af registrerede i stort omfang. Disse virksomheders forretningsmodel er baseret på behandlingen af store mængder personoplysninger, og de producerer betydelige indtægter ved at tilbyde målrettede reklametjenester og give virksomheder tilladelse til at reklamere på webstederne. Målrettede reklamer er en metode for placering af reklamer på baggrund af demografi og forbrugernes tidligere købshistorik eller adfærd. Det kræver derfor en systematisk overvågning af de registreredes onlinevaner og adfærd.

Eksempel: Et hospital og et sygeforsikringsselskab er typiske eksempler på dataansvarlige, hvis aktiviteter består af behandling i stort omfang af særlige kategorier af personoplysninger. Oplysninger, der afslører informationer om en enkeltpersons sundhed, udgør særlige kategorier af personoplysninger under både Europarådets retsorden og EU-retten, hvilket derfor begrunder øget beskyttelse. EU-retten anerkender yderligere genetiske og biometriske data som særlige kategorier. Hvis sundhedsinstitutioner og forsikringsselskaber behandler sådanne oplysninger i et stort omfang, skal de under GDPR udpege en databeskyttelsesrådgiver.

Desuden fastsætter artikel 37, stk. 4, i GDPR, at den dataansvarlige, databehandleren eller sammenslutninger og andre organer, som repræsenterer kategorier af

([462]) *Ibid.*, artikel 37, stk. 1.

([463]) Artikel 29-Gruppen (2017), *Retningslinjer for databeskyttelsesrådgivere*, WP 243 rev.1, senest revideret og vedtaget den 5. april 2017.

dataansvarlige eller databehandlere, kan eller, hvis det er krævet ved EU's eller en medlemsstats lovgivning, skal udpege en databeskyttelsesrådgiver i andre tilfælde end de tre obligatoriske, som påkræves i henhold til artikel 37, stk. 1.

Alle andre organisationer er ikke juridisk forpligtede til at udpege en DPO. GDPR fastlægger dog, at dataansvarlige og databehandlere frivilligt kan vælge at udpege en DPO, hvor der stadig er mulighed for, at medlemsstater kan gøre en sådan udpegelse obligatorisk for flere typer af organisationer end dem, som forordningen beskriver ([464]).

Når en dataansvarlig udpeger en DPO, skal denne sikre, at vedkommende »inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger« inden for organisationen ([465]). For eksempel bør DPO'er inddrages i rådgivning om udførelse af konsekvensanalyser vedrørende databeskyttelse og i oprettelse og føring af registre over en organisations behandlingsaktiviteter. Dataansvarlige og databehandlere skal sørge for, at DPO'er har alle de nødvendige ressourcer, herunder finansielle midler, infrastruktur og udstyr, som de skal bruge til at udføre deres arbejdsopgaver på effektiv vis. Yderligere krav omfatter tildeling af tilstrækkelig tid til DPO'er, så de kan udføre deres arbejdsfunktioner, og løbende undervisning, så de kan udvikle deres ekspertise og holde sig ajourførte med alle udviklinger inden for databeskyttelseslovgivning ([466]).

GDPR fastlægger nogle grundlæggende garantier til at sikre, at DPO'er kan fungere uafhængigt. Dataansvarlige og databehandlere skal sikre, at DPO'er ikke modtager instrukser fra virksomheden, inklusive ledelsen, under udførelse af deres arbejdsopgaver, som vedrører databeskyttelse. Derudover må de ikke afskediges eller straffes på nogen måde for at udføre deres arbejdsopgaver ([467]). Eksempel: En DPO råder en dataansvarlig eller databehandler til at udføre en konsekvensanalyse vedrørende databeskyttelse, da vedkommende mener, at behandlingen sandsynligvis indebærer en høj risiko for registrerede. Virksomheden er uenig med DPO'ens rådgivning, som anser den for at have et dårligt grundlag og beslutter derfor ikke at gennemføre en konsekvensanalyse. Virksomheden kan ignorere rådgivningen, men kan ikke afskedige eller straffe DPO'en for at levere den.

([464]) Generel forordning om databeskyttelse, artikel 37, stk. 3 og 4.

([465]) *Ibid*., artikel 38, stk. 1.

([466]) Artikel 29-Gruppen (2017), Retningslinjer for databeskyttelsesrådgivere, WP 243 rev.1, senest revideret og vedtaget den 5. april 2017, stk. 3.1.

([467]) Generel forordning om databeskyttelse, artikel 38, stk. 2 og 3.

Endelig er DPO'ers opgaver og pligter beskrevet i artikel 39 i GDPR. Disse omfatter krav om at underrette og rådgive virksomhederne og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til lovgivningen samt om at overvåge overholdelsen af europæiske og nationale databeskyttelsesregler igennem udførelse af revisioner og uddannelse af det personale, der medvirker ved behandlingsaktiviteter. DPO'er skal også samarbejde med tilsynsmyndigheden og fungere som kontaktpunkt for sidstnævnte i forbindelse med databehandling, såsom ved et databrud.

I forbindelse med personoplysninger behandlet af EU-institutioner og -organer fastlægger forordning (EF) nr. 45/2001, at hver EU-institution og -organ skal udpege en DPO. DPO'en har ansvar for at sikre, at forordningens bestemmelser anvendes korrekt i EU's institutioner og organer, og at både registrerede og dataansvarlige informeres om deres rettigheder og pligter ([468]). Vedkommende er også ansvarlig for at svare på anmodninger fra EDPS og samarbejde med vedkommende efter behov. Ligesom GDPR indeholder forordning (EF) nr. 45/2001 bestemmelser om DPO'ers afhængighed under udførelsen af deres opgaver og behovet for at give dem det nødvendige personale og ressourcer ([469]). DPO'er skal underrettes, inden en EU-institution eller -organ (eller afdelinger inden for disse organisationer) udfører nogen behandlingsaktiviteter, og de skal føre en fortegnelse over alle meddelte behandlingsaktiviteter ([470]).

4.3.2. Fortegnelser over behandlingsaktiviteter

For at virksomheder kan påvise overholdelse, og for at de kan stilles til ansvar, er det ofte et juridisk krav, at de dokumenterer og registrerer deres aktiviteter. Et vigtigt eksempel er skatteloven og revision, der kræver, at alle virksomheder fører omfattende dokumentation og fortegnelser. Fastlæggelse af lignende krav inden for andre lovområder, navnlig databeskyttelseslovgivning, er også vigtigt, da føring af fortegnelser er en vigtig måde at fremme overholdelse af databeskyttelsesregler. **EU-retten** fastlægger dermed, at dataansvarlige eller deres repræsentanter skal føre fortegnelser over behandlingsaktiviteter under deres ansvar ([471]). Forpligtelsen er nødvendig til at sikre, at tilsynsmyndigheder, om nødvendigt, besidder den fornødne dokumentation til at bekræfte behandlingens lovlighed.

([468]) Se artikel 24, stk. 1, i forordning (EF) nr. 45/2001 for den udførlige liste over DPO'ers opgaver.

([469]) Forordning (EF) nr. 45/2001, artikel 24, stk. 6 og 7.

([470]) *Ibid.*, artikel 25 og 26.

([471]) Generel forordning om databeskyttelse, artikel 30.

Den information, der skal dokumenteres, omfatter følgende:

- navn og kontaktoplysninger for den dataansvarlige, de fælles dataansvarlige, den dataansvarliges repræsentant og DPO'en, om relevant
- behandlingens formål
- beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger relateret til behandlingen
- information om kategorierne af modtagere, hvortil personoplysninger er eller vil blive videregivet
- information om, hvorvidt overførsler af personoplysninger til tredjelande eller internationale organisationer er eller vil blive udført
- hvis det er muligt, de forventede tidsfrister for sletning af de forskellige kategorier af personoplysninger, samt en oversigt over de tekniske foranstaltninger, som er vedtaget for at sikre behandlingens sikkerhed ([472]).

Forpligtelsen om at føre fortegnelser over behandlingsaktiviteter under GDPR vedrører ikke kun dataansvarlige men også databehandlere. Dette er en vigtig udvikling, da kontrakten indgået mellem den dataansvarlige og databehandleren, inden forordningens vedtagelse, primært omfattede databehandlerens forpligtelser. Deres forpligtelse om at føre fortegnelser er nu fastsat direkte i lovgivningen.

GDPR tillader en undtagelse fra denne forpligtelse. Kravet om at føre registre gælder ikke for en virksomhed eller organisation (dataansvarlig eller databehandler), som beskæftiger under 250 personer. Undtagelsen er dog underlagt kravene om, at den pågældende organisation ikke udfører behandling, der sandsynligvis udgør en risiko for registreredes rettigheder og frihedsrettigheder, at behandling kun finder sted lejlighedsvist, og at den ikke vedrører særlige kategorier af oplysninger som angivet i artikel 9, stk. 1, eller personoplysninger om straffedomme og lovovertrædelser angivet i artikel 10.

Føring af fortegnelser over behandlingsaktiviteter burde gøre dataansvarlige og databehandlere i stand til at påvise overholdelse af forordningen. Det bør også gøre

([472]) *Ibid*., artikel 30, stk. 1.

det muligt for tilsynsmyndigheder at overvåge lovligheden af behandlingen. Når en tilsynsmyndighed anmoder om adgang til disse fortegnelser, er dataansvarlige og databehandlere forpligtet til at samarbejde og gøre dem tilgængelige.

4.3.3. Konsekvensanalyse vedrørende databeskyttelse og forudgående høring

Behandlingsaktiviteter udgør nogle iberegnede risici for enkeltpersoners rettigheder. Personoplysninger kan gå tabt, videregives til uautoriserede parter eller behandles på en ulovlig måde. Risici varierer naturligvis alt efter behandlingens art og omfang. Omfattende aktiviteter, der involverer behandling af følsomme oplysninger, indebærer for eksempel en meget højere risiko for registrerede sammenlignet med de potentielle risici, når en mindre virksomhed behandler sine medarbejderes adresser og private telefonnumre.

I takt med at nye teknologier kommer frem, og behandling bliver mere kompleks, skal dataansvarlige håndtere sådanne risici ved at undersøge de sandsynlige følger af den planlagte behandling, inden behandlingsaktiviteten påbegyndes. Dette gør det muligt for organisationer at identificere, håndtere og begrænse risiciene korrekt på forhånd, hvilket væsentligt begrænser sandsynligheden for negative konsekvenser for enkeltpersoner som følge af behandlingen.

Konsekvensanalyser vedrørende databeskyttelse er planlagt **i både Europarådets retsorden og EU-retten**. Under Europarådets retsorden kræver artikel 10, stk. 2, i den moderniserede konvention 108, at kontraherende parter sikrer, at dataansvarlige og databehandlere undersøger de sandsynlige virkninger af databehandling for registreredes rettigheder og grundlæggende frihedsrettigheder, inden denne behandling påbegyndes, og efter vurderingen skal behandlingen udformes på en måde, der forhindrer eller minimerer risiciene knyttet til behandlingen.

EU-retten pålægger en lignende og mere detaljeret forpligtelse for dataansvarlige, som er omfattet af GDPR. Artikel 35 fastlægger, at en konsekvensanalyse skal udføres, når behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Forordningen definerer ikke, hvordan risicienes sandsynlighed skal vurderes, men angiver i stedet, hvad de risici kan være ([473]). Den indeholder en liste over behandlingsaktiviteter, der anses for

([473]) Generel forordning om databeskyttelse, præambel, betragtning 75.

at have en høj risiko, og hvor det er særligt nødvendigt med en forudgående konsekvensanalyse, navnlig i tilfælde, hvor:

- personoplysninger behandles for at træffe afgørelser vedrørende fysiske personer efter udførelse af alle eventuelle systematiske og omfattende evalueringer af enkeltpersonernes personlige forhold (profilering)

- følsomme oplysninger eller personoplysninger om straffedomme og lovovertrædelser behandles i stort omfang

- behandlingen involverer systematisk overvågning af offentligt tilgængelige områder i stort omfang.

Tilsynsmyndighederne skal udarbejde og offentliggøre en liste over de typer af behandlingsaktiviteter, der skal være underlagt konsekvensanalyser. De kan også udarbejde og offentliggøre en liste over de behandlingsaktiviteter, som er undtaget fra denne forpligtelse ([474]).

Når en konsekvensanalyse påkræves, skal dataansvarlige vurdere behandlingens nødvendighed og proportionalitet og de mulige risici for enkeltpersoners rettigheder. Konsekvensanalysen skal også indeholde planlagte sikkerhedsforanstaltninger til at håndtere de identificerede risici. For at udarbejde disse lister skal medlemsstaternes tilsynsmyndigheder samarbejde med hinanden og med Det Europæiske Databeskyttelsesråd. Dette vil sikre en ensartet tilgang i hele EU til de aktiviteter, som kræver en konsekvensanalyse, og dataansvarlige vil være underlagt tilsvarende krav, uanset hvor de befinder sig.

Hvis det efter en konsekvensanalyse virker til, at behandlingen vil indebære en høj risiko for enkeltpersoners rettigheder, og der ikke blev indført foranstaltninger til at begrænse risikoen, skal den dataansvarlige rådføre sig med den relevante tilsynsmyndighed, inden behandlingsaktiviteten påbegyndes ([475]).

Artikel 29-Gruppen har udstedt retningslinjer om konsekvensanalyser vedrørende databeskyttelse, og hvordan man bestemmer, om behandlingen sandsynligvis

([474]) *Ibid.*, artikel 35, stk. 4 og 5.

([475]) *Ibid.*, artikel 36, stk. 1, og Artikel 29-Gruppen (2017), *Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen »sandsynligvis indebærer en høj risiko« i henhold til forordning (EU) 2016/679*, WP 248 rev. 01, Bruxelles, 4. oktober 2017.

indebærer en høj risiko eller ej ([476]). Den udviklede ni kriterier til at hjælpe med at bestemme, om en konsekvensanalyse vedrørende databeskyttelse er påkrævet i et specifikt tilfælde ([477]): (1) evaluering eller analyse; (2) automatiseret beslutningstagning med juridisk eller tilsvarende betydelig virkning; (3) systematisk overvågning; (4) følsomme oplysninger eller oplysninger af meget personlig karakter; (5) oplysninger, der gøres til genstand for omfattende behandling; (6) matching eller kombination af datasæt; (7) oplysninger om sårbare registrerede; (8) innovativ brug eller anvendelse af ny teknologi eller nye organisatoriske løsninger; (9) når behandlingen i sig selv »hindrer registrerede i at udøve en rettighed eller gøre brug af en tjeneste eller en kontrakt«. Artikel 29-Gruppen indførte tommelfingerreglen, at behandlingsaktiviteter, som opfylder under to kriterier, udgør et lavere risikoniveau og ikke kræver en konsekvensanalyse vedrørende databeskyttelse, hvorimod dem, som opfylder to eller flere kriterier, skal udsættes for en sådan analyse. I tilfælde, hvor det ikke er klart, om det er nødvendigt med en konsekvensanalyse vedrørende databeskyttelse, anbefaler Artikel 29-Gruppen, at en sådan analyse udføres, da det »er et nyttigt redskab, som kan hjælpe de dataansvarlige med at overholde databeskyttelseslovgivningen« ([478]). Ved introduktion af en ny databehandlingsteknologi er det vigtigt, at en konsekvensanalyse vedrørende databeskyttelse udføres ([479]).

4.3.4. Adfærdskodekser

Adfærdskodekser er beregnet til at blive anvendt i flere industrisektorer for at fremhæve og angive anvendelsen af GDPR i de enkelte sektorer. For dataansvarlige og databehandlere af personoplysninger kan oprettelsen af sådanne kodekser væsentligt forbedre overholdelsen og øge implementeringen af EU's databeskyttelsesregler. Medlemmerne af sektoren vil, grundet deres ekspertise, tilstræbe at finde løsninger, der er praktiske, og som dermed sandsynligvis vil blive fulgt. GDPR anerkender vigtigheden af sådanne kodekser i forbindelse med den effektive anvendelse af databeskyttelseslovgivningen og opfordrer medlemsstater, tilsynsmyndigheder, Kommissionen og Det Europæiske Databeskyttelsesråd til at tilskynde til udarbejdelse af adfærdskodekser, der kan bidrage til en korrekt anvendelse af forordningen i hele EU ([480]). Kodekserne kan angive forordningens

([476]) Artikel 29-Gruppen (2017), *Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen »sandsynligvis indebærer en høj risiko« i henhold til forordning (EU) 2016/679*, WP 248 rev. 01, Bruxelles, 4. oktober 2017.

([477]) *Ibid.*, s. 9-11.

([478]) *Ibid.*, s. 9.

([479]) *Ibid.*

([480]) Generel forordning om databeskyttelse, artikel 40, stk. 1.

anvendelse inden for bestemte sektorer, herunder med hensyn til indsamling af personoplysninger, informationen der gives til offentligheden og til registrerede, og udøvelsen af registreredes rettigheder.

For at sikre, at adfærdskodekserne opfylder reglerne fastlagt i GDPR, skal de indsendes til den kompetente tilsynsmyndighed inden vedtagelse. Tilsynsmyndigheden afgiver derefter en udtalelse om, hvorvidt det indgivne udkast til adfærdskodeks overholder forordningen, og godkender kodeksen, hvis den finder, at kodeksen sikrer tilstrækkelige fornødne garantier ([481]). Tilsynsmyndigheder skal offentliggøre de godkendte adfærdskodekser samt de kriterier, som deres godkendelse blev baseret på. Når et udkast til adfærdskodeks omhandler behandlingsaktiviteter i flere medlemsstater, skal den kompetente tilsynsmyndighed, inden godkendelse af udkastet til adfærdskodeks, ændring eller udvidelse, indsende kodeksen til Det Europæiske Databeskyttelsesråd, der skal afgive en udtalelse om kodeksens overholdelse af GDPR. Kommissionen kan via gennemførelsesretsakter beslutte, at den godkendte adfærdskodeks, som er indsendt til denne, generelt er gyldig i EU.

Overholdelse af en adfærdskodeks giver store fordele til både registrerede samt dataansvarlige og databehandlere. Disse kodekser giver detaljeret vejledning, som tilrettelægger juridiske krav til bestemte sektorer og fremmer behandlingsaktiviteters gennemsigtighed. Dataansvarlige og databehandlere kan også benytte kodekserne som beviselig dokumentation for deres overholdelse af EU-retten og som et middel til at forbedre deres image udadtil som organisationer, der prioriterer og forpligter sig til databeskyttelse i forbindelse med deres aktiviteter. Godkendte adfærdskodekser kan sammen med bindende forpligtelser, der kan håndhæves, benyttes som passende garantier til at overføre oplysninger til tredjelande. For at sikre, at organisationer, som overholder adfærdskodekserne, faktisk overholder dem, kan et særligt organ (akkrediteret af den relevante tilsynsmyndighed) udpeges til at overvåge og sikre overholdelse. For at organet kan udføre sine opgaver på effektiv vis, skal det være uafhængigt, besidde dokumenteret ekspertise inden for området, som adfærdskodeksen regulerer, og have gennemsigtige procedurer og strukturer, som gør det muligt for den at håndtere klager omkring overtrædelser af kodeksen ([482]).

Under **Europarådets retsorden** fastsætter den moderniserede konvention 108, at graden af databeskyttelse, som national lovgivning garanterer, med fordel kan

([481]) *Ibid.*, artikel 40, stk. 5.

([482]) *Ibid.*, artikel 41, stk. 1 og 2.

forstærkes af frivillige regulerende tiltag, såsom kodekser for god praksis eller faglige kodekser. Dette er dog kun frivillige tiltag i henhold til den moderniserede konvention 108. Man kan ikke aflede nogen retslig forpligtelse heraf om at indføre sådanne tiltag, selvom det anbefales, og sådanne tiltag ikke alene er tilstrækkelige til at sikre overholdelse af konventionen ([483]).

4.3.5. Certificering

Udover adfærdskodekser er certificeringsmekanismer og databeskyttelsesmærkninger og -mærker andre måder, hvorpå dataansvarlige og databehandlere kan bevise overholdelse af GDPR. Til dette formål fastlægger forordningen et frivilligt certificeringssystem, hvormed visse organer eller tilsynsmyndigheder kan udstede certificeringer. Dataansvarlige og databehandlere, som vælger at overholde en certificeringsmekanisme, kan opnå større synlighed og troværdighed, da certificeringer, mærkninger og mærker gør, at registrerede hurtigt kan vurdere en organisations beskyttelsesniveau for databehandling. Det er vigtigt at bemærke, at det faktum, at en dataansvarlig eller databehandler besidder en sådan certificering, ikke indskrænker dennes ansvar for at overholde alle forordningens krav.

4.4. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

Databeskyttelse gennem design

EU-retten kræver, at dataansvarlige fastlægger foranstaltninger, som effektivt implementerer databeskyttelsesprincipper, og integrerer de nødvendige garantier til at overholde forordningens krav og beskytte registreredes rettigheder ([484]). Disse foranstaltninger bør både implementeres ved behandlingstidspunktet og ved bestemmelse af midlerne til behandling. Ved implementering af disse foranstaltninger skal den dataansvarlige tage hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne, den pågældende behandlings karakter,

([483]) Forklarende rapport til den moderniserede konvention 108, stk. 33.

([484]) Generel forordning om databeskyttelse, artikel 25, stk. 1.

omfang og formål samt risiciene og deres alvor for den registreredes rettigheder og frihedsrettigheder ([485]).

Europarådets retsorden kræver, at dataansvarlige og databehandlere vurderer de sandsynlige virkninger ved behandlingen af personoplysninger for den registreredes rettigheder og frihedsrettigheder, inden behandlingen påbegyndes. Desuden skal dataansvarlige og databehandlere udforme databehandlingen på en måde, der forhindrer eller minimerer risikoen for indgreb i disse rettigheder og frihedsrettigheder, og implementere tekniske og organisatoriske foranstaltninger, som tager hensyn til konsekvenserne af retten til beskyttelse af personoplysninger under alle faser af databehandlingen ([486]).

Databeskyttelse gennem standardindstillinger

EU-retten kræver, at den dataansvarlige implementerer passende foranstaltninger til at sikre, at kun de personoplysninger, som er nødvendige til formålet, behandles som en standardindstilling. Denne forpligtelse gælder for mængden af indsamlede personoplysninger, behandlingens omfang, opbevaringsperioden og tilgængeligheden ([487]). En sådan foranstaltning skal blandt andet sikre, at det ikke er alle de dataansvarliges medarbejdere, som har adgang til de registreredes personoplysninger. Yderligere vejledning blev udviklet af EDPS i *Necessity Toolkit* ([488]).

Europarådets retsorden kræver, at dataansvarlige og databehandlere implementerer tekniske og organisatoriske foranstaltninger, der tager hensyn til konsekvenserne af retten til databeskyttelse, og implementerer tekniske og organisatoriske foranstaltninger, som tager hensyn til konsekvenserne af retten til beskyttelse af personoplysninger under alle faser af databehandlingen ([489]).

([485]) Se Artikel 29-Gruppen (2017), *Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen »sandsynligvis indebærer en høj risiko« i henhold til forordning (EU) 2016/679*, WP 248 rev. 01, Bruxelles, 4. oktober 2017. Se også ENISA (2015), Privacy and Data Protection by Design-from policy to engineering, 12. januar 2015.

([486]) Den moderniserede konvention 108, artikel 10, stk. 2 og 3, og forklarende rapport til den moderniserede konvention 108, stk. 89.

([487]) Generel forordning om databeskyttelse, artikel 25, stk. 2.

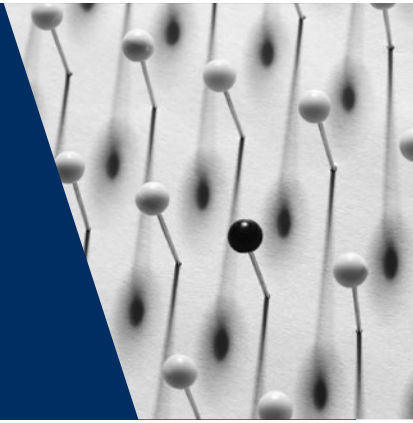
([488]) Den Europæiske Tilsynsførende for Databeskyttelse (EDPS), Necessity Toolkit Toolkit, Bruxelles, 11. april 2017.

([489]) Den moderniserede konvention 108, artikel 10, stk. 3, og forklarende rapport til den moderniserede konvention 108, stk. 89.

I 2016 offentliggjorde ENISA en rapport om tilgængelige værktøjer og tjenester til sikring af privatlivets fred ([490]). Blandt flere overvejelser giver denne vurdering et overblik over kriterier og parametre, som er indikatorer for gode eller dårlige praksisser til beskyttelse af privatlivets fred. Selvom nogle kriterier direkte omhandler bestemmelser i GDPR – såsom brugen af pseudonymisering og godkendte certificeringsmekanismer – indeholder andre nytænkende initiativer, der kan sikre privatlivets fred gennem design og gennem standardindstillinger. For eksempel kan kriteriet om brugervenlighed, selvom det ikke er direkte forbundet til privatlivets fred, forstærke beskyttelse af privatlivets fred, da det muliggør en bredere vedtagelse af et værktøj eller tjeneste til sikring af privatlivets fred. Værktøjer til sikring af privatlivets fred, som er vanskelige at implementere i praksis, kan nemlig have en meget lav udbredelse i den brede offentlighed, selv hvis de tilbyder en meget stærk garanti for sikring af privatlivets fred. Derudover er kriteriet om modenheden og stabiliteten af værktøjet til sikring af privatlivets fred — hvilket betyder måden, som et værktøj udvikler sig på over tid og reagerer på ved eksisterende eller nye udfordringer knyttet til privatlivets fred — meget vigtig. Andre privatlivsfremmende teknologier, for eksempel i forbindelse med sikker kommunikation, inkluderer ende til ende-kryptering (kommunikation, hvor de eneste, som kan læse meddelelserne, er de personer, som deltager i kommunikationen), kryptering mellem klient-server (kryptering af kommunikationskanalen imellem en klient og en server), autentifikation (verifikation af kommunikerende parters identiteter) og anonym kommunikation (ingen tredjemand kan identificere de kommunikerende parter).

([490]) ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, 20. december 2016.

5 Uafhængigt tilsyn



EU	Omhandlede emner	Europarådet
Chartret, artikel 8, stk. 3 Traktaten om Den Europæiske Unions funktionsmåde, artikel 16, stk. 2 Generel forordning om databeskyttelse, artikel 51-59 EU-Domstolen, C-518/07 , *Europa-Kommissionen mod Forbundsrepublikken Tyskland* [GC], 2010 EU-Domstolen, C-614/10, *Europa-Kommissionen mod Republikken Østrig* [GC], 2012 EU-Domstolen, C-288/12, *Europa-Kommissionen mod Ungarn* [GC], 2014 EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 2015	**Tilsynsmyndigheder**	Den moderniserede konvention 108, artikel 15
Generel forordning om databeskyttelse, artikel 60-67	**Samarbejde imellem tilsynsmyndigheder**	Den moderniserede konvention 108, artikel 16-21
Generel forordning om databeskyttelse, artikel 68-76	**Det Europæiske Databeskyttelsesråd**	

Hovedpunkter

- Uafhængigt tilsyn er en vigtig del af europæisk databeskyttelseslovgivning og er fastlagt i Chartrets artikel 8, stk. 3.
- For at sikre effektiv databeskyttelse skal der ved national lov etableres uafhængige tilsynsmyndigheder.
- Nationale tilsynsmyndigheder skal fungere med fuldstændig uafhængighed, som skal garanteres ved loven om oprettelsen af tilsynsmyndigheden og afspejles i dens specifikke organisation.
- Tilsynsmyndigheder har specifikke beføjelser og opgaver. Det drejer sig blandt andet om følgende:
  - at overvåge og fremme databeskyttelse på nationalt plan
  - at rådgive registrerede og dataansvarlige samt regeringen og den generelle offentlighed
  - at behandle klager og bistå registrerede i forbindelse med påståede krænkelser af databeskyttelsesrettighederne
  - at føre tilsyn med dataansvarlige og databehandlere.
- Tilsynsmyndigheder har også beføjelser til at gribe ind, om nødvendigt, ved at:
  - udstede advarsler, påtaler eller endda bøder til dataansvarlige og databehandlere
  - træffe afgørelser om, at oplysninger berigtiges, blokeres eller slettes
  - forbyde behandling eller udstede en administrativ bøde
  - indbringe sager for retten.
- Da behandling af personoplysninger ofte omfatter dataansvarlige, databehandlere og registrerede i forskellige stater, skal tilsynsmyndigheder samarbejde med hinanden ved grænseoverskridende sager for at sikre en effektiv beskyttelse af fysiske personer i Europa.
- I EU fastlægger den generelle forordning om databeskyttelse en one-stop-shop mekanisme for grænseoverskridende behandlingssager. Nogle virksomheder udfører grænseoverskridende behandlingsaktiviteter grundet behandling af personoplysninger i forbindelse med virksomheder med aktiviteter i mere end én medlemsstat eller i forbindelse med et enkelt foretagende i Unionen, men som i væsentlig grad påvirker registrerede i mere end én medlemsstat. Under mekanismen vil sådanne virksomheder kun være underlagt én national tilsynsmyndighed for databeskyttelse.

- En samarbejds- og sammenhængsmekanisme tillader en koordineret tilgang for alle tilsynsmyndighederne, som er omfattet af sagen. Den førende tilsynsmyndighed – for hovedvirksomheden eller et enkelt foretagende – vil rådføre sig hos og indsende sine beslutningsudkast til de andre tilknyttede tilsynsmyndigheder.
- Ligesom den daværende Artikel 29-Gruppe vil tilsynsmyndigheden i hver medlemsstat og Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) være en del af Det Europæiske Databeskyttelsesråd.
- Det Europæiske Databeskyttelsesråds arbejdsopgaver omfatter blandt andet overvågning af forordningens korrekte anvendelse, rådgivning til Kommissionen om relevante problemstillinger og udstedelse af udtalelser, retningslinjer eller bedste praksisser om en række forskellige emner.
- Den primære forskel er, at Det Europæiske Databeskyttelsesråd ikke kun udsteder udtalelser som under direktiv 95/46/EF. Det vil også udstede afgørelser om sager, hvor en tilsynsmyndighed har gjort en relevant og begrundet indsigelse i tilfælde med one-stop-shops; hvor der er modstridende holdninger om, hvilken tilsynsmyndighed der er den ledende, og endelig hvis den kompetente tilsynsmyndighed ikke anmoder om eller ikke følger EDPB's udtalelse. Målet er at sikre en ensartet anvendelse af forordningen i alle medlemsstater.

Uafhængigt tilsyn er en vigtig del af europæisk databeskyttelseslovgivning. Både EU-retten og Europarådets retsorden betragter tilstedeværelsen af uafhængige tilsynsmyndigheder som uundværlige for den effektive beskyttelse af fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandlingen af deres personoplysninger. Da databehandling er allestedsnærværende og stadig mere kompleks for enkeltpersoner at forstå, er disse tilsynsmyndigheder den digitale tidsalders vagthunde. I EU betragtes tilstedeværelsen af uafhængige tilsynsmyndigheder som ét af de vigtigste elementer af retten til beskyttelse af personoplysninger, som er fastlagt i primær EU-ret. Artikel 8, stk. 3, i EU's Charter om grundlæggende rettigheder og artikel 16, stk. 2, i TEUF anerkender beskyttelse af personoplysninger som en grundlæggende rettighed og bekræfter, at overholdelse af databeskyttelsesregler skal være underlagt en uafhængig myndigheds kontrol.

Retspraksis har også anerkendt betydningen af uafhængigt tilsyn for databeskyttelseslovgivningen.

Eksempel: I *Schrems* ([491])-sagen undersøgte EU-Domstolen, om videresendelse af personoplysninger til De Forenede Stater under den første safe harbour-aftale mellem EU og USA var i overensstemmelse med EU's databeskyttelseslovgivning på baggrund af Edward Snowdens afsløringer om det amerikanske nationale sikkerhedsagenturs udførelse af masseovervågning. Overførslen af personoplysninger til USA var baseret på Europa-Kommissionens beslutning vedtaget i 2000, som tillod, at personoplysninger overføres fra EU til amerikanske virksomheder, som foretager selvcertificering på baggrund af safe harbour-ordningen, ud fra den begrundelse, at ordningen sikrer et tilsvarende beskyttelsesniveau af personoplysningerne. Da den irske tilsynsmyndighed blev bedt om at undersøge sagsøgerens klage vedrørende lovligheden af dataoverførsler efter Snowdens afsløringer, afviste myndigheden klagen på baggrund af Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet for den amerikanske databeskyttelsesordning, som var afspejlet i safe harbour-principperne (»safe harbour-beslutningen«), der forhindrede denne i at undersøge klagen yderligere.

EU-Domstolen fastholdt dog, at tilstedeværelsen af en beslutning fra Kommissionen, der tillod dataoverførsler til tredjelande, som sikrer tilstrækkelige beskyttelsesniveauer, ikke fjerner eller reducerer nationale tilsynsmyndigheders beføjelser. EU-Domstolen bemærkede, at disse myndigheders beføjelser til at overvåge og sikre overholdelse af EU-regler om databeskyttelse stammer fra primær EU-ret, navnlig artikel 8, stk. 3, i Chartret og artikel 16, stk. 2, i TEUF. »Oprettelsen af uafhængige tilsynsmyndigheder i medlemsstaterne er derfor [...] af afgørende betydning for beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger« ([492]).

EU-Domstolen besluttede derfor, at selv hvis overførslen af personoplysninger er underlagt Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet, skal den nationale tilsynsmyndighed omhyggeligt undersøge en klage, når den indsendes til denne. Tilsynsmyndigheden kan afvise klagen, hvis den mener, at den er ubegrundet. I så fald understregede EU-Domstolen, at retten til effektive retsmidler kræver, at fysiske personer er i stand til at anfægte en sådan beslutning ved de nationale domstole, der kan henvise sagen til EU-Domstolen for en præjudiciel afgørelse om

([491]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015.

([492]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015, præmis 41.

gyldigheden af Kommissionens beslutning. Hvis tilsynsmyndigheden mener, at klagen er velbegrundet, skal den kunne indlede en retssag og indbringe sagen for de nationale domstole. De nationale domstole kan henvise sagen til EU-Domstolen, siden det er det eneste organ med beføjelser til at træffe afgørelse om gyldigheden af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet fra Kommissionen ([493]).

EU-Domstolen undersøgte derefter gyldigheden af safe harbour-beslutningen for at fastlægge, om systemet med videregivelser var i overensstemmelse med EU's databeskyttelsesregler. Den konstaterede, at artikel 3 i safe harbour-beslutningen begrænsede nationale tilsynsmyndigheders beføjelser (givet under databeskyttelsesdirektivet) til at træffe foranstaltninger til at forhindre dataoverførsler i tilfælde af et utilstrækkeligt databeskyttelsesniveau i USA. Grundet hvor vigtige uafhængige tilsynsmyndigheder er for at sikre overholdelse af databeskyttelseslovgivningen, fastholdt EU-Domstolen, at Kommissionen under databeskyttelsesdirektivet og læst ud fra Chartret ikke besad beføjelsen til at begrænse de uafhængige tilsynsmyndigheders beføjelser på denne måde. Begrænsningen af tilsynsmyndighedernes beføjelser var én af grundene til, at EU-Domstolen erklærede safe harbour-beslutningen for ugyldig.

EU-retten kræver dermed uafhængigt tilsyn som en vigtig mekanisme til at sikre effektiv databeskyttelse. Uafhængige tilsynsmyndigheder er det første kontaktpunkt for registrerede i tilfælde af krænkelser af privatlivets fred ([494]). Under EU-retten og Europarådets retsorden er udpegelse af tilsynsmyndigheder obligatorisk. Begge retsgrundlag beskriver disse myndigheders opgaver og beføjelser på en tilsvarende måde som i GDPR. Principielt bør tilsynsmyndigheder derfor fungere på samme måde under EU-retten og Europarådets retsorden ([495]).

5.1. Uafhængighed

EU-retten og **Europarådets retsorden** kræver, at alle tilsynsmyndigheder fungerer med fuldstændig uafhængighed under udøvelsen af deres opgaver og

([493]) *Ibid.*, præmis 53-66.

([494]) Generel forordning om databeskyttelse, artikel 13, stk. 2, litra d).

([495]) *Ibid.*, artikel 51, og den moderniserede konvention 108, artikel 15.

beføjelser ([496]). Uafhængigheden af tilsynsmyndigheden og dennes medlemmer samt personale fra direkte eller indirekte udefrakommende påvirkninger er nødvendig til at garantere komplet objektivitet ved træfning af afgørelser i sager vedrørende databeskyttelse. Lovgrundlaget for et tilsynsorgans oprettelse skal indeholde bestemmelser, som specifikt garanterer uafhængighed, og myndighedens organisatoriske struktur skal påvise uafhængighed. I 2010 undersøgte EU-Domstolen for første gang, i hvilket omfang tilsynsmyndigheder for databeskyttelse skal være uafhængige ([497]). De fremhævede eksempler viser EU-Domstolens definition af udtrykket »fuld uafhængighed«.

Eksempel: I sagen *Europa-Kommissionen mod Forbundsrepublikken Tyskland* ([498]) nedlagde Europa-Kommissionen påstand over for EU-Domstolen om, at Tyskland havde foretaget en ukorrekt gennemførelse af kravet om, at tilsynsmyndigheder med ansvar for at sikre databeskyttelse udøver deres funktioner »i fuld uafhængighed«, og således ikke havde opfyldt landets forpligtelser i medfør af databeskyttelsesdirektivets artikel 28, stk. 1. Ifølge Kommissionen var problemet, at Tyskland havde underlagt de nationale tilsynsmyndigheder, som overvåger beskyttelse af personoplysninger uden for den offentlige sektor i de forskellige delstater (*Länder*), statsligt tilsyn for at sikre overholdelse af databeskyttelseslovgivningen, hvilket overtrådte kravet om uafhængighed.

EU-Domstolen understregede, at udtrykket »i fuld uafhængighed« skal fortolkes på grundlag af den faktiske ordlyd af denne bestemmelse samt formålet og opbygningen af europæisk databeskyttelseslovgivning ([499]). EU-Domstolen fremhævede, at tilsynsmyndighederne er »vogtere« af rettigheder vedrørende behandling af personoplysninger. Deres oprettelse i medlemsstaterne er derfor »af afgørende betydning for beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger« ([500]). Domstolen konkluderede, at »når tilsynsmyndighederne udøver deres funktioner, skal

([496]) Generel forordning om databeskyttelse, artikel 52, stk. 1, og den moderniserede konvention 108, artikel 15, stk. 5.

([497]) FRA (2010), *Fundamental rights: challenges and achievements in 2010*, årlig rapport 2010, s. 59 og FRA (2010), *Data protection in the European Union: the role of National Data Protection Authorities*, maj 2010.

([498]) EU-Domstolen, C-518/07, *Europa-Kommissionen mod Forbundsrepublikken Tyskland* [GC], 9. marts 2010, præmis 27.

([499]) *Ibid.*, præmis 17 og 29.

([500]) *Ibid.*, præmis 23.

de handle objektivt og upartisk. De skal derfor beskyttes imod enhver form for ydre påvirkning, herunder direkte eller indirekte påvirkning fra staten eller delstaterne« ([501]).

EU-Domstolen fandt også, at betydningen af »i fuld uafhængighed« skal fortolkes i lyset af EDPS' uafhængighed som defineret i forordningen om databeskyttelse inden for EU-institutionerne. I denne forordning kræver uafhængighedsbegrebet, at EDPS hverken må søge eller modtage instrukser fra andre.

EU-Domstolen fastslog følgelig, at tyske tilsynsmyndigheder ikke var fuldstændigt uafhængige i medfør af europæisk databeskyttelseslovgivning, da de var underlagt tilsyn fra offentlige myndigheder.

Eksempel: I sagen *Kommissionen mod Republikken Østrig* ([502]) fremhævede EU-Domstolen lignende problemer vedrørende uafhængigheden af visse medlemmer af og medarbejdere hos den østrigske databeskyttelsesmyndighed (Datenschutzkommission, DSK). Domstolen konkluderede i den sag, at det faktum, at forbundskanslerens kontor leverede tilsynsmyndighedens arbejdsstyrke, var i strid med kravet om uafhængighed defineret i europæisk databeskyttelseslovgivning. EU-Domstolen fastholdt yderligere, at kravet pålagt tilsynsmyndigheden om konstant at informere forbundskansleren om sit arbejde var i strid med førnævntes fuldstændige uafhængighed.

Eksempel: I sagen *Europa-Kommissionen mod Ungarn* ([503]) var lignende nationale praksisser, som påvirkede arbejdsstyrkens uafhængighed, blevet forbudt. EU-Domstolen fremhævede, at det skal undersøges, »om det krav [...] hvorefter det skal sikres, at hver tilsynsmyndighed udøver de funktioner, der tillægges dem, i fuld uafhængighed, således som Kommissionen påstår, omfatter forpligtelsen til for den berørte medlemsstat at respektere varigheden af en sådan myndigheds mandat indtil mandatets oprindeligt fastsatte udløb«. EU-Kommissionen anførte endvidere at, »Ungarn har tilsidesat sine

([501]) *Ibid.*, præmis 25.

([502]) EU-Domstolen, C-614/10 , *Europa-Kommissionen mod Republikken Østrig* [GC], 16. oktober 2012, præmis 59 og 63.

([503]) EU-Domstolen, C-288/12 , Europa-*Kommissionen mod Ungarn* [GC], 8. april 2014, præmis 50 og 67.

> forpligtelser i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF […], idet Ungarn har bragt mandatet for tilsynsmyndigheden for beskyttelse af personoplysninger til ophør før tid«.

Begrebet og kriteriet om »i fuld uafhængighed« er nu udtrykkeligt fastlagt i GDPR, som indarbejder principperne fastlagt i de beskrevne afgørelser fra EU-Domstolen. I medfør af forordningen indebærer fuld uafhængighed under udøvelse af opgaver og beføjelser, at ([504]):

- medlemmerne af hver enkelt tilsynsmyndighed forbliver frie fra ydre påvirkning — direkte eller indirekte — og må ikke modtage instrukser fra andre
- medlemmerne afholder sig fra enhver handling, der er uforenelig med deres hverv, for at forhindre interessekonflikter
- medlemsstater forsyner de enkelte tilsynsmyndigheder med de fornødne menneskelige, tekniske og økonomiske ressourcer og infrastruktur til effektivt at kunne udføre deres opgaver
- medlemsstater sikrer, at hver tilsynsmyndighed vælger sine egne medarbejdere
- den finansielle kontrol, som hver tilsynsmyndighed er underlagt i henhold til national lovgivning, ikke påvirker dennes uafhængighed. Tilsynsmyndigheder skal have særskilte og offentlige årsbudgetter, som gør dem i stand til at fungere ordentligt.

Tilsynsmyndigheders uafhængighed anses også for at være et væsentligt krav under Europarådets retsorden. Den moderniserede konvention 108 kræver, at tilsynsmyndigheder fungerer med fuldstændig uafhængighed og upartiskhed under udøvelse af deres beføjelser uden at søge eller modtage instrukser ([505]). På denne måde anerkender konventionen, at disse myndigheder ikke kan sikre fysiske personers rettigheder og frihedsrettigheder i forbindelse med databehandling på effektiv vis, medmindre de udøver deres funktioner med fuld uafhængighed. Den forklarende rapport til den moderniserede konvention 108 fastlægger en række elementer, der bidrager til at sikre denne uafhængighed. Sådanne elementer omfatter muligheden for, at tilsynsmyndigheder kan ansætte deres egne

([504]) Generel forordning om databeskyttelse, artikel 69.

([505]) Den moderniserede konvention 108, artikel 15, stk. 5.

medarbejdere og vedtage beslutninger uden at være underlagt udefrakommende påvirkninger, samt faktorer vedrørende varigheden af udøvelsen af deres funktioner og de betingelser, hvorunder de kan ophøre med deres funktioner ([506]).

5.2. Kompetencer og beføjelser

I EU-retten fremhæver GDPR kompetencerne og den organisatoriske struktur for tilsynsmyndigheder og påbyder, at de skal være kompetente og besidde beføjelserne til at udføre opgaverne krævet under forordningen.

Tilsynsmyndigheden er det primære organ inden for national lovgivning, som sikrer overholdelse af europæisk databeskyttelseslovgivning. Tilsynsmyndigheder har en omfattende liste over opgaver og beføjelser, som ikke bare omfatter overvågning men også proaktive og forebyggende tilsynsaktiviteter. For at udføre disse opgaver skal tilsynsmyndigheder besidde passende undersøgelsesmæssige, korrigerende og rådgivningsmæssige beføjelser, som er anført i artikel 57 og 58 i GDPR, så de kan ([507]):

- rådgive dataansvarlige og registrerede om alle emner vedrørende databeskyttelse
- godkende standardkontraktbestemmelser, bindende virksomhedsregler eller administrative ordninger
- undersøge behandlingsaktiviteter og følgelig gribe ind
- kræve indsendelse af alle relevante oplysninger for tilsyn med dataansvarliges aktiviteter
- advare eller kritisere dataansvarlige og give påbud om, at underrette registrerede ved brud på persondatasikkerheden
- give påbud om berigtigelse, blokering, sletning eller tilintetgørelse af personoplysninger

([506]) Forklarende rapport til den moderniserede konvention 108.

([507]) Generel forordning om databeskyttelse, artikel 57 og 58. Se også konvention 108, supplerende protokol, artikel 1.

- midlertidigt eller definitivt forbyde behandling eller udstede administrative bøder

- indbringe en sag for en domstol.

For at kunne udøve sine funktioner skal en tilsynsmyndighed have adgang til alle personoplysninger og informationer, der er nødvendige i forbindelse med en undersøgelse, og have adgang til lokaliteter, hvor en dataansvarlig opbevarer relevante informationer. I henhold til EU-Domstolen skal tilsynsmyndigheders beføjelser fortolkes bredt for at sikre den fulde effektivitet af databeskyttelse for registrerede i EU.

Eksempel: I *Schrems*-sagen undersøgte EU-Domstolen, om overførsel af personoplysninger til De Forenede Stater under den første safe harbour-aftale mellem EU og USA var i overensstemmelse med EU's databeskyttelseslovgivning på baggrund af Edward Snowdens afsløringer. EU-Domstolen argumenterede, at nationale tilsynsmyndigheder – der handler i deres egenskab som uafhængige inspektører af dataansvarliges databehandling – kan forhindre oplysninger i at blive overført til et tredjeland på trods af eksistensen af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, hvis der er rimelig dokumentation for, at den tilstrækkelige beskyttelse ikke længere garanteres i tredjelandet ([508]).

Den enkelte tilsynsmyndighed besidder kompetencer til at udøve undersøgelsesbeføjelser og beføjelser til at gribe ind inden for dennes territorium. Men da dataansvarliges og databehandleres aktiviteter ofte er grænseoverskridende, og databehandling påvirker registrerede i flere medlemsstater, opstår der et spørgsmål om kompetencefordelingen imellem de forskellige tilsynsmyndigheder. EU-domstolen havde mulighed for at undersøge dette problem i *Weltimmo*-sagen.

Eksempel: I *Weltimmo* ([509])-sagen undersøgte EU-Domstolen nationale tilsynsmyndigheders kompetencer til at håndtere problemstillinger, som omfattede organisationer, der ikke var etableret inden for deres område. Weltimmo var en virksomhed registreret i Slovakiet, som drev en internetside med

([508]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner*, [GC] 6. oktober 2015, præmis 26-36 og 40-41.

([509]) EU-Domstolen, C-230/14, *Weltimmo s.r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. oktober 2015.

ejendomsannoncer for ungarske ejendomme. Annoncører indsendte en klage til den ungarske tilsynsmyndighed for databeskyttelse om overtrædelse af den ungarske databeskyttelseslovgivning, og myndigheden udstedte en bøde til Weltimmo. Virksomheden anfægtede bøden ved de nationale domstole, og sagen blev henvist til EU-Domstolen for at fastlægge, om EU's databeskyttelsesdirektiv tillod, at en medlemsstats tilsynsmyndigheder anvendte deres nationale databeskyttelseslovgivning på en virksomhed, som er registreret i en anden medlemsstat.

EU-Domstolen fortolkede artikel 4, stk. 1, litra a), i databeskyttelsesdirektivet som at tillade anvendelsen af databeskyttelseslovgivning for en medlemsstat, som ikke er den medlemsstat, hvori den dataansvarlige er registreret, »for så vidt som denne via en permanent struktur på denne medlemsstats område udøver en, selv minimal, faktisk og reel aktivitet, som led i hvilken denne behandling foretages«. EU-Domstolen bemærkede, at Weltimmo på baggrund af de oplysninger, denne besad, forfulgte en faktisk og reel aktivitet i Ungarn, da virksomheden havde en repræsentant i Ungarn, som var optaget i det slovakiske selskabsregister med en ungarsk adresse, samt en ungarsk bankkonto og postboks, og derudover forfulgte den aktiviteter i Ungarn, som var forfattet på ungarsk. Disse oplysninger tydede på, at der var tale om en virksomhed, hvilket ville betyde, at Weltimmos aktiviteter var underlagt ungarsk databeskyttelseslovgivning og den ungarske tilsynsmyndigheds kompetence. EU-Domstolen lod dog den nationale domstol om at bekræfte oplysningerne og beslutte, om Weltimmo var etableret i Ungarn.

Hvis den forelæggende domstol konstaterede, at Weltimmo var etableret i Ungarn, ville den ungarske tilsynsmyndighed have beføjelse til at pålægge en bøde. Hvis den nationale domstol besluttede det modsatte, dvs. at Weltimmo ikke var etableret i Ungarn, ville den gældende lov være den for den/de medlemsstat(er), hvori virksomheden var registreret. I så tilfælde ville den ungarske myndighed ikke kunne pålægge sanktioner, da tilsynsmyndigheders beføjelser skal udøves i henhold til andre medlemsstaters territoriale suverænitet. Da databeskyttelsesdirektivet indeholdt en forpligtelse om samarbejde for tilsynsmyndigheder, kan den ungarske myndighed dog anmode sit slovakiske modstykke om at undersøge sagen, fastlægge en overtrædelse af slovakisk lovgivning og pålægge sanktionerne fastlagt i den slovakiske lovgivning.

Med vedtagelsen af GDPR er der nu fastlagt detaljerede regler vedrørende tilsynsmyndigheders kompetencer i grænseoverskridende sager. Forordningen fastlægger en »one-stop-shop mekanisme« og indeholder bestemmelser, som foreskriver samarbejde mellem forskellige tilsynsmyndigheder. For effektivt samarbejde ved grænseoverskridende sager kræver GDPR, at der udpeges en ledende tilsynsmyndighed som tilsynsmyndigheden for den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering ([510]). Den ledende tilsynsmyndighed er ansvarlig for grænseoverskridende sager, er den dataansvarliges eller databehandlerens eneste kontakt og koordinerer samarbejdet med andre tilsynsmyndigheder med henblik på at nå til enighed. Samarbejdet omfatter udveksling af oplysninger, gensidig bistand med overvågning og undersøgelser og vedtagelse af bindende beslutninger ([511]).

I Europarådets retsorden er tilsynsmyndigheders kompetencer og beføjelser fastlagt i artikel 15 i den moderniserede konvention 108. Disse beføjelser svarer til dem givet til tilsynsmyndigheder under EU-retten, herunder beføjelser til undersøgelse og til at gribe ind, beføjelser til at udstede beslutninger og pålægge administrative sanktioner vedrørende overtrædelser af konventionens bestemmelser og beføjelser til at indlede retssager. Uafhængige tilsynsmyndigheder besidder også kompetencer til at håndtere anmodninger og klager indsendt af registrerede, øge offentlighedens bevidsthed om databeskyttelseslovgivningen og rådgive nationale beslutningstagere i forbindelse med lovmæssige eller administrative foranstaltninger, som tilvejebringer behandling af personoplysninger.

5.3. Samarbejde

GDPR fastlægger generelle rammer for samarbejde mellem tilsynsmyndigheder og giver detaljerede regler for samarbejde mellem tilsynsmyndigheder ved grænseoverskridende databehandlingsaktiviteter.

I medfør af GDPR skal tilsynsmyndigheder yde gensidig bistand og dele relevante oplysninger for at gennemføre og anvende forordningen på en ensartet måde ([512]). Dette omfatter, at den anmodede tilsynsmyndighed udfører høringer, inspektioner og undersøgelser. Tilsynsmyndigheder kan udføre fælles aktiviteter, herunder

([510]) Generel forordning om databeskyttelse, artikel 56, stk. 1.

([511]) *Ibid.*, artikel 60.

([512]) *Ibid.*, artikel 61, stk. 1-3, og artikel 62, stk. 1.

fælles undersøgelses- og håndhævelsesforanstaltninger, som medarbejdere fra alle tilsynsmyndigheder deltager i ([513]).

I EU fungerer dataansvarlige og databehandlere i stigende grad på tværs af nationale grænser. Dette kræver et tæt samarbejde mellem de kompetente tilsynsmyndigheder i medlemsstaterne for at sikre, at behandlingen af personoplysninger overholder GDPR's krav. Hvis en dataansvarlig eller databehandler er etableret i flere medlemsstater, eller hvis denne er etableret et enkelt sted, men behandlingsaktiviteterne i væsentlig grad påvirker registrerede i mere end én medlemsstat, er tilsynsmyndigheden for hovedvirksomheden (eller det enkelte foretagende) under forordningens »one-stop-shop mekanisme« den ledende tilsynsmyndighed for den dataansvarliges eller databehandlerens grænseoverskridende aktiviteter. Ledende tilsynsmyndigheder besidder beføjelser til at træffe håndhævelsesforanstaltninger mod den dataansvarlige eller databehandleren. One-stop-shop mekanismen har til formål at forbedre harmonisering og den ensartede anvendelse af europæisk databeskyttelseslovgivning i forskellige medlemsstater. Den er også til fordel for virksomheder, da de kun skal have kontakt med den ledende tilsynsmyndighed i stedet for flere tilsynsmyndigheder. Dette forbedrer retssikkerheden for virksomheder, og i praksis bør det også betyde, at beslutninger træffes hurtigere, og at virksomheder ikke udsættes for, at forskellige tilsynsmyndigheder pålægger dem modstridende krav.

Identifikation af den ledende tilsynsmyndighed indebærer, at placeringen af et foretagendes hovedvirksomhed i EU bestemmes. Udtrykket »hovedvirksomhed« er defineret i GDPR. Derudover har Artikel 29-Gruppen udstedt retningslinjer for identifikation af en ledende tilsynsmyndighed for en dataansvarlig eller databehandler, hvilket omfatter kriterier for at udpege hovedvirksomheden ([514]).

For at sikre et højt niveau af databeskyttelse i EU handler den ledende tilsynsmyndighed ikke alene. Den skal samarbejde med andre berørte tilsynsmyndigheder ved vedtagelsen af beslutninger om dataansvarliges og databehandleres behandling af personoplysninger for at opnå enighed og sikre sammenhæng. Samarbejdet imellem relevante tilsynsmyndigheder omfatter udveksling af oplysninger, gensidig bistand og udførelse af fælles undersøgelses- og overvågningsaktiviteter ([515]). Når

([513]) *Ibid*., artikel 62, stk. 1.

([514]) Artikel 29-Gruppen (2016), Retningslinjer for udpegelse af en ledende tilsynsmyndighed for en dataansvarlig eller databehandler, WP 244, Bruxelles, 13. december 2016, revideret den 5. april 2017.

([515]) Generel forordning om databeskyttelse, artikel 60, stk. 1-3.

tilsynsmyndigheder yder gensidig bistand til hinanden, skal de korrekt håndtere anmodninger om oplysninger fra andre tilsynsmyndigheder og gennemføre tilsynsforanstaltninger, som f.eks. forudgående godkendelser og høringer med den dataansvarlige om dennes behandlingsaktiviteter, inspektioner eller undersøgelser. Gensidig bistand til tilsynsmyndigheder i andre medlemsstater skal ydes efter anmodning uden unødig forsinkelse og senest en måned efter modtagelse af anmodningen ([516]).

Når den dataansvarlige er etableret i flere medlemsstater, kan tilsynsmyndighederne udføre fælles aktiviteter, herunder undersøgelses- og håndhævelsesforanstaltninger, som medarbejdere fra tilsynsmyndighederne i andre medlemsstater deltager i ([517]).

Samarbejdet mellem forskellige tilsynsmyndigheder er også et vigtigt krav under Europarådets retsorden. Den moderniserede konvention 108 fastsætter, at tilsynsmyndigheder skal samarbejde med hinanden i det omfang, som er nødvendigt til at udføre deres opgaver ([518]). Dette bør for eksempel gennemføres ved at udveksle alle relevante og brugbare oplysninger og ved at koordinere undersøgelser og udføre fælles aktioner ([519]).

5.4. Det Europæiske Databeskyttelsesråd

Dette kapitel har tidligere beskrevet betydningen af uafhængige tilsynsmyndigheder og de primære kompetencer, de besidder under europæisk databeskyttelseslovgivning. Det Europæiske Databeskyttelsesråd (EDPB) er en anden vigtig aktør til at sikre, at databeskyttelsesregler anvendes effektivt og konsistent i hele EU.

GDPR oprettede EDPB som et EU-organ med status som en juridisk person ([520]). Det erstatter Artikel 29-Gruppen ([521]), som databeskyttelsesdirektivet oprettede for at rådgive Kommissionen om EU-foranstaltninger, som påvirkede enkeltpersoners rettigheder vedrørende behandling af personoplysninger og

([516]) *Ibid.*, artikel 61, stk. 1 og 2.

([517]) *Ibid.*, artikel 62, stk. 1.

([518]) Den moderniserede konvention 108, artikel 16 og 17.

([519]) *Ibid.*, artikel 17.

([520]) Generel forordning om databeskyttelse, artikel 68.

([521]) Under direktiv 95/46/EF skulle Artikel 29-Gruppen rådgive Kommissionen om EU-foranstaltninger, som påvirkede enkeltpersoners rettigheder vedrørende behandling af personoplysninger og beskyttelse af privatlivets fred, fremme direktivets ensartede anvendelse og give ekspertudtalelser til Kommissionen i forbindelse med sager omkring databeskyttelse. Artikel 29-Gruppen bestod af repræsentanter fra tilsynsmyndigheder i EU's medlemsstater samt Kommissionen og EDPS.

beskyttelse af privatlivets fred, fremme direktivets ensartede anvendelse og give ekspertudtalelser til Kommissionen i forbindelse med sager omkring databeskyttelse. Artikel 29-Gruppen bestod af repræsentanter fra tilsynsmyndigheder i EU's medlemsstater samt repræsentanter fra Kommissionen og EDPS.

Ligesom Artikel 29-Gruppen består EDPB af cheferne for tilsynsmyndighederne i hver medlemsstat og EDPS eller deres repræsentanter ([522]). EDPS har lige stemmeret, undtagen i sager vedrørende bilæggelse af tvister, hvor det kun kan stemme på afgørelser vedrørende principper og regler, som er gældende for EU-institutioner, der indholdsmæssigt svarer til dem i GDPR. Kommissionen har ret til at deltage i EDPB's aktiviteter og møder, men har ikke stemmeret ([523]). Databeskyttelsesrådets vælger en formand (som det repræsenteres af) og to næstformænd blandt sine medlemmer med simpelt flertal for en embedsperiode på fem år. Derudover har EDPB også et sekretariat, som EDPS stiller til rådighed, så Databeskyttelsesrådet har analytisk, administrativ og logistisk støtte ([524]).

EDPB's opgaver er beskrevet i artikel 64, 65 og 70 i GDPR og består af omfattende pligter, der kan inddeles i tre hovedaktiviteter:

- **Sammenhæng:** EDPB kan udstede juridisk bindende afgørelser i tre tilfælde: hvor en tilsynsmyndighed har gjort en relevant og begrundet indsigelse i tilfælde med one-stop-shops, når der er modstridende holdninger om, hvilken tilsynsmyndighed er den ledende, og endelig hvis den kompetente tilsynsmyndighed ikke anmoder om eller ikke følger EDPB's udtalelse ([525]). EDPB's hovedansvar er at sikre, at GDPR anvendes ensartet i hele EU, og det spiller en vigtig rolle i sammenhængsmekanismen som beskrevet i afsnit 5.5.

- **Høring:** EDPB's opgaver omfatter rådgivning til Kommissionen om alle spørgsmål vedrørende beskyttelse af personoplysninger i EU, såsom ændringer af GDPR; revisioner af EU-lovgivning, der omfatter databehandling og kan være i konflikt med europæiske databeskyttelsesregler, eller udstedelsen af Kommissionens beslutninger om tilstrækkelighed, der muliggør overførsel af personoplysninger til et tredjeland eller en international organisation.

([522]) Generel forordning om databeskyttelse, artikel 68, stk. 3.

([523]) *Ibid.*, artikel 68, stk. 4 og 5.

([524]) *Ibid.*, artikel 73 og 75.

([525]) *Ibid.*, artikel 65.

- **Vejledning:** Databeskyttelsesrådet udsteder også retningslinjer, henstillinger og bedste praksis for at fremme forordningens ensartede anvendelse og fremmer samarbejde og udveksling af oplysninger mellem tilsynsmyndigheder. Derudover skal det tilskynde sammenslutninger af dataansvarlige eller databehandlere til at udarbejde adfærdskodekser og fastlægge certificeringsmekanismer for databeskyttelse og databeskyttelsesmærkninger.

EDPB's beslutninger kan anfægtes ved EU-Domstolen.

5.5. GDPR's sammenhængsmekanisme

GDPR fastlægger en sammenhængsmekanisme for at sikre, at forordningen anvendes ensartet i medlemsstaterne, hvormed tilsynsmyndighederne samarbejder med hinanden og, om relevant, med Kommissionen. Sammenhængsmekanismen anvendes i to situationer. Den første vedrører EDPB's udtalelser i tilfælde, hvor en kompetent tilsynsmyndighed planlægger at vedtage foranstaltninger, såsom en liste over behandlingsaktiviteter, som kræver en konsekvensanalyse vedrørende databeskyttelse (DPIA), eller bestemme standardkontraktbestemmelser. Den anden omhandler EDPB's bindende beslutninger for tilsynsmyndigheder i one-stop-shop-tilfælde, og når en tilsynsmyndighed ikke følger eller ikke anmoder om en udtalelse fra EDPB.

6

De registreredes rettigheder og håndhævelsen heraf

EU	Omhandlede emner	Europarådet
Ret til at blive underrettet		
Generel forordning om databeskyttelse, artikel 12 EU-Domstolen, C-473/12, *Institut professionnel des agents immobiliers (IPI) mod Geoffrey Englebert*, 2013 EU-Domstolen, C-201/14, *Smaranda Bara m.fl. mod Casa Națională de Asigurări de Sănătate m.fl.*, 2015	**Gennemsigtighed af oplysninger**	Den moderniserede konvention 108, artikel 8
Generel forordning om databeskyttelse, artikel 13, stk. 1 og 2, og artikel 14, stk. 1 og 2	**Indhold af informationerne**	Den moderniserede konvention 108, artikel 8, stk. 1
Generel forordning om databeskyttelse, artikel 13, stk. 1, og artikel 14, stk. 3	**Tidspunkt for meddelelse**	Den moderniserede konvention 108, artikel 9, stk. 1, litra b)
Generel forordning om databeskyttelse, artikel 12, stk. 1, 5 og 7	**Metoder til meddelelse**	Den moderniserede konvention 108, artikel 9, stk. 1, litra b)
Generel forordning om databeskyttelse, artikel 13, stk. 2, litra d), artikel 14, stk. 2, litra e), og artikel 77, 78 og 79	**Ret til at indgive klage**	Den moderniserede konvention 108, artikel 9, stk. 1, litra f)

EU	Omhandlede emner	Europarådet
Ret til aktindsigt		
Generel forordning om databeskyttelse, artikel 15, stk. 1 EU-Domstolen, C-553/07, *College van burgemeester en wethouders van Rotterdam mod M. E. E. Rijkeboer*, 2009 EU-Domstolen, forenede sager C-141/12 og C-372/12, *YS mod Minister voor Immigratie, Integratie en Asiel* og *Minister voor Immigratie, Integratie en Asiel mod M og S*, 2014 EU-Domstolen, C-434/16, *Peter Nowak mod Data Protection Commissioner*, 2017	**Ret til indsigt i egne oplysninger**	Den moderniserede konvention 108, artikel 9, stk. 1, litra b) EMD, *Leander mod Sverige*, nr. 9248/81, 1987
Ret til berigtigelse		
Generel forordning om databeskyttelse, artikel 16	**Berigtigelse af urigtige personoplysninger**	Den moderniserede konvention 108, artikel 9, stk. 1, litra e) EMD, *Cemalettin Canli mod Tyrkiet*, nr. 22427/04, 2008 EMD, *Ciubotaru mod Moldova*, nr. 27138/04, 2010
Ret til sletning		
Generel forordning om databeskyttelse, artikel 17, stk. 1	**Sletning af personoplysninger**	Den moderniserede konvention 108, artikel 9, stk. 1, litra e) EMD, *Segerstedt-Wiberg m.fl. mod Sverige*, nr. 62332/00, 2006
EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 2014 EU-Domstolen, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 2017	**Retten til at blive glemt**	

EU	Omhandlede emner	Europarådet
Ret til begrænsning af behandling		
Generel forordning om databeskyttelse, artikel 18, stk. 1	Ret til begrænsning af brugen af personoplysninger	
Generel forordning om databeskyttelse, artikel 19	Underretningspligt	
Ret til dataportabilitet		
Generel forordning om databeskyttelse, artikel 20	Ret til dataportabilitet	
Ret til indsigelse		
Generel forordning om databeskyttelse, artikel 21, stk. 1 EU-Domstolen, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 2017	Ret til indsigelse i medfør af den registreredes særlige situation	Henstilling om profilering, artikel 5.3 Den moderniserede konvention 108, artikel 9, stk. 1, litra d)
Generel forordning om databeskyttelse, artikel 21, stk. 2	Ret til indsigelse mod behandling af oplysninger med henblik på markedsføring	Henstilling om direkte markedsføring, artikel 4.1
Generel forordning om databeskyttelse, artikel 21, stk. 5	Ret til indsigelse gennem automatiske midler	
Rettigheder vedrørende automatiske afgørelser og profilering		
Generel forordning om databeskyttelse, artikel 22	Rettigheder vedrørende automatiske afgørelser og profilering	Den moderniserede konvention 108, artikel 9, stk. 1, litra a)
Generel forordning om databeskyttelse, artikel 21	Ret til indsigelse mod automatiske afgørelser	
Generel forordning om databeskyttelse, artikel 13, stk. 2, litra f)	Ret til en meningsfuld forklaring	Den moderniserede konvention 108, artikel 9, stk. 1, litra c)

EU	Omhandlede emner	Europarådet
Retsmidler, ansvar, sanktioner og erstatning		
Chartret, artikel 47 EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 2015 Generel forordning om databeskyttelse, artikel 77-84	**For overtrædelser af den nationale databeskyttelses-lovgivning**	EMRK, artikel 13 (kun for Europarådets medlemsstater) Den moderniserede konvention 108, artikel 9, stk. 1, litra f), artikel 12, 15 og 16-21 EMD, *K.U. mod Finland*, nr. 2872/02, 2008 EMD, *Biriuk mod Litauen*, nr. 23373/03, 2008
Forordningen om databeskyttelse inden for EU-institutionerne, artikel 34 og 49 EU-Domstolen, C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd* [GC], 2010	**For overtrædelser af EU-retten begået af EU-institutioner og -organer**	

Effektiviteten af juridiske regler generelt og registreredes rettigheder i særdeleshed afhænger i betydelig grad af adgangen til hensigtsmæssige håndhævelsesmekanismer. I den digitale tidsalder er databehandling blevet allestedsnærværende og sværere at forstå for enkeltpersoner. For at mindske skævheden i magtbalancen mellem registrerede og dataansvarlige har fysiske personer fået tildelt visse rettigheder til at udøve større kontrol over behandlingen af deres personoplysninger. Retten til adgang i sine egne oplysninger og retten til at berigtige disse er fastlagt i artikel 8, stk. 2, i EU's charter om grundlæggende rettigheder, hvilket er et dokument, der indgår i EU's primære ret og har en grundlæggende værdi inden for EU's retsorden. Afledt EU-ret – navnlig den generelle forordning om databeskyttelse – har fastlagt en sammenhænde lovramme, som styrker registreredes status ved at tillægge dem rettigheder i forbindelse med dataansvarlige. Udover rettighederne til adgang og berigtigelse anerkender GDPR en række andre rettigheder, såsom retten til sletning (»retten til at blive glemt«), retten til at gøre indsigelse eller begrænse databehandling og rettigheder vedrørende automatiske afgørelser og profilering. Lignende garantier, som gør registrerede i stand til at udøve effektiv kontrol over deres oplysninger, er også inkluderet i den moderniserede konvention 108. Artikel 9 angiver de rettigheder, som fysiske personer bør kunne udøve vedrørende behandlingen af deres personoplysninger. Kontraherende parter skal sikre, at disse rettigheder tillægges alle registrerede i deres område og ledsages af effektive retsmidler og praktiske midler, som gør registrerede i stand til at udøve disse.

Udover at tildele registrerede rettigheder er det ligeså vigtigt at fastlægge mekanismer, som gør registrerede i stand til at anfægte krænkelser af deres rettigheder, holde dataansvarlige ansvarlige og kræve erstatning. Retten til effektive retsmidler, hvilket garanteres under EMRK og Chartret, kræver, at alle personer har adgang til retsmidler.

6.1. De registreredes rettigheder

Hovedpunkter

- Alle registrerede har ret til information om en dataansvarligs behandling af vedkommendes oplysninger, underlagt visse undtagelser.
- Registrerede har ret til at:
  - få adgang til deres egne oplysninger og modtage visse informationer om behandlingen
  - få deres oplysninger berigtiget af den dataansvarlige, som behandler oplysningerne, hvis oplysningerne er urigtige
  - få deres oplysninger slettet af den dataansvarlige, hvis denne behandler deres oplysninger ulovligt
  - midlertidigt begrænse behandling
  - få deres oplysninger overført til en anden dataansvarlig under visse betingelser.
- Derudover skal registrerede have ret til at gøre indsigelse mod behandling:
  - på baggrund af deres særlige situation
  - når det finder sted med henblik på direkte markedsføring.
- Registrerede skal have retten til ikke at være underlagt afgørelser udelukkende baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende. Registrerede har også ret til:
  - menneskelig indgriben fra den dataansvarliges side
  - at fremkomme med deres synspunkter og til at bestride en afgørelse baseret på automatisk behandling.

6.1.1. Ret til at blive underrettet

I medfør af **Europarådets retsorden** samt **EU-retten** er dataansvarlige for behandlingsaktiviteter forpligtede til at underrette den registrerede omkring den planlagte behandling af deres personoplysninger ved tidspunktet, hvor disse indsamles. Denne forpligtelse afhænger ikke af en anmodning fra den registrerede. I stedet skal den dataansvarlige proaktivt overholde forpligtelsen, uanset om den registrerede viser interesse i informationen eller ej.

Under Europarådets retsorden, i henhold til artikel 8 i den moderniserede konvention 108, skal kontraherende parter foreskrive, at dataansvarlige underretter de registrerede om deres identitet og sædvanlige opholdssted, behandlingens lovgrundlag og formål, kategorierne for de behandlede personoplysninger, modtagerne af deres personoplysninger (om nogen) og hvordan de kan udøve deres rettigheder under artikel 9, hvilket omfatter retten til adgang, berigtigelse og retsmidler. Alle andre yderligere oplysninger, der anses som nødvendige til at sikre en rimelig og gennemsigtig behandling af personoplysninger, skal også meddeles til de registrerede. Den forklarende rapport til den moderniserede konvention 108 præciserer, at informationen fremført for de registrerede skal være lettilgængelig, læsbar, forståelig og tilpasset til de relevante registrerede ([526]).

Under EU-retten kræver princippet om gennemsigtighed, at enhver behandling af personoplysninger generelt skal være gennemsigtig for fysiske personer. Fysiske personer har ret til at vide, hvilke personoplysninger som indsamles, bruges eller på anden måde behandles og hvordan, og de skal underrettes om risici, garantier og deres egne rettigheder vedrørende behandlingen ([527]). Artikel 12 i GDPR fastlægger dermed en bred omfattende forpligtelse for dataansvarlige om at give gennemsigtige informationer og/eller kommunikere, hvordan registrerede kan udøve deres rettigheder ([528]). Informationen skal være kortfattet, gennemsigtig, letforståelig og lettilgængelig i et klart og enkelt sprog. Den skal gives skriftligt, herunder, hvis det er hensigtsmæssigt, elektronisk. Den kan endda gives mundtligt, hvis den registrerede anmoder om det, forudsat at den registreredes identitet klart er bevist. Informationen skal gives uden unødig forsinkelse og være gratis ([529]).

([526]) Forklarende rapport til den moderniserede konvention 108, stk. 68.

([527]) Generel forordning om databeskyttelse, betragtning 39.

([528]) *Ibid.*, artikel 13 og 14, og den moderniserede konvention 108, artikel 8, stk. 1, litra b).

([529]) Generel forordning om databeskyttelse, artikel 12, stk. 5, og den moderniserede konvention 108, artikel 9, stk. 1, litra b).

Artikel 13 og 14 i GDPR omhandler henholdsvis registreredes ret til at blive underrettet enten i situationer, hvor personoplysninger blev indsamlet direkte fra dem, eller i situationer, hvor oplysningerne ikke blev indhentet fra dem.

Omfanget af retten til at blive underrettet og dennes begrænsninger under EU-retten er præciseret i EU-Domstolens retspraksis.

Eksempel: I sagen *Institut professionnel des agents immobiliers (IPI) mod Geoffrey Englebert* ([530]) blev EU-Domstolen bedt om at fortolke artikel 13, stk. 1, i direktiv 95/46/EF. Denne artikel gav medlemsstaterne valget om at vedtage retsakter til at begrænse omfanget af den registreredes ret til at blive underrettet, hvor det var nødvendigt for at beskytte, bl.a., andres rettigheder og frihedsrettigheder og til at forebygge og efterforske kriminalitet eller brud på etiske regler for lovregulerede erhverv. IPI er et fagligt organ bestående af ejendomsmæglere i Belgien, der har til opgave at tilse, at ejendomsmæglerfaget udøves tilfredsstillende. Det bad en national domstol om at erklære, at de anklagede havde overtrådt faglige regler, og give dem påbud om at indstille diverse ejendomsmægleraktiviteter. Søgsmålet var baseret på faktiske oplysninger indhentet af privatdetektiver, som IPI havde gjort brug af.

De nationale domstole var i tvivl om værdien af detektivernes oplysninger, da der var en mulighed for, at de var indhentet uden at at overholde databeskyttelseskravet i belgisk lovgivning, navnlig forpligtelsen om at underrette registrerede om behandlingen af deres personoplysninger, inden disse oplysninger indsamles. EU-Domstolen bemærkede, at artikel 13, stk. 1, fastslog, at medlemsstater »kan« men er ikke forpligtet til at fastlægge undtagelser i deres nationale lovgivning fra forpligtelsen om at underrette registrerede om behandlingen af deres oplysninger. Da artikel 13, stk. 1, angiver forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger eller brud på etiske regler som værende grundlag, hvormed medlemsstater kan begrænse enkeltpersoners rettigheder, kan aktiviteterne for et organ som IPI og privatdetektiverne, som handler på dennes vegne, påberåbe sig denne bestemmelse. Hvis en medlemsstat ikke har fastlagt en sådan undtagelse, skal de registrerede dog underrettes.

([530]) EU-Domstolen, C-473/12, *Institut professionnel des agents immobiliers (IPI) mod Geoffrey Englebert m.fl.*, 7. november 2013.

Eksempel: I sagen *Smaranda Bara m.fl. mod Casa Națională de Asigurări de Sănătate m.fl.* ([531]) præciserede EU-Domstolen, hvorvidt EU-retten forhindrer en national offentlig myndighed i at overføre personoplysninger til en anden offentlig myndighed til efterfølgende behandling, uden at registrerede underrettes om denne overførsel og behandling. I dette tilfælde havde skattestyrelsen ikke oplyst sagsøgerne om overførslen af deres oplysninger til det nationale sygeforsikringsinstitut, inden denne fandt sted.

EU-Domstolen vurderede, at kravet i EU-retten om at underrette registrerede om behandlingen af deres personoplysninger er »så meget desto vigtigere, som det er en nødvendig betingelse for, at de pågældende personer kan udøve deres ret til indsigt i og til at foretage berigtigelse af de behandlede oplysninger [...] deres ret til indsigelse mod behandlingen af disse oplysninger«. Princippet om rimelig behandling kræver, at registrerede underrettes om overførslen af deres oplysninger til et andet offentligt organ med henblik på efterfølgende behandling. I medfør af artikel 13, stk. 1, i direktiv 95/46/EF kan medlemsstater begrænse retten til at blive underrettet, hvis det vurderes nødvendigt til at beskytte en af statens vigtige økonomiske interesser, herunder skatteanliggender. Sådanne begrænsninger skal dog træffes ved lovmæssige foranstaltninger. Da hverken definitionen af oplysningerne, som overføres, eller retningslinjerne for videregivelsen var fastlagt i en lovmæssig foranstaltning, men i stedet udelukkende stammede fra en protokol mellem de to offentlige myndigheder, var afvigelsesbetingelserne i EU-retten ikke opfyldt. Sagsøgerne burde være blevet underrettet på forhånd om overførslen af deres oplysninger til det nationale sygeforsikringsinstitut og instituttets efterfølgende behandling af disse oplysninger.

Indhold af informationerne

Under artikel 8, stk. 1, i den moderniserede konvention 108 er den dataansvarlige forpligtet til at give den registrerede de informationer, som sikrer en rimelig og gennemsigtig behandling af personoplysninger, herunder:

- den dataansvarliges identitet og sædvanlige opholdssted eller forretningssted
- lovgrundlag bag og formålene med den planlagte behandling
- kategorierne af behandlede oplysninger

([531]) EU-Domstolen, C-201/14, *Smaranda Bara m.fl. mod Casa Națională de Asigurări de Sănătate m.fl.*, 1. oktober 2015.

- eventuelle modtagere eller kategorier af modtagere af personoplysningerne
- måder, hvorpå registrerede kan udøve deres rettigheder.

Under GDPR er den dataansvarlige ved indsamling af personoplysninger fra den registrerede forpligtet til at give den registrerede følgende oplysninger på tidspunktet, hvor personoplysningerne indhentes ([532]):

- identitet på og kontaktoplysninger for den dataansvarlige, inklusive eventuelle detaljer om DPO'en
- behandlingens formål og retsgrundlag, f.eks. en kontrakt eller retlig forpligtelse
- de legitime interesser, som forfølges af den dataansvarlige, hvis de udgør behandlingens grundlag
- eventuelle modtagere eller kategorier af modtagere af personoplysningerne
- om personoplysninger overføres til et tredjeland eller en international organisation, og om det er baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller passende garantier
- det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum
- den registreredes rettigheder i forbindelse med behandlingen, såsom indsigt i, berigtigelse eller sletning af personoplysninger eller begrænsning af eller indsigelse mod behandling
- om meddelelse af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt, samt om den registrerede har pligt til at give personoplysningerne og de eventuelle konsekvenser af ikke at give sådanne oplysninger
- forekomsten af automatiske afgørelser, herunder profilering
- retten til at indgive en klage til en tilsynsmyndighed
- tilstedeværelsen af retten til at trække samtykke tilbage.

([532]) Generel forordning om databeskyttelse, artikel 13, stk. 1.

I tilfælde med automatiske afgørelser, herunder profilering, skal registrerede modtage meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede.

I tilfælde, hvor personoplysninger ikke indhentes direkte fra den registrerede, skal den dataansvarlige underrette den registrerede om personoplysningernes oprindelse. Under alle omstændigheder skal den dataansvarlige blandt andet underrette registrerede om tilstedeværelsen af automatiske afgørelser, herunder profilering ([533]). Endelig, hvis en dataansvarlig planlægger at behandle personoplysninger til et andet formål end det, som oprindeligt var givet til den registrerede, kræver principperne om formålsbegrænsning og gennemsigtighed, at den dataansvarlige underretter den registrerede om dette nye formål. Dataansvarlige skal meddele information inden nogen yderligere behandling. Med andre ord skal den dataansvarlige i tilfælde, hvor den registrerede gav samtykke til behandlingen af dennes personoplysninger, indhente fornyet samtykke fra den registrerede, hvis databehandlingens formål ændres, eller hvis flere formål tilføjes.

Tidspunkt for meddelelse

GDPR sondrer mellem to scenarier og to tidspunkter, hvor den dataansvarlige skal informere den registrerede.

- Når personoplysningerne indhentes direkte fra den registrerede, skal den dataansvarlige meddele den registrerede om alle relevante oplysninger og rettigheder i medfør af GDPR ved tidspunktet, hvor oplysningerne indsamles ([534]). Hvis den dataansvarlige planlægger at viderebehandle personoplysningerne til et andet formål, skal denne meddele alle relevante informationer, inden behandlingen finder sted.

- Når personoplysningerne ikke er indhentet direkte fra den registrerede, er den dataansvarlige forpligtet til at oplyse den registrerede om behandlingen »inden for en rimelig frist efter indsamlingen af personoplysningerne, men senest inden for en måned«, eller inden oplysninger videregives til en tredjemand ([535]).

([533]) Generel forordning om databeskyttelse, artikel 13, stk. 2, og artikel 14, stk. 2, litra f).

([534]) *Ibid.*, artikel 13, stk. 1 og 2, indledningen, hvor GDPR henviser til, at oplysningspligten gælder »på det tidspunkt, hvor personoplysningerne indsamles«.

([535]) *Ibid.*, artikel 13, stk. 3, og artikel 14, stk. 3. Se også henvisningen til rimelige intervaller og fraværet af unødig forsinkelse i den moderniserede konvention 108, artikel 8, stk. 1, litra b).

Den forklarende rapport til den moderniserede konvention 108 fastlægger, at hvis underretning af registrerede ikke er muligt ved behandlingens påbegyndelse, kan det udføres på et senere tidspunkt, såsom når den dataansvarlige kommer i kontakt med den registrerede, uanset grunden ([536]).

Forskellige metoder til underretning

Under både Europarådets retsorden og EU-retten skal de informationer, som den dataansvarlige giver den registrerede, være kortfattede, gennemsigtige, letforståelige og lettilgængelige. De skal være i et skriftligt eller andet format, herunder elektroniske, og benytte et klart, enkelt og letforståeligt sprog. I forbindelse med underretningen kan den dataansvarlige benytte standardikoner til at formidle informationen på en synlig og letforståelig måde ([537]). For eksempel kan et ikon, der repræsenterer en lås, signalere, at oplysningerne indsamles på sikker vis og/eller krypteres. Registrerede kan anmode om, at informationen meddeles mundtligt. Informationer skal være gratis, medmindre den registreredes anmodninger er åbenbart grundløse eller overdrevne (dvs. de gentages) ([538]). Let adgang til de meddelte informationer er afgørende for, at den registrerede kan udøve sine rettigheder i henhold til europæisk databeskyttelseslovgivning.

Princippet om rimelig behandling kræver, at oplysninger er lette at forstå for registrerede. Der skal benyttes et sprog, som er hensigtsmæssigt for modtagerne. Sprogets kompleksitet og udformning skal være tilpasset til den påtænkte målgruppe. Der er for eksempel stor forskel, hvis det er rettet mod en voksen eller et barn, den brede offentlighed eller en akademisk ekspert. Spørgsmålet om at balancere dette aspekt af informationens forståelighed undersøges i Artikel 29-Gruppens udtalelse om mere harmoniserede bestemmelser om oplysningspligt. Dette fremmer ideen om såkaldte flerlagsmeddelelser ([539]), der giver den registrerede mulighed for at beslutte, hvilket detaljeniveau denne foretrækker. Denne måde at præsentere informationer på fritager dog ikke den dataansvarlige fra sine forpligtelser

([536]) Forklarende rapport til den moderniserede konvention 108, stk. 70.

([537]) Europa-Kommissionen vil videreudvikle brugen af ikoner til at formidle oplysninger og procedurer for tilvejebringelse af standardiserede koner via delegerede retsakter. Se generel forordning om databeskyttelse, artikel 12, stk. 8.

([538]) Generel forordning om databeskyttelse, artikel 12, stk. 1, 5 og 7, og den moderniserede konvention 108, artikel 9, stk. 1, litra b).

([539]) Artikel 29-Gruppen (2004), *Udtalelse 10/2004 om mere harmoniserede bestemmelser om oplysningspligt*, WP 100, Bruxelles, 25. november 2004.

i medfør af GDPR's artikel 13 og 14. Den dataansvarlige skal stadig meddele alle informationer til den registrerede.

Én af de mest effektive måder at underrette på er at anbringe passende bestemmelser om oplysning på den dataansvarliges hjemmeside, såsom en privatlivspolitik for webstedet. Der er dog en væsentlig del af befolkningen, som ikke bruger internettet, og en virksomheds eller offentlig myndigheds informationspolitik skal tage hensyn hertil.

En meddelelse om beskyttelse af privatlivets fred i forbindelse med behandling af personoplysninger på et websted kan se ud som følger:

Hvem er vi?

Den dataansvarlige for databehandlingen er Bed and Breakfast C&U, beliggende ved [adresse: xxx], tlf. xxx, fax xxx, e-mail: info@c&u.com. Databeskyttelsesrådgiverens kontaktoplysninger: [xxx].

Informationsmeddelelse omkring personoplysninger udgør en del af de vilkår og betingelser, som vores hoteltjeneste overholder.

Hvilke oplysninger indsamler vi fra dig?

Vi indsamler følgende personoplysninger fra dig: navn, postadresse, telefonnummer, e-mail-adresse, information om opholdet, kredit- og debitkortnummer og IP-adresser eller domænenavne for de computere, som du har brugt til at forbinde til vores hjemmeside.

Hvorfor indsamler vi dine oplysninger?

Vi behandler dine oplysninger på baggrund af dit samtykke og med henblik på at udføre reservationer, indgå og opfylde kontrakter vedrørende de tjenester, vi tilbyder dig, og for at overholde lovkrav, for eksempel loven om lokale gebyrer, der kræver, at vi indsamler personoplysninger for at betale byafgiften for ferieophold.

Hvordan behandler vi dine oplysninger?

Dine personoplysninger opbevares i en periode på tre måneder. Dine oplysninger udsættes ikke for en procedure med automatiske afgørelser.

Vores Bed and Breakfast C&U overholder strenge procedurer for at sikre, at dine personoplysninger ikke beskadiges, ødelægges eller videregives til en tredjemand uden din tilladelse, og for at forhindre uautoriseret adgang. De computere, der lagrer oplysningerne, er opbevaret i et sikkert miljø med begrænset fysisk adgang. Vi benytter sikre firewalls og andre foranstaltninger til at begrænse elektronisk adgang. Hvis oplysningerne skal overføres til tredjemand, kræver vi, at denne har fastlagt tilsvarende foranstaltninger til at beskytte dine personoplysninger.

Alle de oplysninger, som vi indsamler eller registrerer, er begrænset til vores kontorer. Kun personer, som behøver oplysninger til at opfylde deres forpligtelser under denne kontrakt, tildeles adgang til personoplysninger. Vi spørger dig udtrykkeligt, når vi behøver oplysninger til at identificere dig. Vi kan have brug for, at du samarbejder med vores sikkerhedskontroller, inden vi videregiver information til dig. Du kan ajourføre de personoplysninger, som du giver til os, på ethvert tidspunkt ved at kontakte os direkte.

Hvilke rettigheder har du?

Du har ret til at få adgang til dine oplysninger, få en kopi af dine oplysninger, anmode om deres sletning eller berigtigelse eller anmode om, at dine oplysninger overføres til en anden dataansvarlig.

Du kan sende dine anmodninger til os via info@c&u.com. Vi skal svare på din anmodning inden for en måned, men hvis din anmodning er for kompleks, eller vi modtager for mange andre anmodninger, oplyser vi dig om, at denne periode kan forlænges med yderligere to måneder.

Adgang til dine personoplysninger

Du har ret til at få adgang til dine oplysninger og anmode om at få baggrunden for behandlingen af dem at vide, anmode om deres sletning eller berigtigelse og ret til ikke at være underlagt afgørelse, som alene er baseret på automatisk behandling, uden at der tages hensyn til dine holdninger. Du

kan sende dine anmodninger til os via info@c&u.com. Du har også ret til at gøre indsigelse mod behandlingen, trække dit samtykke tilbage og indgive en klage ved den nationale tilsynsmyndighed, hvis du mener, at denne databehandling er i strid med loven, og kræve erstatning for skader pådraget som følge af den ulovlige behandling.

Retten til at indgive en klage

GDPR kræver, at den dataansvarlige underretter registrerede om håndhævelsesmekanismer under national og EU-ret i tilfælde af brud på persondatasikkerheden. Den dataansvarlige skal oplyse registrerede om deres ret til at indgive en klage om et brud på persondatasikkerheden til en tilsynsmyndighed og, om nødvendigt, til en national domstol ([540]). Europarådets retsorden fastlægger også registreredes ret til at blive underrettet omkring midler til at udøve deres rettigheder, herunder retten til retsmidler fastlagt i artikel 9, stk. 1, litra f).

Undtagelser fra retten til at blive underrettet

GDPR fastsætter undtagelser fra forpligtelsen om underretning. I medfør af artikel 13, stk. 4, og artikel 14, stk. 5, i GDPR gælder forpligtelsen om at underrette registrerede ikke, hvis den registrerede allerede besidder de relevante informationer ([541]). Derudover, når personoplysningerne ikke er indhentet fra den registrerede, vil forpligtelsen om underretning ikke finde anvendelse, hvis leveringen af oplysninger er umulig eller uforholdsmæssig, navnlig når personoplysningerne behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål ([542]).

Desuden giver GDPR medlemsstater skønsbeføjelser til at begrænse forpligtelser og rettigheder givet til fysiske personer under forordningen, hvis dette er en nødvendig og proportionel foranstaltning i et demokratisk samfund, for eksempel til at sikre den nationale og offentlige sikkerhed, forsvaret, beskytte retslige efterforskninger og procedurer eller beskytte økonomiske og finansielle interesser samt private interesser, som er mere presserende end interesser i beskyttelse af oplysninger ([543]).

([540]) Generel forordning om databeskyttelse, artikel 13, stk. 2, litra d), og artikel 14, stk. 2, litra e), og den moderniserede konvention 108, artikel 8, stk. 1, litra f).

([541]) *Ibid.*, artikel 13, stk. 4, og artikel 14, stk. 5, litra a).

([542]) *Ibid.*, artikel 14, stk. 5, litra b)-e).

([543]) Generel forordning om databeskyttelse, artikel 23, stk. 1.

Alle undtagelser eller begrænsninger skal være nødvendige i et demokratisk samfund og forholdsmæssige med det forfulgte mål. I meget usædvanlige tilfælde, for eksempel grundet medicinske indikationer, kan selve den registreredes beskyttelse kræve en begrænsning af gennemsigtighed. Dette gælder ligeledes for begrænsning af registreredes indsigtsret ([544]). Som et minimumsniveau af beskyttelse skal national lovgivning dog respektere det væsentligste indhold i de grundlæggende rettigheder og frihedsrettigheder, som er beskyttet i EU-retten ([545]). Dette kræver, at den nationale lovgivning indeholder bestemte bestemmelser, som præciserer formålet med behandlingen, de omhandlede kategorier af personoplysninger, garantier og andre proceduremæssige krav ([546]).

Når oplysninger indsamles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål kan EU-retten eller medlemsstaters lovgivning fastlægge undtagelser fra forpligtelsen om underretning, hvis det ellers bliver umuligt eller meget svært at opnå de bestemte formål ([547]).

Lignende begrænsninger findes i Europarådets retsorden, hvor rettigheder tildelt til registrerede i henhold til artikel 9 i den moderniserede konvention 108 kan være underlagt eventuelle begrænsninger i artikel 11 i den moderniserede konvention 108 under strenge betingelser. Endvidere gælder forpligtelsen om gennemsigtighed for behandling i henhold til artikel 8, stk. 2, i den moderniserede konvention 108 ikke, når den registrerede allerede besidder informationen.

Ret til indsigt i egne oplysninger

Under Europarådets retsorden anerkendes retten til indsigt i egne oplysninger udtrykkeligt i artikel 9 i den moderniserede konvention 108. Denne fastlægger, at alle fysiske personer, efter anmodning, har ret til at få informationer om behandlingen af personoplysninger vedrørende vedkommende, og at de skal kommunikeres på en letforståelig måde. Indsigtsretten er ikke kun anerkendt i bestemmelserne i den moderniserede konvention 108, men også i EMD's retspraksis. EMD har gentagne gange fastholdt, at fysiske personer har indsigtsret i informationer om deres personoplysninger, og at denne ret stammer fra behovet

([544]) Generel forordning om databeskyttelse, artikel 15.

([545]) Generel forordning om databeskyttelse, artikel 23, stk. 1.

([546]) *Ibid*., artikel 23, stk. 2.

([547]) *Ibid*., artikel 89, stk. 2 og 3.

for at respektere privatlivets fred ([548]). Retten til indsigt i personoplysninger, der lagres af offentlige eller private organisationer, kan under visse omstændigheder være begrænset ([549]).

Under EU-retten er indsigtsretten i egne oplysninger udtrykkeligt anerkendt i artikel 15 i GDPR, og det er også fastlagt som et element i den grundlæggende ret til beskyttelse af personoplysninger i artikel 8, stk. 2, i Den Europæiske Unions charter om grundlæggende rettigheder ([550]). En fysisk persons indsigtsret i sine egne personoplysninger er et grundlæggende element i europæisk databeskyttelseslovgivning ([551]).

GDPR fastlægger, at alle registrerede har indsigtsret i deres egne personoplysninger og visse oplysninger om behandlingen, som dataansvarlige skal forsyne ([552]). Navnlig har alle registrerede ret til at indhente bekræftelse (fra den dataansvarlige), om hvorvidt oplysninger vedrørende vedkommende behandles, og, som minimum, information om følgende:

- behandlingens formål
- omhandlede kategorier af personoplysninger
- modtagere eller kategorier af modtagere, som oplysningerne videregives til
- det tidsrum, hvori personoplysningerne planlægges at være lagret, eller, hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum
- tilstedeværelsen af rettigheder til at berigtige eller slette personoplysninger eller begrænse behandling af personoplysninger
- retten til at indgive klage til en tilsynsmyndighed

([548]) EMD, *Gaskin mod Det Forenede Kongerige*, nr. 10454/83, 7. juli 1989; EMD, *Odièvre mod Frankrig* [GC], nr. 42326/98, 13. februar 2003; EMD, *K.H. m.fl. mod Slovakiet*, nr. 32881/04, 28. april 2009 og EMD, *Godelli mod Italien*, nr. 33783/09, 25. september 2012.

([549]) EMD, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987.

([550]) Se også EU-Domstolen, forenede sager C-141/12 og C-372/12, *YS mod Minister voor Immigratie, Integratie en Asiel* og *Minister voor Immigratie, Integratie en Asiel mod M og S*, 17. juli 2014; EU-Domstolen, C-615/13 P, *ClientEarth og Pesticide Action Network Europe (PAN Europe) mod Den Europæiske Fødevaresikkerhedsautoritet (EFSA) og Europa-Kommissionen*, 16. juli 2015.

([551]) EU-Domstolen, forenede sager C-141/12 og C-372/12, *YS mod Minister voor Immigratie, Integratie en Asiel* og *Minister voor Immigratie, Integratie en Asiel mod M og S*, 17. juli 2014.

([552]) Generel forordning om databeskyttelse, artikel 15, stk. 1.

- alle tilgængelige oplysninger om kilden til oplysninger, der behandles, hvis oplysningerne ikke er indsamlet fra den registrerede

- logikken bag enhver automatiseret databehandling i forbindelse med automatiske afgørelser.

Databehandleren skal forsyne den registrerede med en kopi af de personoplysninger, der behandles. Alle informationer meddelt til den registrerede skal formidles på en letforståelig måde, hvilket betyder, at den dataansvarlige skal sørge for, at den registrerede kan forstå de informationer, som meddeles. For eksempel vil det normalt ikke være tilstrækkeligt at bruge tekniske forkortelser, kryptiske fagudtryk eller forkortelser i et svar på en anmodning om aktindsigt, medmindre betydningen af disse udtryk forklares. Ved udførelse af automatiske afgørelser, herunder profilering, skal den generelle logik, der styrer de automatiske afgørelser, forklares, inklusive de kriterier, som skal overvejes ved evaluering af den registrerede. Lignende krav findes i **Europarådets retsorden** ([553]).

Eksempel: Ved at få adgang til sine personoplysninger kan en registreret bedre afgøre, om oplysningerne er korrekte. Det er derfor vigtigt, at den registrerede på en letforståelig måde ikke kun informeres om de faktiske personoplysninger, som behandles, men også de kategorier, hvorunder disse personoplysninger behandles, såsom navn, IP-adresse, koordinater til geoplacering, kreditkortnummer osv.

Information om oplysningskilden – når oplysningerne ikke indsamles fra den registrerede – skal gives som svar på en anmodning om aktindsigt, hvis denne information er tilgængelig. Denne meddelelse skal tolkes under hensyntagen til principperne om rimelighed, gennemsigtighed og ansvarlighed. En dataansvarlig må ikke ødelægge information om oplysningskilden for at være fritaget fra at meddele denne – medmindre sletningen ville være fundet sted, uanset om anmodningen om aktindsigt var modtaget eller ej – og denne skal stadig overholde de generelle ansvarlighedskrav.

Som fastlagt i EU-Domstolens retspraksis kan retten til adgang til personoplysninger ikke begrænses af tidsgrænser uden grund. Registrerede skal også have en rimelig mulighed for at indhente informationer om databehandlingsaktiviteter, som tidligere fandt sted.

([553]) Se den moderniserede konvention 108, artikel 8, stk. 1, litra c).

Eksempel: I *Rijkeboer* ([554])-sagen blev EU-Domstolen anmodet om at afgøre, om en enkeltpersons ret til indsigt i information om modtagerne eller kategorierne af modtagere af personoplysninger og om indholdet af oplysningerne kan begrænses til et år forud for indgivelsen af vedkommendes anmodning om adgang.

For at afgøre, om en sådan tidsfrist er berettiget i henhold til EU-retten, besluttede EU-Domstolen at fortolke artikel 12 i lyset af direktivets formål. EU-Domstolen tilkendegav først, at retten til indsigt er nødvendig, for at den registrerede kan udøve sine rettigheder til, at dennes oplysninger berigtiges, slettes eller blokeres af den dataansvarlige, eller at den dataansvarlige underretter tredjemand, som disse oplysninger er meddelt til, om sådanne berigtigelser, slettelser eller blokeringer. En effektiv ret til indsigt er også nødvendig for, at den registrerede kan udøve sin ret til at gøre indsigelse mod behandlingen af vedkommendes personoplysninger eller sin ret til at indgive en klage og gøre krav på erstatning ([555]).

For at sikre den praktiske virkning af rettighederne tildelt registrerede, konstaterede EU-Domstolen, »at denne ret nødvendigvis må vedrøre fortiden. Hvis ikke dette var tilfældet, ville den pågældende ikke være i stand til effektivt at udøve sin ret til at sikre, at de oplysninger, som angiveligt er ulovlige eller urigtige, berigtiges, slettes eller blokeres, eller til at anlægge sag og opnå erstatning for den forvoldte skade«.

6.1.2. Ret til berigtigelse

Under EU-retten og **Europarådets retsorden** skal registrerede have ret til at få deres personoplysninger berigtiget. Personoplysningers nøjagtighed er nødvendig til at sikre et højt databeskyttelsesniveau for registrerede ([556]).

([554]) EU-Domstolen, C-553/07, *College van burgemeester en wethouders van Rotterdam mod M. E. E. Rijkeboer*, 7. maj 2009.

([555]) Generel forordning om databeskyttelse, artikel 15, stk. 1, litra c) og f), artikel 16, artikel 17, stk. 2, og artikel 21, samt kapitel VIII.

([556]) *Ibid.*, artikel 16 og betragtning 65 samt den moderniserede konvention 108, artikel 9, stk. 1, litra e).

Eksempel: I sagen *Ciubotaru mod Moldova* ([557]) kunne sagsøgeren ikke ændre registreringen af sin etniske oprindelse i officielle fortegnelser fra moldover til rumæner, fordi han angiveligt ikke kunne underbygge sin anmodning. EMD fandt det acceptabelt, at stater kræver objektivt bevis ved registrering af en enkeltpersons etniske identitet. Når et sådant krav alene var baseret på subjektive forhold, der ikke var underbyggede, kunne myndighederne afvise det. Sagsøgerens krav var dog baseret på mere end hans subjektive opfattelse af vedkommendes egen etnicitet. Han kunne angive forbindelser til den rumænske etniske gruppe, som f.eks. sprog, navn, empati osv., som kunne efterprøves objektivt. I henhold til den nationale lovgivning skulle sagsøgeren dog dokumentere, at hans forældre havde tilhørt den rumænske etniske gruppe. Som følge af Moldovas historie havde et sådant krav skabt en uoverstigelig hindring for at registrere en anden etnisk identitet end den, som de sovjetiske myndigheder havde registreret for hans forældre. Ved at forhindre sagsøgeren i at få undersøgt sit krav i lyset af beviser, der objektivt kunne efterprøves, havde staten ikke overholdt sin positive forpligtelse til at sikre sagsøgeren effektiv respekt for vedkommendes privatliv. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

I nogle tilfælde vil det være tilstrækkeligt, hvis den registrerede bare anmoder om berigtigelse af, for eksempel, stavningen af et navn, en adresse eller et telefonnummer. I medfør af **EU-retten** og **Europarådets retsorden** skal urigtige personoplysninger berigtiges uden unødig eller overdreven forsinkelse ([558]). Hvis sådanne anmodninger dog er knyttet til emner af retlig betydning, såsom den registreredes juridiske identitet eller den korrekte bopæl for leveringen af juridisk dokumentation, er anmodninger om berigtigelse muligvis ikke nok, og den dataansvarlige kan være berettiget til at kræve dokumentation for den påståede unøjagtighed. Sådanne krav må ikke pålægge den registrerede en urimelig bevisbyrde og dermed udelukke registrerede fra at få deres oplysninger berigtiget. EMD har konstateret overtrædelser af artikel 8 i EMRK i flere tilfælde, hvor sagsøgeren ikke havde været i stand til at anfægte nøjagtigheden af oplysninger, som blev opbevaret i hemmelige registre ([559]).

([557]) EMD, *Ciubotaru mod Moldova*, nr. 27138/04, 27. april 2010, præmis 51 og 59.

([558]) Generel forordning om databeskyttelse, artikel 16, og den moderniserede konvention 108, artikel 9, stk. 1.

([559]) EMD, *Rotaru mod Rumænien* [GC], nr. 28341/95, 4. maj 2000.

Eksempel: I sagen *Cemalettin Canli mod Tyrkiet* ([560]) vurderede EMD, at artikel 8 i EMRK var blevet overtrådt i forbindelse med urigtige politirapporter under en straffesag.

Sagsøgeren havde to gange været involveret i en straffesag som følge af påstået medlemskab af illegale organisationer, men var aldrig blevet dømt. Da sagsøgeren igen blev anholdt og sigtet for en anden strafbar handling, forelagde politiet straffedomstolen en rapport med titlen »*information om yderligere lovovertrædelser*«, hvori sagsøgeren optrådte som medlem af to illegale organisationer. Sagsøgerens anmodning om at få udleveret rapporten og politiets fortegnelser blev ikke imødekommet. EMD fastslog, at informationen i politirapporten var inden for rammerne af artikel 8 i EMRK, da offentlige informationer også var omfattet af udtrykket »privatlivet«, når de systematisk blev indsamlet og lagret i sagsakter, som myndighederne var i besiddelse af. Politiets rapport var endvidere urigtig, og dens udarbejdelse og forelæggelse for straffedomstolen var ikke i overensstemmelse med den nationale lovgivning. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Under civile søgsmål eller retssager ved en offentlig myndighed kan den registrerede, for at afgøre om oplysningerne er korrekte eller ej, bede om at få en fortegnelse eller bemærkning anbragt i vedkommendes sagsakt, der angiver, at nøjagtigheden bestrides, og at en officiel afgørelse fremkommer ([561]). Under denne periode må den dataansvarlige ikke fremføre oplysningerne som korrekte eller ikke værende genstand for ændringer, navnlig over for tredjemænd.

6.1.3. Ret til sletning (»ret til at blive glemt«)

Det er særligt vigtigt at give registrerede retten til at få deres egne oplysninger slettet med henblik på den effektive gennemførelse af databeskyttelsesprincipper og, navnlig, princippet om dataminimering (personoplysninger skal begrænses til det, der er nødvendigt til de formål, som oplysningerne behandles til). En ret til sletning findes derfor i både Europarådets og EU's retslige instrumenter ([562]).

([560]) EMD, *Cemalettin Canli mod Tyrkiet*, nr. 22427/04, 18. november 2008, præmis 33 og 42-43 og EMD, *Dalea mod Frankrig*, nr. 964/07, 2. februar 2010.

([561]) Generel forordning om databeskyttelse, artikel 18 og betragtning 67.

([562]) *Ibid.*, artikel 17.

Eksempel: I sagen *Segerstedt-Wiberg m.fl. mod Sverige* ([563]) var sagsøgerne tilknyttet visse liberale og kommunistiske politiske partier. De havde mistanke om, at oplysninger om dem var indført i sikkerhedspolitiets registre og anmodede om, at de blev slettet. EMD var tilfredse med, at lagringen af de omstridte oplysninger havde et retsligt grundlag og legitimt formål. EMD konstaterede dog i forbindelse med nogle sagsøgere, at den fortsatte lagring af oplysningerne var et uforholdsmæssigt indgreb i deres privatliv. Myndighederne opbevarede, for eksempel, oplysninger om, at en sagsøger i 1969 angiveligt havde opfordret til voldelig modstand mod politikontrol under demonstrationer. EMD konstaterede, at disse oplysninger ikke havde nogen relevant national sikkerhedsmæssig interesse, navnlig grundet deres historiske natur. Domstolen konstaterede, at artikel 8 i EMRK var blevet overtrådt vedrørende fire af de fem sagsøgere, da den fortsatte lagring af deres oplysninger ikke var relevant grundet det lange tidsforløb siden sagsøgernes påståede handlinger.

Eksempel: I sagen *Brunet mod Frankrig* ([564]) gjorde sagsøgerne indsigelse mod lagringen af deres personoplysninger i en politidatabase, som indeholdt oplysninger om dømte personer, anklagede personer og ofre. Selvom straffesagen mod sagsøgeren var afsluttet, optrådte hans oplysninger i databasen. EMD fastholdt, at EMRK's artikel 8 var blevet overtrådt. I sin konklusion overvejede Domstolen, at der i praksis ikke var nogen mulighed for, at sagsøgeren kunne få sine personoplysninger slettet fra databasen. EMD overvejede også arten af oplysningerne inkluderet i databasen og vurderede, at det krænkede sagsøgerens privatliv, da de indeholdt detaljer om vedkommendes identitet og personlighed. Desuden konstaterede domstolen, at opbevaringsperioden i databasen på 20 år var unødigt lang, navnlig da ingen domstol nogensinde havde dømt sagsøgeren.

Den moderniserede konvention 108 anerkender udtrykkeligt, at alle fysiske personer har en ret til sletning af unøjagtige, urigtige eller ulovligt behandlede oplysninger ([565]).

([563]) EMD, *Segerstedt-Wiberg m.fl. mod Sverige*, nr. 62332/00, 6. juni 2006, præmis 89 og 90. Se, for eksempel, også EMD, *M.K. mod Frankrig*, nr. 19522/09, 18. april 2013.

([564]) EMD, *Brunet mod Frankrig*, nr. 21010/10, 18. september 2014.

([565]) Den moderniserede konvention 108, artikel 9, stk. 1, litra e).

Under EU-retten giver artikel 17 i GDPR registrerede ret til at anmode om at få oplysninger fjernet eller slettet. Retten til at få sine personoplysninger slettet uden unødig forsinkelse er gældende, når:

- personoplysningerne ikke længere er nødvendige til de formål, hvortil de blev indsamlet eller på anden vis behandlet
- den registrerede trækker sit samtykke tilbage, som behandlingen var baseret på, og der ikke er noget retsgrundlag for behandlingen
- den registrerede gør indsigelse mod behandlingen, og der ikke er noget retsgrundlag for behandlingen
- personoplysningerne er blevet behandlet ulovligt
- personoplysningerne skal slettes for at overholde en retlig forpligtelse i EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt
- personoplysningerne er indsamlet i forbindelse med udbud af informationssamfundstjenester til børn i medfør af artikel 8 i GDPR ([566]).

Bevisbyrden for, at databehandlingen er legitim, hviler hos de dataansvarlige, da de er ansvarlige for behandlingens lovlighed ([567]). I medfør af princippet om ansvarlighed skal den dataansvarlige på ethvert tidspunkt være i stand til at påvise, at der er et forsvarligt retsgrundlag bag dennes databehandling; ellers skal behandlingen indstilles ([568]). GDPR definerer undtagelser fra retten til at blive glemt, herunder når behandling af personoplysninger er nødvendig for:

- at udøve retten til ytrings- og informationsfrihed
- at overholde en retlig forpligtelse, der kræver behandling i henhold til EU-retten eller medlemsstaternes nationale ret, og som den dataansvarlige er underlagt, eller for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt
- hensyn til samfundsinteresser på folkesundhedsområdet

([566]) Generel forordning om databeskyttelse, artikel 17, stk. 1.

([567]) *Ibid.*

([568]) *Ibid.*, artikel 5, stk. 2.

- arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål

- at retskrav kan fastlægges, gøres gældende eller forsvares ([569]).

EU-Domstolen har bekræftet vigtigheden af retten til sletning for at sikre et højt niveau af databeskyttelse.

Eksempel: I sagen *Google Spain* ([570]) undersøgte EU-Domstolen, om Google var forpligtet til at slette forældede oplysninger om sagsøgerens finansielle vanskeligheder fra sin liste over søgeresultater. Google anfægtede, bl.a., at de ikke var ansvarlige, da de kun tilvejebringer et hyperlink til webside-udgiverens webside, hvor oplysningerne befinder sig, som i dette tilfælde var en avis, der rapporterede om sagsøgerens konkursproblemer ([571]). Google argumenterede, at anmodningen om at slette forældede oplysninger fra et websted skal sendes til værten for websiden og ikke Google, der kun giver et link til den oprindelige side. EU-Domstolen konkluderede, at Google, når denne søger efter oplysninger og websider på internettet, og når den indekserer indhold til at levere søgeresultater, bliver en dataansvarlig, hvortil ansvarsområder og forpligtelser i medfør af EU-retten er gældende.

EU-Domstolen præciserede, at søgemaskiner på internettet og søgeresultater, der indeholder personoplysninger, kan tegne en detaljeret profil af en fysisk person ([572]). Søgemaskiner gør oplysningerne i en sådan liste over søgeresultater allestedsnærværende. På baggrund af dets potentielle alvor kan indgrebet ikke alene begrundes af den økonomiske interesse, som søgemaskineudbyderen har i behandlingen. Der skal være en rimelig balance navnlig imellem internetbrugeres legitime interesse i at få adgang til oplysninger og den registreredes grundlæggende rettigheder under artikel 7

([569]) *Ibid.*, artikel 17, stk. 3.

([570]) EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014, præmis 55-58.

([571]) Google anfægtede også anvendelsen af europæiske databeskyttelsesregler grundet det faktum, at Google Inc. er etableret i USA, og behandlingen af de pågældende oplysninger i sagen også blev udført i USA. Et andet argument for uanvendeligheden af europæisk databeskyttelseslovgivning påstod, at søgemaskiner ikke kan betragtes som »dataansvarlige« for oplysningerne vist i deres resultater, da de ikke ved noget om oplysningerne eller udøver nogen kontrol over dem. EU-Domstolen afviste begge argumenter og fastholdt, at direktiv 95/46/EF var gældende i det pågældende tilfælde og fortsatte med at undersøge omfanget af de garanterede rettigheder, navnlig retten til sletning af personoplysningerne.

([572]) *Ibid.*, præmis 36, 38, 80-81 og 97.

og 8 i Den Europæiske Unions charter om grundlæggende rettigheder. Grundet den stigende digitalisering af samfundet er kravet om, at personoplysninger skal være nøjagtige og begrænses til det nødvendige, dvs. offentlig oplysning, grundlæggende for at sikre, at enkeltpersoner får et højt databeskyttelsesniveau. Så »skal søgemaskineudbyderen i sin egenskab af registeransvarlig inden for rammerne af sit ansvar, sine kompetencer og sine muligheder således sikre, at behandlingen opfylder kravene« i EU-retten for at sikre fastlagte retsgarantiers fulde virkning ([573]). Dette betyder, at retten til få sine personoplysninger slettet, når behandlingen er forældet eller unødvendig, også omfatter dataansvarlige, som reproducerer oplysningerne ([574]).

Ved undersøgelsen af, om Google skulle fjerne links vedrørende sagsøgeren, fastholdt EU-Domstolen, at fysiske personer under visse omstændigheder har ret til at anmode om at få slettet deres personoplysninger. Man kan påberåbe sig denne ret, når oplysninger om en fysisk person er ukorrekte, utilstrækkelige, irrelevante eller omfatter mere end, hvad der er nødvendigt i forhold til formålene med databehandlingen. EU-Domstolen anerkendte, at denne ret ikke er absolut. Den skal afvejes mod andre rettigheder og interesser, navnlig den brede offentligheds interesse i at have adgang til visse oplysninger. Hver sletningsanmodning skal vurderes individuelt for at afveje de grundlæggende rettigheder til beskyttelse af personoplysninger og den registreredes privatliv med alle internetbrugeres, inklusive webside-udgiveres, legitime interesser. EU-Domstolen vejledte omkring de faktorer, der skal tages i betragtning under denne afvejning. Arten af de pågældende oplysninger er en særlig vigtig faktor. Hvis oplysningerne omhandler den berørte persons privatliv, og offentligheden ikke har nogen interesse i at råde over disse oplysninger, vil databeskyttelse og privatliv veje tungere end den brede offentligheds ret til at få adgang til oplysningerne. Hvis det på den anden side virker som om, at den registrerede er en fremtrædende person, eller at oplysningernes art begrunder, at den brede offentlighed gives adgang til dem, så kan offentlighedens vægtige interesse i at have adgang til oplysningerne begrunde indgrebet i den registreredes grundlæggende ret til databeskyttelse og privatliv.

([573]) *Ibid.*, præmis 81-83.

([574]) EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014, præmis 88. Se også Artikel 29-Gruppen (2014), *Guidelines on the implementation of the CJEU judgment on »Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González« C-131/12*, WP 225, Bruxelles, 26. november 2014, og Recommendation CM/Rec 2012(3) of the Committee of Ministers to member states on the protection of human rights with regard to search engines, 4. april 2012.

Efter dommen vedtog Artikel 29-Gruppen retningslinjer om gennemførelse af EU-Domstolens afgørelse ([575]). Retningslinjerne indeholder en liste over fælles kriterier, som tilsynsmyndighederne kan benytte ved håndtering af klager vedrørende fysiske personers sletningsanmodninger, og som forklarer hvad retten til sletning indebærer og kan vejlede dem under denne afvejning af rettigheder. Retningslinjerne gentager, at vurderinger skal udføres på et individuelt grundlag. Da retten til at blive glemt ikke er absolut, kan resultatet af en anmodning afvige alt efter den pågældende sag. Dette er også illustreret i EU-Domstolens retspraksis efter Google.

Eksempel: I sagen *Camera di Commercio di Lecce mod Manni* ([576]) skulle EU-Domstolen undersøge, om en enkeltperson havde ret til at opnå sletningen af sine personoplysninger offentliggjort i et offentligt selskabsregister, da vedkommendes selskab ophørte med at eksistere. Salvatore Manni havde anmodet Camera di Commercio di Lecce om at slette hans personoplysninger fra det pågældende register, efter at han opdagede, at potentielle kunder kiggede i registret og så, at han tidligere havde administreret en virksomhed, som blev erklæret konkurs for mere end ti år siden. Sagsøgeren mente, at disse oplysninger ville skræmme potentielle kunder væk.

Under afvejningen af Salvatore Mannis ret til beskyttelse af sine personoplysninger mod den brede offentligheds interesse i at få adgang til oplysningerne undersøgte EU-Domstolen først formålet med det offentlige register. Den pegede på det faktum, at offentliggørelse var fastlagt i lovgivningen, og navnlig et EU-direktiv, som var rettet mod at gøre selskabsoplysninger mere lettilgængelige for tredjemænd. Tredjemænd skal dermed have adgang til og kunne undersøge et selskabs grundlæggende dokumenter og andre oplysninger vedrørende selskabet, »navnlig om identiteten af de personer, som har ret til at forpligte selskabet«. Offentliggørelsens formål var også at garantere retssikkerhed på baggrund af større handel mellem medlemsstater ved at sikre, at tredjemænd har adgang til alle relevante oplysninger om selskaber i hele EU.

([575]) Artikel 29-Gruppen (2014), *Guidelines on the implementation of the CJEU judgment on »Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González« C-131/12*, WP 225, Bruxelles, 26. november 2014.

([576]) EU-Domstolen, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 9. marts 2017.

EU-Domstolen bemærkede yderligere, at rettigheder og retslige forpligtelser vedrørende selskabet ofte fortsætter med at eksistere, selv efter et længere tidsforløb og selskabets opløsning. Tvister vedrørende opløsninger kan være lange, og der kan opstå spørgsmål vedrørende et selskab, dets forvaltere og likvidatorer i mange år efter, at et selskab er ophørt med at eksistere. EU-Domstolen fastholdt, at henset til den flerhed af mulige scenarier og forskelle vedrørende forældelsesfrister, der er fastsat i de forskellige medlemsstater, »synes det imidlertid på nuværende tidspunkt umuligt at identificere én enkelt frist, fra opløsningen af et selskab, ved hvis udløb indførslen af de nævnte oplysninger i registret og disses offentliggørelse ikke længere er nødvendig«. Grundet det legitime mål med offentliggørelsen og vanskelighederne med at etablere en tidsperiode, hvorefter personoplysningerne kan slettes fra registret uden at skade tredjemænds interesser, konstaterede EU-Domstolen, at europæiske databeskyttelsesregler ikke garanterer en ret til sletning af personoplysninger for personer i Salvatore Mannis situation.

Når den dataansvarlige har offentliggjort personoplysninger og skal slette oplysningerne, er den dataansvarlige forpligtet og skal tage »rimelige« skridt til at informere andre dataansvarlige, som behandler de samme oplysninger, om den registreredes anmodning om sletning. Den dataansvarliges aktiviteter skal tage hensyn til tilgængelige teknologier og omkostningen til gennemførelse ([577]).

6.1.4. Ret til begrænsning af behandling

Artikel 18 i GDPR tillægger registrerede beføjelser til midlertidigt at begrænse en dataansvarlig i at behandle deres personoplysninger. Registrerede kan anmode den dataansvarlige om at begrænse behandlingen, når:

- rigtigheden af personoplysningerne bestrides af den registrerede
- behandlingen er ulovlig, og den registrerede modsætter sig sletning af personoplysningerne og i stedet anmoder om, at anvendelse heraf begrænses
- oplysningerne skal opbevares, for at retskrav kan gøres gældende eller forsvares

([577]) Generel forordning om databeskyttelse, artikel 17, stk. 2, og betragtning 66.

- man afventer beslutning, om den dataansvarliges legitime interesser går forud for den registreredes interesser ([578]).

Metoderne, hvormed en dataansvarlig kan begrænse behandling af personoplysninger, kan, for eksempel, omfatte midlertidig flytning af de udvalgte oplysninger til et andet behandlingssystem, som gør oplysningerne utilgængelige for brugere, eller midlertidig fjernelse af personoplysninger ([579]). Den dataansvarlige skal underrette den registrerede, inden begrænsningen af behandlingen ophæves ([580]).

Forpligtelse om underretning vedrørende berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

Den dataansvarlige skal meddele enhver berigtigelse eller sletning af personoplysninger eller enhver begrænsning af behandling til alle modtagere, som den dataansvarlige videregav personoplysningerne til, hvis dette er muligt og forholdsmæssigt ([581]). Hvis den registrerede anmoder om oplysninger om disse modtagere, skal den dataansvarlige give vedkommende de oplysninger ([582]).

6.1.5. Ret til dataportabilitet

I medfør af GDPR har registrerede ret til dataportabilitet i situationer, hvor de personoplysninger, de har videregivet til en dataansvarlig, behandles automatisk på baggrund af samtykke, eller når behandlingen af personoplysninger er nødvendig til at gennemføre en kontrakt og udføres ved automatisk databehandling. Dette betyder, at retten til dataportabilitet ikke er gældende i situationer, hvor behandlingen af personoplysninger er baseret på et retsgrundlag, som ikke er samtykke eller en kontrakt ([583]).

Hvis retten til dataportabilitet finder anvendelse, er registrerede berettiget til at få deres oplysninger overført direkte fra én dataansvarlig til en anden, hvis dette er teknisk muligt ([584]). For at fremme dette bør den dataansvarlige udvikle indbyrdes

([578]) *Ibid.*, artikel 18, stk. 1.
([579]) *Ibid.*, betragtning 67.
([580]) *Ibid.*, artikel 18, stk. 3.
([581]) *Ibid.*, artikel 19.
([582]) *Ibid.*
([583]) *Ibid.*, betragtning 68 og artikel 20, stk. 1.
([584]) *Ibid.*, artikel 20, stk. 2.

kompatible formater, der muliggør dataportabilitet for registrerede ([585]). GDPR angiver, at disse formater skal være strukturerede, almindeligt anvendte og maskinlæsbare for at fremme indbyrdes kompatibilitet ([586]). Indbyrdes kompatibilitet kan bredt defineres som informationssystemers evne til at udveksle data og muliggøre informationsdeling ([587]). Selvom formålet med de anvendte formater er at opnå indbyrdes kompatibilitet, pålægger GDPR ikke særlige henstillinger om det særlige format, som skal stilles til rådighed: Formaterne kan være forskellige fra sektor til sektor ([588]).

I medfør af Artikel 29-Gruppens retningslinjer understøtter retten til dataportabilitet »brugervalg, brugerkontrol og brugerbestemmelse« og er rettet mod at give registrerede kontrol over deres egne personoplysninger ([589]). Retningslinjerne præciserer de væsentligste elementer i dataportabilitet, som omfatter:

- de registreredes ret til at modtage deres egne personoplysninger, som den dataansvarlige har behandlet, i et struktureret, almindeligt anvendt, maskinlæsbart og indbyrdes kompatibelt format

- retten til at overføre personoplysninger fra én dataansvarlig til en anden uden hindring, hvis dette er teknisk muligt

- kontrolordningen – når en dataansvarlig svarer på en anmodning om dataportabilitet, handler denne ud fra den registreredes anvisninger, hvilket betyder, at denne ikke er ansvarlig for modtagerens overholdelse af databeskyttelseslovgivningen, siden den registrerede bestemmer, hvem oplysningerne overføres til

- udøvelsen af retten til dataportabilitet er uden forbehold for andre rettigheder, hvilket er tilfældet for alle rettigheder i GDPR.

([585]) *Ibid.*, betragtning 68 og artikel 20, stk. 1.

([586]) *Ibid.*, betragtning 68.

([587]) Europa-Kommissionen, Meddelelse om stærkere og mere intelligente informationssystemer for grænser og sikkerhed, COM(2016) 205 final, 2. april 2016.

([588]) Artikel 29-Gruppen (2016), *Retningslinjer vedrørende retten til dataportabilitet*, WP 242, 13. december 2016 og revideret den 5. april 2017, s. 13.

([589]) *Ibid.*

6.1.6. Ret til indsigelse

Registrerede kan påberåbe sig deres ret til indsigelse mod behandling af personoplysninger på baggrund af deres særlige situation og i forbindelse med oplysninger behandlet med henblik på direkte markedsføring. Retten til indsigelse kan udøves gennem automatiske midler.

Retten til indsigelse i medfør af den registreredes særlige situation

Registrerede har ingen generel ret til at gøre indsigelse mod behandlingen af deres oplysninger ([590]). Artikel 21, stk. 1, i GDPR tillægger den registrerede beføjelser til at fremkomme med indsigelser i medfør af vedkommendes særlige situation, når behandlingens retsgrundlag er den dataansvarliges udførelse af en opgave, som udføres i offentlighedens interesse, eller når behandlingen er baseret på den dataansvarliges legitime interesser ([591]). Retten til indsigelse er gældende ved aktiviteter med profilering. En lignende rettighed er blevet anerkendt i den moderniserede konvention 108 ([592]).

Retten til indsigelse i medfør af den registreredes særlige situation er rettet mod at opnå den rigtige balance mellem den registreredes databeskyttelsesrettigheder og andres legitime rettigheder til behandlingen af oplysninger. EU-Domstolen har dog præciseret, at den registreredes rettigheder generelt vejer tungere end en dataansvarligs økonomiske interesser, alt efter denne »oplysnings art, og hvor følsom den er for den berørte persons privatliv, samt offentlighedens interesse i at råde over denne oplysning« ([593]). I henhold til GDPR hviler bevisbyrden hos dataansvarlige, som skal komme med en vægtig begrundelse for at fortsætte behandlingen ([594]). På lignende vis præciserer den forklarende rapport til den moderniserede konvention 108, at de legitime begrundelser for databehandling (som kan veje tungere end de registreredes ret til indsigelse) skal påvises på et individuelt grundlag ([595]).

([590]) Se også EMD, *M.S. mod Sverige*, nr. 20837/92, 27. august 1997 (hvor medicinske data blev videregivet uden samtykke eller mulighed for indsigelse); EMD, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987 og EMD, *Mosley mod Det Forenede Kongerige*, nr. 48009/08, 10. maj 2011.

([591]) Generel forordning om databeskyttelse, betragtning 69, og artikel 6, stk. 1, litra e) og f).

([592]) Den moderniserede konvention 108, artikel 9, stk. 1, litra d). Henstilling om profilering, artikel 5, stk. 3.

([593]) EU-Domstolen, C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014, præmis 81.

([594]) Se også den moderniserede konvention 108, artikel 98, stk. 1, litra d), som fastlægger, at den registrerede kan gøre indsigelse mod behandlingen af vedkommendes oplysninger, medmindre den dataansvarlige påviser legitime grundlag for behandlingen, der vejer tungere end vedkommendes interesser eller rettigheder og grundlæggende frihedsrettigheder.

([595]) Forklarende rapport til den moderniserede konvention 108, stk. 78.

Eksempel: I *Manni* ([596])-sagen fastholdt EU-Domstolen, at Salvatore Manni ikke havde ret til at indhente sletningen af hans personoplysninger fra selskabsregistret grundet det legitime formål med offentliggørelsen af personoplysningerne i selskabsregistret, navnlig behovet for at beskytte tredjemænds interesser og sikre retssikkerhed. Den anerkendte dog eksistensen af en ret til indsigelse mod behandlingen ved at fastlægge, at »der kan findes specifikke situationer, i hvilke der foreligger vægtige legitime grunde, der vedrører den registreredes særlige situation, der undtagelsesvis berettiger, at aktindsigten i personoplysninger om vedkommende, der er indført i registret, efter udløb af en tilstrækkelig lang tidsfrist [...] begrænses til tredjemænd, som godtgør, at de har en specifik interesse i at foretage søgninger heri«.

EU-Domstolen vurderede, at det er de nationale domstoles ansvar at foretage en vurdering i de enkelte sager, hvor de tager hensyn til enkeltpersonens pågældende omstændigheder, og om der eksisterede legitime og vægtige grunde, som undtagelsesvis kan berettige, at tredjemænd har begrænset adgang til personoplysninger i selskabsregistre. I sagen med Salvatore Manni gjorde Domstolen det dog klart, at det faktum, at offentliggørelsen af hans personoplysninger i registret angiveligt påvirkede hans kundekreds, ikke kan anses som værende en legitim og vægtig grund. Salvatore Mannis potentielle kunder havde en legitim interesse i at have adgang til oplysninger vedrørende hans tidligere virksomheds konkurserklæring.

Konsekvensen af en berettiget indsigelse er, at den dataansvarlige ikke længere må behandle de pågældende oplysninger. Behandlingsaktiviteter udført på den registreredes oplysninger inden indsigelsen forbliver dog legitime.

Retten til indsigelse mod behandling af oplysninger med henblik på direkte markedsføring

Artikel 21, stk. 2, i GDPR fastlægger en særlig ret til at gøre indsigelse mod brugen af personoplysninger med henblik på direkte markedsføring, hvilket nærmere præciserer artikel 13 i e-databeskyttelsesdirektivet. En sådan ret er også fastlagt i den moderniserede konvention 108 samt i Europarådets henstilling om direkte

([596]) EU-Domstolen, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 9. marts 2017, præmis 47 og 60.

markedsføring ([597]). Den forklarende rapport til den moderniserede konvention 108 præciserer, at indsigelser mod behandling af oplysninger med henblik på direkte markedsføring bør føre til ubetinget sletning eller fjernelse af de pågældende personoplysninger ([598]).

Den registrerede har ret til at gøre indsigelse mod brugen af vedkommendes personoplysninger til direkte markedsføring på ethvert tidspunkt og uden vederlag. Registrerede skal oplyses om denne ret på en tydelig måde, som er adskilt fra andre informationer.

Retten til indsigelse gennem automatiske midler

Når personoplysninger benyttes og behandles til informationssamfundstjenester, kan den registrerede udøve sin ret til indsigelse mod behandlingen af vedkommendes oplysninger gennem automatiske midler.

Informationssamfundstjenester defineres som »enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager« ([599]).

Dataansvarlige, der tilbyder informationssamfundstjenester, skal have fastlagt passende tekniske ordninger og procedurer til at sikre, at retten til indsigelse gennem automatiske midler kan udøves effektivt ([600]). Dette kan for eksempel omfatte blokering af cookies på websteder eller deaktivering af sporing af navigation på internettet.

Retten til at gøre indsigelse med henblik på videnskabelig eller historisk forskning eller statistiske formål

Under EU-retten skal videnskabelig forskning fortolkes bredt, inklusive, for eksempel, teknologisk udvikling og demonstration, grundforskning, anvendt forskning og privat finansieret forskning ([601]). Historisk forskning omfatter også forskning i genealogisk

([597]) Europarådet, Ministerudvalget (1985), Henstilling Rec(85)20 til medlemsstaterne om beskyttelse af personoplysninger, der anvendes med henblik på markedsføring, 25. oktober 1985, artikel 4, stk. 1.

([598]) Forklarende rapport til den moderniserede konvention 108, stk. 79.

([599]) Direktiv 98/34/EF, som ændret ved 98/48/EF om en informationsprocedure med hensyn til tekniske standarder og forskrifter, artikel 1, stk. 2.

([600]) Generel forordning om databeskyttelse, artikel 21, stk. 5.

([601]) *Ibid*., betragtning 159.

øjemed, idet forordningen dog ikke bør gælde for afdøde personer ([602]). Ved statistiske formål forstås enhver indsamling og behandling af personoplysninger, der er nødvendig for statistiske undersøgelser eller frembringelse af statistiske resultater ([603]). Den registreredes særlige situation er som sagt retsgrundlaget for retten til at gøre indsigelse mod behandling af personoplysninger med henblik på forskning ([604]). Den eneste undtagelse er behandlingens nødvendighed til gennemførelse af en opgave, som udføres i offentlighedens interesse. Retten til sletning gælder dog ikke, når behandlingen er nødvendig (med eller uden hensyn til samfundsinteresser) for videnskabelig eller historisk forskning eller statistiske formål ([605]).

GDPR afvejer kravene til videnskabelig, statistisk eller historisk forskning og registreredes rettigheder med særlige garantier og undtagelser i artikel 89. EU's eller medlemsstaters lovgivning kan fastlægge undtagelser fra retten til indsigelse, hvis en sådan ret gør det umuligt eller alvorligt hæmmer at opnå forskningens formål, og hvis sådanne undtagelser er nødvendige til at opfylde disse formål.

Under **Europarådets retsorden** fastsætter artikel 9, stk. 2, i den moderniserede konvention 108, at begrænsninger af registreredes rettigheder, herunder retten til indsigelse, kan fastlægges i lovgivningen vedrørende databehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål, når der ikke er nogen identificerbar risiko for overtrædelse af registreredes rettigheder og frihedsrettigheder.

Den forklarende rapport (stk. 41) anerkender også, at registrerede bør have mulighed for kun at give deres samtykke til visse forskningsområder eller dele af forskningsprojekter i det omfang, at det planlagte formål tillader det, og gøre indsigelse, hvis de mener, at behandlingen i overdreven grad overskrider deres rettigheder og frihedsrettigheder uden en legitim grund.

Med andre ord vil en sådan behandling derfor på forhånd betragtes som værende forenelig, hvis andre garantier er fastlagt, og aktiviteterne principielt udelukker enhver brug af informationen indsamlet til afgørelser eller foranstaltninger vedrørende en bestemt enkeltperson.

([602]) *Ibid.*, betragtning 160.

([603]) *Ibid.*, betragtning 162.

([604]) *Ibid.*, artikel 21, stk. 6.

([605]) *Ibid.*, artikel 17, stk. 3, litra d).

6.1.7. Automatiske individuelle afgørelser, herunder profilering

Automatiske afgørelser er afgørelser, som foretages ved brug af personoplysninger, der udelukkende er behandlet via automatiske midler uden menneskelig indgriben. **Under EU-retten** må registrerede ikke udsættes for automatiske afgørelser, som har retsvirkninger, eller på tilsvarende vis betydeligt påvirker den pågældende. Hvis sådanne afgørelser med sandsynlighed vil påvirke enkeltpersoners dagligdag i væsentlig grad, da de for eksempel vedrører kreditværdighed, elektronisk rekruttering, arbejdsindsats eller analyser af adfærd og pålidelighed, så er det nødvendigt med særlig beskyttelse for at undgå negative følger. Automatisk behandling omfatter profilering, der består af enhver form for automatisk evaluering af »personoplysninger, der evaluerer de personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den registreredes arbejdsindsats, økonomisk situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografiske position eller bevægelser« ([606]).

Eksempel: Kreditoplysningsbureauer indsamler visse oplysninger for hurtigt at vurdere en fremtidig kundes kreditværdighed, såsom hvordan kunden har forvaltet sine kredit- og forsyningstjenestekonti, detaljer om kundens tidligere adresser samt oplysninger fra offentlige kilder, såsom valglister, offentlige registre (herunder retsafgørelser), eller oplysninger om konkurserklæring og insolvens. Disse personoplysninger indføres herefter i en vurderingsalgoritme, som beregner en samlet værdi for den potentielle kundes kreditværdighed.

I henhold til Artikel 29-Gruppen udgør retten til ikke at være underlagt afgørelser udelukkende baseret på automatisk behandling, der kan have retsvirkninger for den registrerede, eller som i væsentlig grad påvirker vedkommende, et generelt forbud og kræver ikke, at den registrerede proaktivt gør indsigelse mod en sådan afgørelse ([607]).

I medfør af GDPR kan automatiske afgørelser med retsvirkning, eller som betydeligt påvirker den pågældende, dog være acceptabelt, hvis det er nødvendigt til

([606]) *Ibid.*, betragtning 71, artikel 4, stk. 4, og artikel 22.

([607]) Se også Artikel 29-Gruppen, *Retningslinjer for automatiseret individuel beslutningstagning og profilering i medfør af forordning 2016/679*, WP 251, 3. oktober 2017, s. 15.

at indgå en kontrakt eller fuldføre en kontrakt mellem den dataansvarlige og den registrerede, eller hvis den registrerede har afgivet udtrykkeligt samtykke. Automatiske afgørelser er også acceptabelt, hvis det er godkendt ved lov, og hvis den registreredes rettigheder, frihedsrettigheder og legitime interesser er passende beskyttet ([608]).

GDPR fastlægger også, at en af den dataansvarliges forpligtelser i forbindelse med oplysning ved indsamling af personoplysninger er, at registrerede skal meddeles om eksistensen af automatiske afgørelser, herunder profilering ([609]). Retten til adgang til personoplysninger behandlet af den dataansvarlige forbliver upåvirket ([610]). Informationen bør ikke kun angive det faktum, at profilering finder sted, men bør også indeholde meningsfulde oplysninger om logikken involveret i profileringen samt behandlingens forventede konsekvenser for enkeltpersoner ([611]). For eksempel skal et sygeforsikringsselskab, som benytter automatiske afgørelser på ansøgninger, give registrerede generelle oplysninger om, hvordan algoritmen fungerer, og hvilke faktorer algoritmen benytter til at beregne deres forsikringspræmier. På lignende vis kan registrerede, når de udøver deres »ret til indsigt«, anmode om oplysninger fra den dataansvarlige om eksistensen af automatiske afgørelser og meningsfulde oplysninger om logikken heri ([612]).

Oplysningerne givet til registrerede er beregnet til at sikre gennemsigtighed og gøre det muligt for registrerede at give informeret samtykke, hvis det er tilfældet, eller sikre menneskelig indgriben. Den dataansvarlige skal gennemføre passende foranstaltninger til at sikre den registreredes rettigheder, frihedsrettigheder og legitime interesser. Dette omfatter som minimum retten til menneskelig indgriben fra den dataansvarliges side og muligheden for, at den registrerede kan fremkomme med sine synspunkter og bestride en afgørelse baseret på automatisk behandling af deres personoplysninger ([613]).

Artikel 29-Gruppen har givet videre vejledning i brugen af automatiske afgørelser under GDPR ([614]).

([608]) Generel forordning om databeskyttelse, artikel 22, stk. 2.

([609]) *Ibid.*, artikel 12.

([610]) *Ibid.*, artikel 15.

([611]) *Ibid.*, artikel 13, stk. 2, litra f).

([612]) *Ibid.*, artikel 15, stk. 1, litra h).

([613]) *Ibid.*, artikel 22, stk. 3.

([614]) Artikel 29-Gruppen (2017), *Retningslinjer for automatiseret individuel beslutningstagning og profilering i medfør af forordning 2016/679*, WP 251, 3. oktober 2017.

Under Europarådets retsorden har fysiske personer en ret til ikke at være underlagt en afgørelse, som påvirker dem i væsentlig grad og udelukkende er baseret på automatisk behandling, uden at deres holdninger tages under overvejelse ([615]). Kravet om at tage hensyn til den registreredes holdninger, når afgørelser er baseret på automatisk behandling, betyder, at vedkommende har ret til at anfægte sådanne afgørelser og bør kunne bestride alle unøjagtigheder i de personoplysninger, som den dataansvarlige benytter, og anfægte, om en profil, som tillægges vedkommende, er relevant ([616]). En fysisk person kan dog ikke udøve denne ret, hvis den automatiske afgørelse er godkendt ved en lov, som den dataansvarlige er underlagt, og som også fastlægger passende foranstaltninger til at garantere den registreredes rettigheder, frihedsrettigheder og legitime interesser. Derudover har registrerede ret til at få baggrunden for den udførte databehandling at vide ved anmodning ([617]). Den forklarende rapport til den moderniserede konvention 108 bruger credit scoring som eksempel. Fysiske personer bør være berettiget til ikke kun at kende til den positive eller negative afgørelse om deres kredit, men også *logikken* bag behandlingen af deres personoplysninger, der resulterede i denne afgørelse. En forståelse af disse elementer bidrager til den effektive udøvelse af andre vigtige garantier, såsom retten til indsigelse og retten til at indgive klage til en kompetent myndighed ([618]).

Henstillingen om profilering angiver, selvom den ikke er juridisk bindende, betingelser for indsamling og behandling af personoplysninger i forbindelse med profilering ([619]). Den indeholder bestemmelser om behovet for at sikre, at behandlingen i forbindelse med profilering skal være rimelig, lovlig, forholdsmæssig og til fastlagte og legitime formål. Den indeholder også bestemmelser om de informationer, som dataansvarlige skal give til registrerede. Datapålidelighedsprincippet – som kræver, at dataansvarlige træffer foranstaltninger til at korrigere faktorer for dataunøjagtighed for at begrænse de risici og fejl, som profilering kan medføre, og for periodisk at evaluere kvaliteten af de anvendte oplysninger og algoritmer – optræder også i henstillingen.

([615]) Den moderniserede konvention 108, artikel 9, stk. 1, litra a).

([616]) Forklarende rapport til den moderniserede konvention 108, stk. 75.

([617]) Den moderniserede konvention108, artikel 9, stk. 1, litra c).

([618]) Forklarende rapport til den moderniserede konvention 108, stk. 77.

([619]) Europarådet, Henstilling CM/Rec(2010)13 til medlemsstaterne om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger så vidt angår profilering, artikel 5, stk. 5.

6.2. Retsmidler, ansvar, sanktioner og erstatning

Hovedpunkter

- I henhold til den moderniserede konvention 108 skal den nationale lovgivning for de kontraherende parter fastlægge passende retsmidler og sanktioner mod overtrædelser af retten til databeskyttelse.
- I EU fastlægger GDPR retsmidler til registrerede i tilfælde af overtrædelser af deres rettigheder samt sanktioner mod dataansvarlige og databehandlere, som ikke overholder forordningens bestemmelser. Den fastlægger også retten til erstatning og ansvar.
    - Registrerede har ret til at indgive en klage til en tilsynsmyndighed vedrørende påståede overtrædelser af forordningen samt retten til effektive retsmidler og til at modtage erstatning.
    - Under udøvelse af deres ret til effektive retsmidler kan enkeltpersoner repræsenteres af nonprofitorganisationer, som er aktive på området for databeskyttelse.
    - Den dataansvarlige eller databehandleren er ansvarlig for alle materielle og ikke-materielle skader som følge af overtrædelsen.
    - Tilsynsmyndighederne har beføjelser til at pålægge administrative bøder for overtrædelser af forordningen på op til 20 000 000 EUR eller, i tilfælde af en virksomhed, 4 % af den samlede årlige omsætning på verdensplan – alt efter hvad der er størst.
- Registrerede kan som sidste udvej og under visse betingelser indbringe overtrædelser af databeskyttelseslovgivningen for EMD.
- Alle juridiske eller fysiske personer har ret til at indgive en klage mod en afgørelse fra Det Europæiske Databeskyttelsesråd ved EU-Domstolen under betingelserne fastlagt i traktaterne.

Vedtagelse af retslige instrumenter er ikke tilstrækkeligt til at sikre beskyttelsen af personoplysninger i Europa. For at gøre europæiske databeskyttelsesregler effektive er det nødvendigt at fastlægge mekanismer, som gør det muligt for enkeltpersoner at modarbejde overtrædelser af deres rettigheder og kræve erstatning for eventuel forvoldt skade. Det er også vigtigt, at tilsynsmyndigheder har beføjelsen til at pålægge sanktioner, som er effektive, afskrækkende og forholdsmæssige i forhold til den pågældende overtrædelse.

Rettigheder under databeskyttelseslovgivningen kan udøves af den person, hvis rettigheder er på spil. Dette vil være den registrerede. Andre personer, som opfylder de fornødne krav i national lovgivning, kan dog også repræsentere registrerede under udøvelse af deres rettigheder. I henhold til flere nationale lovgivninger skal børn og personer med intellektuelle handicap repræsenteres af deres værger ([620]). Under europæisk databeskyttelseslovgivning kan en forening, hvis lovlige formål er at fremme databeskyttelsesrettigheder, repræsentere registrerede foran en tilsynsmyndighed eller domstol ([621]).

6.2.1. Ret til at indgive klage til en tilsynsmyndighed

Under både **Europarådets retsorden** og **EU-retten** har enkeltpersoner ret til at indgive anmodninger og klager til den kompetente tilsynsmyndighed, hvis vedkommende mener, at behandlingen af deres personoplysninger ikke udføres i overensstemmelse med loven.

Den moderniserede konvention 108 anerkender registreredes ret til at modtage bistand fra en tilsynsmyndighed til udøvelsen af deres rettigheder under konventionen, uanset deres nationalitet eller bopæl ([622]). En anmodning om bistand må kun afvises under usædvanlige omstændigheder, og registrerede skal ikke dække omkostninger og gebyrer knyttet til bistanden ([623]).

Lignende bestemmelser kan findes i EU's retsorden. GDPR kræver, at tilsynsmyndigheder vedtager foranstaltninger til at imødekomme indsendelse af klager, såsom oprettelse af en elektronisk klageformular ([624]). Den registrerede kan indgive klagen ved tilsynsmyndigheden i medlemsstaten med vedkommendes sædvanlige opholdssted, arbejdssted, eller hvor den påståede overtrædelse har fundet sted ([625]). Klager skal undersøges, og tilsynsmyndigheden skal underrette den berørte person omkring resultatet af klagens retsforløb ([626]).

([620]) FRA (2015), Håndbog om europæisk lovgivning om børns rettigheder, Luxembourg, Publikationskontoret og FRA (2013), Retlig handleevne for personer med udviklingshæmninger og personer med sindslidelser, Luxembourg, Publikationskontoret.

([621]) Generel forordning om databeskyttelse, artikel 80.

([622]) Den moderniserede konvention 108, artikel 18.

([623]) *Ibid*., artikel 16-17.

([624]) Generel forordning om databeskyttelse, artikel 57, stk. 2.

([625]) *Ibid*., artikel 77, stk. 1.

([626]) *Ibid*., artikel 77, stk. 2.

EU-institutioners eller -organers potentielle overtrædelser kan meddeles til Den Europæiske Tilsynsførende for Databeskyttelse ([627]). Undlader EDPS at svare inden udløbet af fristen på seks måneder, er dette at sidestille med en afgørelse om afvisning af klagen. Appeller mod EDPS' afgørelser kan forelægges for EU-Domstolen inden for rammerne af forordning (EF) nr. 45/2001, som forpligter EU-institutioner og -organer til at overholde databeskyttelsesregler.

Der skal være mulighed for at appellere til domstolene mod afgørelser fra en national tilsynsmyndighed. Dette gælder både for registrerede samt dataansvarlige og databehandlere, som har været part i et retssag ved en tilsynsmyndighed.

Eksempel: I september 2017 udstedte den spanske databeskyttelsesmyndighed en bøde til Facebook for at overtræde flere databeskyttelsesforskrifter. Tilsynsmyndigheden fordømte det sociale netværk for at indsamle, lagre og behandle personoplysninger, inklusive særlige kategorier af personoplysninger, til reklameformål og uden at indhente samtykke fra den registrerede. Afgørelsen var baseret på en undersøgelse udført på tilsynsmyndighedens eget initiativ.

6.2.2. Ret til effektive retsmidler

Udover retten til at klage til tilsynsmyndigheden skal fysiske personer have ret til effektive retsmidler og til at indbringe deres sag for en domstol. Retten til effektive retsmidler er veletableret i den europæiske retstradition og anerkendes som en grundlæggende rettighed både under artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 13 i EMRK ([628]).

Under EU-retten understreges vigtigheden af at give registrerede adgang til effektive retsmidler i tilfælde af en overtrædelse af deres rettigheder både i bestemmelser i GDPR – der fastlægger en ret til effektive retsmidler over for tilsynsmyndigheder, dataansvarlige og databehandlere – og i EU-Domstolens retspraksis.

([627]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, EFT L 8 af 12. januar 2001.

([628]) Se for eksempel EMD, *Karabeyoğlu mod Tyrkiet*, nr. 30083/10, 7. juni 2016, og EMD, *Mustafa Sezgin Tanrıkulu mod Tyrkiet*, nr. 27473/06, 18. juli 2017.

Eksempel: I *Schrems* ([629])-sagen erklærede EU-Domstolen beslutningen om tilstrækkeligheden af safe harbour-ordningen for ugyldig. Den afgørelse har tilladt internationale dataoverførsler fra EU til organisationer i USA, som er selvcertificerede under safe harbour-ordningen. EU-Domstolen anså safe harbour-ordningen for at have flere mangler, der tilsidesatte EU-borgeres grundlæggende rettigheder til beskyttelse af privatlivets fred og beskyttelse af personoplysninger samt retten til effektive retsmidler.

I forbindelse med overtrædelsen af rettighederne til privatlivets fred og databeskyttelse fremhævede EU-Domstolen, at amerikansk lovgivning tillod, at visse offentlige myndigheder fik adgang til de personoplysninger, der blev overført fra medlemsstater til USA, og kunne behandle dem på en måde, som var uforenelig med overførslens oprindelige formål og ikke var begrænset til det strengt nødvendige og forholdsmæssige til at beskytte den nationale sikkerhed. Vedrørende retten til effektive retsmidler bemærkede den, at registrerede ikke havde nogen administrative eller retslige klagemuligheder, hvormed de kunne få adgang til og berigtige eller slette, alt efter tilfældet, oplysningerne omhandlende dem. EU-Domstolen konkluderede, at lovgivning, som ikke gav mulighed for at gøre brug af retsmidler til at få adgang til, berigtige eller slette deres personoplysninger, ikke opfylder »det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som denne er sikret ved chartrets artikel 47«. Den understregede, at eksistensen af en effektiv domstolsbeskyttelse, som skal sikre overholdelsen af retlige bestemmelser, er uløseligt forbundet med eksistensen af en retsstat.

Fysiske personer, dataansvarlige eller databehandlere kan anfægte en tilsynsmyndigheds juridisk bindende afgørelse ved at indbringe sagen for en domstol ([630]). Udtrykket »afgørelse« skal fortolkes bredt og omfatter tilsynsmyndigheders udøvelse af beføjelser vedrørende undersøgelser, sanktioner og godkendelse samt afgørelser om at nægte eller afvise en klage. Foranstaltninger, som ikke er juridisk bindende, såsom udtalelser eller rådgivning afgivet af tilsynsmyndigheden, kan dog ikke danne grundlag for en sag ved en

([629]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015.

([630]) Generel forordning om databeskyttelse, artikel 78.

domstol ([631]). Sagen skal anlægges ved domstolene i den medlemsstat, hvor den pågældende tilsynsmyndighed er etableret ([632]).

I tilfælde, hvor en dataansvarlig eller databehandler overtræder en registrerets rettigheder, er registrerede berettiget til at indbringe en klage for en domstol ([633]). Ved sager, som indledes mod en dataansvarlig eller databehandler, er det særligt vigtigt, at enkeltpersoner får mulighed for at vælge, hvor sagen anlægges henne. De kan vælge at gøre dette enten i medlemsstaten, hvor den dataansvarlige eller databehandleren er etableret, eller i medlemsstaten, hvor de berørte registrerede har deres sædvanlige opholdssted ([634]). Den anden mulighed gør det i høj grad lettere for enkeltpersoner at udøve deres rettigheder, da det gør dem i stand til at anlægge sager i den stat, hvor de har bopæl, og inden for en kendt jurisdiktion. Begrænsning af området for retssager mod dataansvarlige og databehandlere til den medlemsstat, som sidstnævnte er etableret i, kan afskrække registrerede med bopæl i andre medlemsstater fra at indbringe sagen for en domstol, da det ville indebære omkostninger til rejser og andet, og retssagen ville muligvis foregå på et fremmed sprog og i en udenlandsk jurisdiktion. Den eneste undtagelse omhandler sager, hvor den dataansvarlige eller databehandleren er offentlige myndigheder, og behandlingen gennemføres under udøvelse af deres offentligretlige beføjelser. I dette tilfælde er det kun domstolene i staten for den relevante offentlige myndighed, som har kompetence til at anlægge søgsmålet ([635]).

Selvom sager vedrørende databeskyttelsesregler i de fleste tilfælde afgøres i medlemsstaternes domstole, kan nogle sager forelægges for EU-Domstolen. Den første mulighed er, når en registreret, dataansvarlig, databehandler eller tilsynsmyndighed vil anlægge sag om annullering af en afgørelse fra EDPB. Sagen er dog underlagt betingelserne i artikel 263 i TEUF, hvilket betyder, at disse enkeltpersoner og enheder, for at sagen kan indbringes, skal påvise, at Databeskyttelsesrådets afgørelse berører dem direkte og individuelt.

Det andet scenarie omhandler tilfælde, hvor EU-institutioner eller -organer ulovligt behandler personoplysninger. I tilfælde, hvor EU-institutioner overtræder databeskyttelseslovgivning, kan registrerede anlægge en sag ved Den Europæiske Unions

([631]) *Ibid.*, betragtning 143.
([632]) *Ibid.*, artikel 78, stk. 3.
([633]) *Ibid.*, artikel 79.
([634]) *Ibid.*, artikel 79, stk. 2.
([635]) *Ibid.*

Ret (Retten er en del af EU-Domstolen). Retten er i første instans ansvarlig for sager vedrørende EU-institutioners overtrædelser af EU-retten. Sager mod EDPS – som er en EU-institution – kan dermed også indbringes for Den Europæiske Unions Ret ([636]).

Eksempel: I *Bavarian Lager* ([637])-sagen anmodede virksomheden Europa-Kommissionen om adgang til det fulde referat af et møde, som Kommissionen havde afholdt, og som angiveligt vedrørte retlige spørgsmål, som var relevante for virksomheden. Kommissionen afviste virksomhedens anmodning om indsigt med henvisning til databeskyttelsesinteresser, der var vigtigere ([638]). Med henvisning til artikel 32 i forordningen om databeskyttelse inden for EU-institutionerne indbragte Bavarian Lager denne beslutning for Retten i Første Instans (forgængeren for Retten). I sin afgørelse i sag T-194/04, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd*, annullerede Retten Kommissionens beslutning om at afvise anmodningen om indsigt. Kommissionen appellerede denne afgørelse til EU-Domstolen.

EU-Domstolens Store Afdeling afsagde sin dom, som tilsidesatte Rettens dom og bekræftede Europa-Kommissionens afvisning af anmodningen om indsigt i det fulde referat af mødet for at beskytte personoplysningerne for personerne ved mødet. EU-Domstolen mente, at Europa-Kommissionen havde handlet rigtigt ved at afvise at offentliggøre oplysningerne, da deltagerne ikke havde givet deres samtykke til offentliggørelse af deres personoplysninger. Derudover havde Bavarian Lager ikke påvist nødvendigheden af at tilgå oplysningerne.

Endelig kan registrerede, tilsynsmyndigheder, dataansvarlige eller databehandlere i forbindelse med nationale retssager bede den nationale domstol om at anmode om, at EU-Domstolen præciserer fortolkningen og gyldigheden af retsakter fra EU-institutioner, -organer, -kontorer eller -agenturer. Sådanne præciseringer kaldes for præjudicielle afgørelser. Dette er ikke et direkte retsmiddel for klageren, men det gør det muligt for nationale domstole at sikre, at de benytter den korrekte fortolkning af EU-retten. Det er igennem denne mekanisme med præjudicielle afgørelser, at skelsættende sager — såsom *Digital Rights Ireland* og *Kärntner Landesregierung*

([636]) Forordning (EF) nr. 45/2001, artikel 32, stk. 3.

([637]) EU-Domstolen, C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd* [GC], 2010.

([638]) Der findes en analyse af sagen i EDPS (2011), Public access to documents containing personal data after the Bavarian Lager ruling, Bruxelles, EDPS.

m.fl. ([639]) samt *Schrems* ([640]) — som i stor grad påvirkede udviklingen af europæisk databeskyttelseslovgivning, nåede EU-Domstolen.

Eksempel: *Digital Rights Ireland* og *Kärntner Landesregierung m.fl.* ([641]) var en forenet sag indbragt af den irske højesteret og den østrigske forfatningsdomstol vedrørende overensstemmelsen af direktiv 2006/24/EF (datalagringsdirektivet) med europæisk databeskyttelseslovgivning. Den østrigske forfatningsdomstol indsendte spørgsmål til EU-Domstolen vedrørende gyldigheden af artikel 3-9 i direktiv 2006/24/EF på baggrund af artikel 7, 9 og 11 i Den Europæiske Unions charter om grundlæggende rettigheder. Disse omhandlede, hvorvidt visse bestemmelser i den østrigske forbundslov om telekommunikationer, som gennemfører datalagringsdirektivet, var uforenelige med aspekter af det tidligere databeskyttelsesdirektiv og forordningen om databeskyttelse inden for EU-institutionerne.

I sagen *Kärntner Landesregierung m.fl.* påstod Michael Seitlinger, som er en af sagsøgerne i hovedsagen ved forfatningsdomstolen, at han anvendte telefonen, internettet og e-mail til både arbejdsformål og private formål. De oplysninger, han sendte og modtog, passerede følgelig offentlige telekommunikationsnet. I henhold til den østrigske telekommunikationslov fra 2003 er hans telekommunikationsudbyder retligt forpligtet til at indsamle og lagre data om hans anvendelse af nettet. Michael Seitlinger mente, at denne indsamling og lagring af hans personoplysninger er teknisk unødvendig for at sende og modtage informationer via nettet. Indsamlingen og lagringen af disse oplysninger er heller ikke på nogen måde nødvendig for at kunne fakturere ham. Michael Seitlinger har bestemt ikke givet sit samtykke til denne anvendelse af sine personoplysninger. Den eneste grund til indsamlingen og lagringen heraf var den østrigske telekommunikationslov fra 2003.

Michael Seitlinger anlagde derfor sag ved den østrigske forfatningsdomstol med påstand om, at de lovfæstede forpligtelser, der var pålagt hans telekommunikationsudbyder, krænkede hans grundlæggende rettigheder

([639]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl. og Kärntner Landesregierung m.fl.* [GC], 8. april 2014.

([640]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015.

([641]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014.

sikret ved artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder. Da den østrigske lovgivning gennemførte EU-lovgivning (det daværende datalagringsdirektiv), henviste den østrigske forfatningsdomstol sagen til EU-Domstolen, så denne kunne vurdere direktivets forenelighed med rettighederne til privatliv og databeskyttelse fastlagt i Den Europæiske Unions charter om grundlæggende rettigheder.

EU-Domstolens Store Afdeling afsagde dom i sagen, hvilket resulterede i, at EU's datalagringsdirektiv blev annulleret. EU-Domstolen konkluderede, at direktivet medførte et særligt groft indgreb i de grundlæggende rettigheder til privatliv og databeskyttelse, uden at dette indgreb var begrænset til det strengt nødvendige. Direktivet havde et legitimt formål, da det gav nationale myndigheder yderligere muligheder for at efterforske og retsforfølge kriminalitet, hvilket gjorde det til et værdifuldt værktøj til strafferetlige efterforskninger. EU-Domstolen bemærkede dog, at begrænsningerne af de grundlæggende rettigheder kun bør finde anvendelse, når det er strengt nødvendigt, og bør ledsages af klare og tydelige regler vedrørende deres omfang samt garantier for enkeltpersoner.

I henhold til EU-Domstolen opfyldte direktivet ikke dette nødvendighedskriterie. For det første fastlagde den ikke klare og tydelige regler, som begrænsede indgrebets omfang. Direktivet fandt anvendelse for alle metadata for alle brugere af alle elektroniske kommunikationsmidler i stedet for at kræve, at der var en forbindelse mellem de lagrede oplysninger og alvorlig kriminalitet. Det udgjorde derfor et indgreb i rettighederne til privatliv og databeskyttelse for praktisk set hele EU's befolkning, hvilket kan betragtes som uforholdsmæssigt. Det indeholdt ingen betingelser, som begrænsede de personer, som havde tilladelse til at tilgå personoplysninger, og denne adgang var heller ikke underlagt proceduremæssige betingelser, såsom kravet om at indhente godkendelse fra en administrativ myndighed eller domstol inden adgang. Endelig fastlagde direktivet ikke klare garantier for beskyttelsen af lagrede oplysninger. Det var dermed ikke i stand til at sikre en effektiv beskyttelse af oplysningerne mod farerne for misbrug og mod ulovlig adgang og brug ([642]).

([642]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014, præmis 69.

Principielt skal EU-Domstolen svare på henviste spørgsmål, og den kan ikke nægte at afgive en præjudiciel afgørelse på den baggrund, at svaret hverken ville være relevant eller rettidigt i forbindelse med den oprindelige sag. Den kan dog afvise spørgsmålet, hvis det ikke hører under dennes kompetenceområde ([643]). EU-Domstolen træffer kun afgørelse om elementerne i anmodningen om en præjudiciel afgørelse, den har fået forelagt. Den nationale domstol har stadig kompetence til at afgøre hovedsagen ([644]).

Under Europarådets retsorden skal kontraherende parter fastlægge passende retslige og udenretslige mekanismer for overtrædelser af bestemmelserne i den moderniserede konvention 108 ([645]). Krænkelser af databeskyttelsesrettigheder, som udgør en overtrædelse af EMRK's artikel 8, der angiveligt er begået af en af EMRK's kontraherende parter, kan derudover indbringes for EMD, når alle de tilgængelige nationale retsmidler er udtømte. For at en påstand om overtrædelse af artikel 8 i EMRK kan indbringes for EMD, skal andre antagelighedskriterier (EMRK's artikel 34-35) også opfyldes ([646]).

Selv om anmodninger til EMD kun kan rettes mod kontraherende parter, kan de også indirekte vedrøre private parters handlinger eller manglende handling, for så vidt som en kontraherende part ikke har opfyldt sine positive forpligtelser i medfør af EMRK og ikke har ydet tilstrækkelig beskyttelse mod krænkelser af databeskyttelsesrettigheder i sin nationale lovgivning.

Eksempel: I sagen *K.U. mod Finland* ([647]) klagede sagsøgeren, en mindreårig, over, at en annonce af seksuel karakter om ham var blevet offentliggjort på et datingsite på internettet. Tjenesteudbyderen havde ikke oplyst identiteten af den person, der havde offentliggjort informationen, grundet en tavshedspligt i henhold til finsk lovgivning. Sagsøgeren påstod, at finsk lovgivning ikke sikrede tilstrækkelig beskyttelse mod sådanne handlinger fra en privat person, som offentliggjorde inkriminerende oplysninger om sagsøgeren på internettet. EMD fastslog, at stater ikke kun havde pligt til at afstå fra

([643]) EU-Domstolen, C-244 /80, *Pasquale Foglia mod Mariella Novello*, 16. december 1981, og EU-Domstolen, C-467/04, *straffesagen mod Gasparini m.fl.*, 28. september 2006.

([644]) EU-Domstolen, C-438/05, *International Transport Workers' Federation og Finnish Seamen's Union mod Viking Line ABP og Ou Viking Line Eesti* [GC], 11. december 2007, præmis 85.

([645]) Den moderniserede konvention 108, artikel 12.

([646]) EMRK, artikel 34-37.

([647]) EMD, *K.U. mod Finland*, nr. 2872/02, 2. december 2008.

vilkårlig indgriben i personers privatliv, men at de også var underlagt positive forpligtelser, der kan indebære vedtagelsen af foranstaltninger med henblik på at sikre respekten for privatlivets fred, også i relationer mellem privatpersoner. I sagsøgerens tilfælde var det nødvendigt at iværksætte effektive foranstaltninger for at identificere og retsforfølge lovovertræderen for at sikre reel og effektiv beskyttelse af sagsøgeren. En sådan beskyttelse blev dog ikke sikret af staten, og Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Eksempel: I sagen *Köpke mod Tyskland* ([648]) havde sagsøgeren været under mistanke for tyveri på sin arbejdsplads og havde været udsat for skjult videoovervågning. EMD konkluderede, at der var ingen tegn på, at de nationale myndigheder ikke havde sikret en rimelig balance — inden for deres skønsbeføjelser — mellem sagsøgerens ret til respekt for sit privatliv i medfør af artikel 8 og både hendes arbejdsgivers interesse i at beskytte sine ejendomsrettigheder og offentlighedens interesse i korrekt retspleje. Sagen blev derfor afvist.

Hvis EMD finder, at en kontraherende part har krænket rettigheder, der er beskyttet af EMRK, er den kontraherende part forpligtet til at fuldbyrde EMD's dom (artikel 46 i EMRK). Fuldbyrdelsesforanstaltninger skal først bringe krænkelsen til ophør og så vidt muligt afhjælpe de negative følger for sagsøgeren. Fuldbyrdelse af domme kan også kræve generelle foranstaltninger, der kan forhindre krænkelser lig dem konstateret af EMD, enten i form af lovændring, ændring af retspraksis eller andre foranstaltninger.

Hvis EMD konstaterer en overtrædelse af EMRK, kan den i henhold til konventionens artikel 41 pålægge den kontraherende part at betale passende erstatning til sagsøgeren.

Ret til at bemyndige et organ, en organisation eller en sammenslutning, som ikke arbejder med gevinst for øje

GDPR giver enkeltpersoner mulighed for at indsende en klage til en tilsynsmyndighed eller anlægge sag ved en domstol for at bemyndige et organ, en organisation eller en sammenslutning, som ikke arbejder med gevinst for øje, til at repræsentere

([648]) EMD, *Köpke mod Tyskland*, nr. 420/07, 5. oktober 2010.

vedkommende ([649]). Disse enheder, som ikke arbejder med gevinst for øje, skal have vedtægtsmæssige formål af almen interesse og være aktive på området for databeskyttelse. De kan indgive klagen eller udøve retten til retsmidler på vegne af den/de registrerede. Forordningen giver medlemsstater mulighed for i medfør af national lovgivning at beslutte, om et organ kan indgive klager på vegne af registrerede, uafhængigt af en bemyndigelse fra den registrerede.

Denne repræsentationsrettighed giver fysiske personer mulighed for at drage nytte af sådanne ikkekommercielle enheders ekspertise og organisatoriske samt finansielle kapacitet, hvilket i høj grad øger fysiske personers mulighed for at udøve deres rettigheder. GDPR tillader, at disse enheder kan indbringe kollektive søgsmål på vegne af flere registrerede. Dette hjælper også retssystemets funktion og effektivitet, da ensartede sager grupperes og undersøges sammen.

6.2.3. Ansvar og ret til erstatning

Retten til effektive retsmidler skal bemyndige enkeltpersoner til at kunne kræve erstatning for skader, der er forvoldt som følge af behandlingen af deres personoplysninger på en måde, som overtræder den gældende lovgivning. Dataansvarliges og databehandleres ansvar for ulovlig behandling fastsættes udtrykkeligt i GDPR ([650]). Forordningen giver enkeltpersoner ret til at modtage erstatning fra den dataansvarlige eller databehandleren for både materielle og ikke-materielle skader, og dens betragtninger fastlægger, at begrebet skade »bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler formålene for denne forordning« ([651]). Dataansvarlige er ansvarlige og kan pålægges erstatningskrav, hvis de ikke opfylder deres forpligtelser under forordningen. Databehandlere hæfter kun for den skade, som er forvoldt af behandlingen, hvis pågældende ikke har opfyldt forpligtelserne i forordningen, der er rettet specifikt mod databehandlere, eller hvis pågældende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser. Hvis en dataansvarlig eller databehandler har betalt fuld erstatning, fastlægger GDPR, at den dataansvarlige eller databehandleren efterfølgende kan kræve en del af erstatningen tilbage svarende til graden af ansvar for skaden fra de andre dataansvarlige eller databehandlere, der er involveret i samme behandling ([652]). På samme tid er undtagelser

([649]) Generel forordning om databeskyttelse, artikel 80.

([650]) *Ibid.*, artikel 82.

([651]) *Ibid.*, betragtning 146.

([652]) *Ibid.*, artikel 82, stk. 2 og 5.

fra ansvarspådragelse underlagt strenge krav og dokumentation for, at den dataansvarlige eller databehandleren på ingen måde er ansvarlig for hændelsen, som gav anledning til skaden.

Erstatningen skal være »fuldstændig« i forbindelse med den forvoldte skade. Når flere dataansvarliges og databehandleres behandling fører til skader, skal hver dataansvarlig og databehandler holdes ansvarlig for alle skader. Denne regel har til mål at sikre effektiv erstatning for registrerede og en koordineret tilgang til overholdelse af databeskyttelsesreglerne for de dataansvarlige og databehandlere, som er involveret i behandlingsaktiviteter.

Eksempel: Det er ikke et krav, at registrerede anlægger en retssag og kræver erstatning fra alle enheder, som er ansvarlige for skaden, da dette kan medføre dyre og langvarige sagsforløb. Det er tilstrækkeligt at anlægge en retssag mod en af de fælles dataansvarlige, som derefter kan holdes ansvarlig for hele skaden. I sådanne tilfælde er en dataansvarlig eller databehandler, som betaler skaden, derefter berettiget til at opkræve det betalte beløb fra de andre enheder, som er involveret i behandlingen og er ansvarlige for krænkelsen, i forhold til deres ansvar for skaden. Disse procedurer mellem de forskellige fælles dataansvarlige og databehandlere finder sted, efter at den registrerede har modtaget erstatning, og den registrerede ikke er en del af disse.

Under Europarådets retsorden kræver artikel 12 i den moderniserede konvention 108, at kontraherende parter fastlægger passende retsmidler for overtrædelser af national lovgivning, som gennemfører konventionens krav. Den forklarende rapport til den moderniserede konvention 108 angiver, at retsmidler skal omfatte muligheden for at anfægte en beslutning eller praksis, hvor udenretslige mekanismer også skal være tilgængelige ([653]). Modaliteter og forskellige regler knyttet til adgangen til disse retsmidler samt proceduren, som følges, er overladt til hver kontraherende parts skøn. Kontraherende parter og nationale domstole bør også overveje bestemmelser om finansiel kompensation for materielle og ikke-materielle skader som følge af behandlingen samt muligheden for kollektive søgsmål ([654]).

([653]) Forklarende rapport til den moderniserede konvention 108, stk. 100.

([654]) *Ibid*.

6.2.4. Sanktioner

I Europarådets retsorden fastlægger artikel 12 i den moderniserede konvention 108, at hver kontraherende part skal indføre passende sanktioner og retsmidler for overtrædelser af bestemmelser i den nationale lovgivning, som gennemfører de grundlæggende principper om databeskyttelse, der er fastsat ved konvention 108. Konventionen fastlægger eller pålægger ikke en bestemt række sanktioner. Tværtimod angiver den tydeligt, at hver kontraherende part råder over en skønsbeføjelse til at fastlægge arten af de retslige eller udenretslige mekanismer, som kan være kriminelle, administrative eller civile. Den forklarende rapport til den moderniserede konvention 108 fastlægger, at sanktioner skal være effektive, proportionale og afskrækkende ([655]). Kontraherende parter skal overholde dette princip ved bestemmelse af arten og alvoren af de sanktioner, som er tilgængelige i deres nationale retsorden.

Under EU-retten giver artikel 83 i GDPR medlemsstaters tilsynsmyndigheder beføjelser til at pålægge administrative bøder ved overtrædelser af forordningen. Bødernes størrelse og de omstændigheder, som de nationale myndigheder tager hensyn til ved beslutning af, om en bøde skal pålægges, samt denne bødes samlede maksimale størrelse, er fastlagt i artikel 83. Sanktionsordningen er dermed harmoniseret for hele EU.

GDPR har en niveauinddelt tilgang til bøder. Tilsynsmyndighederne har beføjelser til at pålægge administrative bøder for overtrædelser af forordningen på op til 20 000 000 EUR eller, i tilfælde af en virksomhed, 4 % af dennes samlede årlige omsætning på verdensplan — alt efter hvad der er størst. Overtrædelser, som kan udløse dette bødeniveau, omfatter brud på de grundlæggende principper for behandling og betingelser for samtykke samt brud på registreredes rettigheder og forordningens bestemmelser vedrørende overførsel af personoplysninger til modtagere i tredjelande. For andre overtrædelser kan tilsynsmyndigheder pålægge bøder på op til 10 000 000 EUR eller, i tilfælde af en virksomhed, 2 % af dennes samlede årlige omsætning på verdensplan — alt efter hvad der er størst.

Tilsynsmyndigheder skal tage hensyn til en række faktorer ved bestemmelse af typen og niveauet for den bøde, som pålægges ([656]). For eksempel skal de tage særligt hensyn til overtrædelsens art, alvor og varighed, kategorierne af de berørte personoplysninger, og om den havde en forsætlig eller forsømmelig karakter. Når

([655]) *Ibid.*

([656]) Generel forordning om databeskyttelse, artikel 83, stk. 2.

en dataansvarlig eller databehandler har iværksat foranstaltninger til at mindske skaden, som forvoldes på registrerede, skal dette også tages under overvejelse. På tilsvarende vis er samarbejdsgraden med tilsynsmyndigheden efter overtrædelsen og måden, hvorpå tilsynsmyndighed lærte overtrædelsen at kende på (for eksempel om den blev rapporteret af enheden, som var ansvarlig for behandlingen, eller af en registreret, hvis rettigheder blev overtrådt), andre vigtige faktorer, som vejleder tilsynsmyndighedernes beslutning ([657]).

Udover evnen til at pålægge administrative bøder har tilsynsmyndigheder en bred række af andre korrigerende beføjelser, de kan gøre brug af. Tilsynsmyndighedernes såkaldte »korrigerende« beføjelser er fastlagt i GDPR's artikel 58. De rækker fra udstedelse af påbud, advarsler og kritik til dataansvarlige og databehandlere, til pålæggelse af midlertidige eller endda permanente forbud mod behandlingsaktiviteter.

I forbindelse med sanktionerne mod EU-institutioners eller -organers overtrædelser af EU-retten kan sanktioner være i form af disciplinære sanktioner grundet det særlige ansvarsområde for forordningen om databeskyttelse inden for EU-institutionerne. I henhold til denne forordnings artikel 49 kan der »iværksættes disciplinære sanktioner over for en tjenestemand eller en af de øvrige ansatte i De Europæiske Fællesskaber, som forsætligt eller uagtsomt undlader at opfylde de forpligtelser, der påhviler ham i henhold til denne forordning [...]«.

([657]) Artikel 29-Gruppen (2017), *Retningslinjer vedrørende anvendelse og fastsættelse af administrative bøder i overensstemmelse med forordning (EU) 2016/679*, WP 253, 3. oktober 2017.

7

Internationale data-overførsler og udvekslinger af personoplysninger

EU	Omhandlede emner	Europarådet
Overførsler af personoplysninger		
Generel forordning om databeskyttelse, artikel 44	Begreb	Den moderniserede konvention 108, artikel 14, stk. 1 og 2
Fri udveksling af personoplysninger		
Generel forordning om databeskyttelse, artikel 1, stk. 3, og betragtning 170	Mellem EU-medlemsstater	
	Mellem kontraherende parter til konvention 108	Den moderniserede konvention 108, artikel 14, stk. 1
Overførsler af personoplysninger til tredjelande eller internationale organisationer		
Generel forordning om databeskyttelse, artikel 45 EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 2015	Afgørelse om tilstrækkeligheden af beskyttelsesniveauet/ tredjelande eller internationale organisationer med tilstrækkelige beskyttelsesniveauer	Den moderniserede konvention 108, artikel 14, stk. 2
Generel forordning om databeskyttelse, artikel 46, stk. 1, og artikel 46, stk. 2	Passende garantier, inklusive rettigheder, der kan håndhæves, og retsmidler for registrerede, der leveres igennem standardkontraktbestemmelser, bindende virksomhedsregler, adfærdskodekser og certificeringsmekanismer	Den moderniserede konvention 108, artikel 14, stk. 2, 3, 5 og 6

EU	Omhandlede emner	Europarådet
Generel forordning om databeskyttelse, artikel 46, stk. 3	**Underlagt godkendelse fra den kompetente tilsynsmyndighed: kontraktbestemmelser og bestemmelser i administrative ordninger mellem offentlige myndigheder**	
Generel forordning om databeskyttelse, artikel 46, stk. 5	**Eksisterende godkendelser på baggrund af direktiv 95/46/EF**	
Generel forordning om databeskyttelse, artikel 47	**Bindende virksomhedsregler**	
Generel forordning om databeskyttelse, artikel 49	**Undtagelser i særlige situationer**	Den moderniserede konvention 108, artikel 14, stk. 4
Eksempler: PNR-aftale mellem EU og USA SWIFT-aftale mellem EU og USA	**Internationale aftaler**	Den moderniserede konvention 108, artikel 14, stk. 3, litra a)

Under EU-retten fastlægger den generelle forordning om databeskyttelse fri udveksling af personoplysninger inden for EU. Den indeholder dog specifikke krav vedrørende overførsler af personoplysninger til tredjelande uden for EU samt til internationale organisationer. Forordningen anerkender vigtigheden af sådanne overførsler, særligt med henblik på international handel og samarbejde, men anerkender også den øgede risiko for personoplysninger. Forordningen er derfor rettet mod at give personoplysninger, der overføres til tredjelande, det samme beskyttelsesniveau, som de har i EU ([658]). Europarådets retsorden anerkender også vigtigheden af at gennemføre regler for grænseoverskridende dataudveksling på baggrund af en fri udveksling mellem parter og særlige krav til overførsler til ikke-parter.

([658]) Generel forordning om databeskyttelse, betragtning 101 og 116.

7.1. Arten af overførsler af personoplysninger

Hovedpunkter

- EU-retten og Europarådets retsorden har regler for overførsler af personoplysninger til modtagere i tredjelande eller til internationale organisationer.
- Ved at sikre registreredes rettigheder, når oplysninger overføres uden for EU, kan beskyttelsen, som sikres i EU-retten, følge personoplysninger, som stammer fra EU.

Under **Europarådets retsorden** beskrives grænseoverskridende dataudvekslinger som overførsler af personoplysninger til modtagere, som er underlagt en udenlandsk jurisdiktion ([659]). Grænseoverskridende dataudvekslinger til en modtager, som ikke er underlagt en kontraherende parts jurisdiktion, tillades kun, hvis der er et tilstrækkeligt beskyttelsesniveau ([660]).

EU-retten regulerer overførsler »af personoplysninger, som underkastes behandling eller planlægges behandlet efter overførsel til et tredjeland eller en international organisation [...]« ([661]). Sådanne dataudvekslinger tillades kun, hvis de overholder reglerne fastlagt i GDPR's kapitel V.

Grænseoverskridende udvekslinger af personoplysninger tillades, hvis modtageren er underlagt jurisdiktionen for en kontraherende part eller medlemsstat under, henholdsvist, Europarådets retsorden eller EU-retten. Begge retsordener tillader også, at oplysninger overføres til et land, som ikke er en kontraherende part eller en medlemsstat, hvis bestemte betingelser er opfyldt.

([659]) Forklarende rapport til den moderniserede konvention 108, stk. 102.

([660]) Den moderniserede konvention 108, artikel 14, stk. 2.

([661]) Generel forordning om databeskyttelse, artikel 44.

7.2. Fri udveksling af personoplysninger mellem medlemsstater eller kontraherende parter

Hovedpunkter

- Udveksling af personoplysninger i EU samt udvekslinger af personoplysninger imellem kontraherende parter til den moderniserede konvention 108 skal være fri for begrænsninger. Men da ikke alle kontraherende parter til den moderniserede konvention 108 er medlemsstater i EU, er overførsler fra en EU-medlemsstat til et tredjeland, som dog er en kontraherende part til konvention 108, ikke muligt, medmindre de opfylder betingelserne i GDPR.

Under Europarådets retsorden skal der være en fri udveksling af personoplysninger mellem kontraherende parter til den moderniserede konvention 108. Overførslen kan dog forbydes, hvis der er en reel og alvorlig risiko for, at overførslen til en anden part ville føre til, at konventionens bestemmelser omgås, eller hvis en part er forpligtet til at gøre dette på grund af harmoniserede beskyttelsesregler, som deles af stater, der henhører under en regional international organisation ([662]).

Under EU-retten er indskrænkninger eller forbud mod den frie udveksling af personoplysninger mellem EU-medlemsstater ud fra grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, forbudt ([663]). Området for fri dataudveksling blev udvidet ved aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS) ([664]), som indlemmede Island, Liechtenstein og Norge i det indre marked.

Eksempel: Hvis et selskab i en international koncern, som er etableret i flere EU-medlemsstater, herunder Slovenien og Frankrig, overfører personoplysninger fra Slovenien til Frankrig, må en sådan overførsel ikke begrænses eller forbydes ved slovensk lov med henblik på at beskytte personoplysninger.

([662]) Den moderniserede konvention 108, artikel 14, stk. 1.

([663]) Generel forordning om databeskyttelse, artikel 1, stk. 3.

([664]) Rådets og Kommissionens afgørelse af 13. december 1993 om indgåelse af aftalen om Det Europæiske Økonomiske Samarbejdsområde mellem De Europæiske Fællesskaber, deres medlemsstater og Republikken Finland, Republikken Island, Fyrstendømmet Liechtenstein, Kongeriget Norge, Det Schweiziske Edsforbund, Kongeriget Sverige og Republikken Østrig, EFT L 1 af 3. januar 1994, s. 1.

Hvis det samme slovenske selskab ønsker at overføre de samme personoplysninger til moderselskabet i Malaysia, så skal den slovenske dataeksportør tage hensyn til reglerne i GDPR's kapitel V. Disse bestemmelser er beregnet til at sikre personoplysninger for registrerede, som er underlagt EU's jurisdiktion.

Under EU-retten er udvekslinger af personoplysninger mellem EØS-medlemsstater med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner underlagt direktiv (EU) 2016/680 ([665]). Dette sikrer også, at udvekslingen af personoplysninger mellem kompetente myndigheder inden for Unionen ikke begrænses eller forbydes på baggrund af databeskyttelseshensyn. Under Europarådets retsorden er behandling af alle personoplysninger (inklusive deres grænseoverskridende udveksling med andre parter til konvention 108), uden undtagelser baseret på formål eller indsatsområder, omfattet af konvention 108; dog kan de kontraherende parter fastlægge undtagelser. Alle medlemmer af EØS er også parter til konvention 108.

7.3. Overførsler af personoplysninger til tredjelande/ikke-parter eller internationale organisationer

Hovedpunkter

- Både **Europarådet** og **EU** tillader overførsler af personoplysninger til tredjelande eller internationale organisationer, hvis visse betingelser opfyldes med henblik på beskyttelse af personoplysninger.
    - **Under Europarådets retsorden** kan et tilstrækkeligt beskyttelsesniveau opnås igennem statens eller en international organisations lovgivning eller ved at fastlægge passende standarder.

([665]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA, EUT L 119 af 4. maj 2016.

- **Under EU-retten** må overførsler finde sted, hvis tredjelandet sikrer et tilstrækkeligt beskyttelsesniveau, eller hvis den dataansvarlige eller databehandleren sikrer passende garantier, inklusive håndhævelige rettigheder for registrerede og retsmidler, igennem mekanismer som standardbestemmelser om databeskyttelse eller bindende virksomhedsregler.

- **Både Europarådets retsorden og EU-retten** fastlægger undtagelsesklausuler, som tillader overførsel af personoplysninger under bestemte omstændigheder, selv når hverken et tilstrækkeligt beskyttelsesniveau eller passende garantier er på plads.

Selvom både Europarådets retsorden og EU-retten tillader dataudvekslinger til tredjelande eller til internationale organisationer, fastlægger de forskellige betingelser. Hvert sæt af betingelser tager hensyn til de forskellige organisationers struktur og formål.

Under **Europarådets retsorden** er der principielt to måder at tillade overførslen af personoplysninger til tredjelande eller til internationale organisationer. Overførsler af personoplysninger kan finde sted på baggrund af: en afgørelse om tilstrækkeligheden af beskyttelsesniveauet fra Europa-Kommissionen ([666]) eller, hvis en sådan afgørelse om tilstrækkeligheden af beskyttelsesniveauet ikke forefindes, når den dataansvarlige eller databehandleren giver passende garantier, herunder rettigheder, der kan håndhæves, og retsmidler for den registrerede ([667]). Hvis enten en sådan afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller passende garantier mangler, er der mulighed for en række undtagelser.

Under **Europarådets retsorden** tillades fri overførsel af oplysninger til dem, som ikke er parter til konventionen, kun på baggrund af:

- loven i staten eller den internationale organisation, herunder de gældende internationale traktater eller aftaler, der garanterer passende garantier

- ad hoc- eller godkendte standardgarantier, der sikres ved retligt bindende instrumenter, som kan håndhæves og er vedtaget og implementeret af personerne involveret i overførslen og den videre behandling ([668]).

Ligesom EU-retten er der ved mangel på et tilstrækkeligt databeskyttelsesniveau mulighed for en række undtagelser.

([666]) Generel forordning om databeskyttelse, artikel 45.

([667]) *Ibid.*, artikel 46.

([668]) Den moderniserede konvention 108, artikel 14, stk. 3, litra a) og b).

7.3.1. Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet

I EU-retten fastlægges den frie udveksling af personoplysninger med tredjelande, som har et tilstrækkeligt databeskyttelsesniveau, i GDPR's artikel 45. EU-Domstolen har præciseret, at begrebet »tilstrækkeligt beskyttelsesniveau« kræver, at tredjelandet sikrer et beskyttelsesniveau af grundlæggende rettigheder og frihedsrettigheder, som »i det væsentlige svarer til« garantierne sikret ved EU-lovgivningen ([669]). På samme tid må de midler, som et tredjeland anvender til at sikre et sådant beskyttelsesniveau, afvige fra dem, der benyttes inden for EU. Standarden om tilstrækkelighed kræver ikke en punktvis gentagelse af EU's regler ([670]).

Europa-Kommissionen vurderer niveauet af databeskyttelse i tredjelande ved at undersøge deres nationale lovgivning og gældende internationale forpligtelser. Der tages også hensyn til et lands deltagelse i multilaterale eller regionale systemer, navnlig vedrørende beskyttelse af personoplysninger. Hvis Europa-Kommissionen konstaterer, at tredjelandet eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau, kan den udstede en afgørelse om tilstrækkeligheden af beskyttelsesniveauet med bindende virkning ([671]). Ikke desto mindre har EU-Domstolen fastlagt, at nationale tilsynsmyndigheder stadig har beføjelser til at undersøge anmodningen fra en person vedrørende beskyttelsen af vedkommendes personoplysninger, som er overført til et tredjeland, der af Kommissionen er vurderet til at garantere et tilstrækkeligt beskyttelsesniveau, hvor denne person påstår, at gældende lovgivning og praksisser i tredjelandet ikke sikrer et tilstrækkeligt beskyttelsesniveau ([672]).

Europa-Kommissionen kan også vurdere tilstrækkeligheden af beskyttelsesniveauet i et tredjelands område eller begrænse sig til bestemte sektorer, hvilket for

([669]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015, præmis 96.

([670]) *Ibid*., præmis 74. Se også Europa-Kommissionen (2017), Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden, COM(2017) 7 final af 10. januar 2017, s. 6.

([671]) Der findes en liste, der løbende opdateres, over lande, som har fået konstateret et tilstrækkeligt beskyttelsesniveau på hjemmesiden for Europa-Kommissionen, Generaldirektorat for Retlige Anliggender.

([672]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner*, [GC] 6. oktober 2015, præmis 63 og 65– 66.

eksempel var tilfældet for Canadas lovgivning for private virksomheder ([673]). Der er også afgørelser om tilstrækkeligheden af beskyttelsesniveauet for overførsler baseret på aftaler mellem EU og tredjelande. Disse afgørelser henviser udelukkende til en enkelt form for dataoverførsel, såsom et flyselskabs overførsel af passagerlisteoplysninger (PNR) til udenlandske grænsekontrolmyndigheder, når flyselskabet flyver fra EU til visse oversøiske destinationer (se afsnit 7.3.4.).

Afgørelser om tilstrækkeligheden af beskyttelsesniveauet er underlagt løbende overvågning. Europa-Kommissionen gennemgår regelmæssigt sådanne afgørelser for at holde styr på udviklinger, som kan påvirke deres status. Hvis Europa-Kommissionen derfor konstaterer, at tredjelandet eller den internationale organisation ikke længere opfylder betingelserne, som begrunder afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, kan den ændre, suspendere eller ophæve afgørelsen. Kommissionen kan også indlede forhandlinger med det berørte tredjeland eller internationale organisation for at afhjælpe problemet, som ligger til grund for afgørelsen.

Afgørelser om tilstrækkeligheden af beskyttelsesniveauet vedtaget af Europa-Kommissionen på baggrund af direktiv 95/46/EF forbliver gældende, indtil de ændres, erstattes eller ophæves af en beslutning fra Kommissionen, som er vedtaget i henhold til reglerne i GDPR's artikel 45.

Til dato har Europa-Kommissionen anerkendt Andorra, Argentina, Canada (kommercielle organisationer, som er omfattet af lov om beskyttelse af personoplysninger og elektroniske dokumenter – PIPEDA), Færøerne, Guernsey, Isle of Man, Jersey, Israel, New Zealand, Schweiz og Uruguay for at give tilstrækkelig beskyttelse. I forbindelse med overførsler til USA har Europa-Kommissionen vedtaget en beslutning om tilstrækkeligheden af beskyttelsesniveauet i 2000, som tillod overførsler til virksomheder, der har selvcertificeret, at de ville beskytte personoplysninger overført fra EU samt overholde de såkaldte »safe harbour-principper« ([674]). EU-Domstolen

([673]) Europa-Kommissionen (2002), beslutning 2002/2/EF af 20. december 2001 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse af personoplysninger, der opnås ved hjælp af Canadas lov om beskyttelse af personoplysninger og elektroniske dokumenter (Canadian Personal Information Protection and Electronic Documents Act), EFT L 2 af 4. januar 2002.

([674]) Kommissionens beslutning 2000/520/EF af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbour-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium, EFT L 215. Beslutningen blev erklæret ugyldig af EU-Domstolen i C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC].

erklærede denne beslutning for ugyldig i 2015, og en ny beslutning om tilstrækkeligheden af beskyttelsesniveauet blev vedtaget i juli 2016, som tillod tilslutning af virksomheder fra 1. august 2016.

Eksempel: I *Schrems* ([675])-sagen havde Maximilian Schrems, en østrigsk statsborger, været en bruger af Facebook i flere år. Nogle eller alle oplysningerne, som Maximilian Schrems havde givet til Facebook, blev overført fra Facebooks irske datterselskab til servere placeret i USA, hvor de blev behandlet. Maximilian Schrems indgav en klage til den irske tilsynsmyndighed for databeskyttelse, da han på baggrund af Edward Snowdens, en amerikansk whistleblowers, afsløringer omkring amerikanske overvågningstjenesters overvågningsaktiviteter havde den holdning, at USA's love og praksisser ikke beskytter oplysninger overført til landet i tilstrækkelig grad. Den irske myndighed afviste klagen på den baggrund, at Kommissionen i sin beslutning af 26. juli 2000 vurderede, at USA under »safe harbour«-ordningen sikrer et tilstrækkeligt beskyttelsesniveau for de overførte personoplysninger. Sagen blev forelagt for den irske højesteret, som henviste den til EU-Domstolen for en præjudiciel afgørelse.

EU-Domstolen afsagde dom om, at Kommissionens beslutning om tilstrækkeligheden af safe harbour-rammerne var ugyldig. EU-Domstolen bemærkede for det første, at beslutningen gjorde det muligt at begrænse anvendelsen af safe harbour-databeskyttelsesprincipperne på baggrund af national sikkerhed, offentlige interesser, krav til retshåndhævelse eller USA's nationale lovgivning. Beslutningen tillod dermed et indgreb i de grundlæggende rettigheder for de personer, hvis personoplysninger blev eller kunne blive overført til USA ([676]). Den bemærkede endvidere, at beslutningen ikke indeholdt nogen konklusioner om tilstedeværelsen af regler i USA, som er beregnet til at begrænse sådanne indgreb, eller om tilstedeværelsen af en effektiv domstolsbeskyttelse mod sådanne indgreb ([677]). EU-Domstolen fremhævede, at det inden for Unionen sikrede beskyttelsesniveau for frihedsrettigheder og grundlæggende rettigheder krævede, at lovgivning, som indebar et indgreb i artikel 7 og 8, skal fastsætte klare og præcise regler, som regulerer rækkevidden og anvendelsen af en foranstaltning og opstiller

([675]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015.

([676]) *Ibid.*, præmis 84.

([677]) *Ibid.*, præmis 88-89.

en række mindstekrav, undtagelser fra og begrænsninger af beskyttelsen af personoplysninger ([678]). Da Kommissionens beslutning ikke fastlægger, at USA faktisk sikrer et sådant beskyttelsesniveau på baggrund af landets nationale love eller internationale forpligtelser, konkluderede EU-Domstolen, at beslutningen ikke opfyldte kravene i den gældende bestemmelse om overførsler i databeskyttelsesdirektivet og derfor var ugyldig ([679]).

USA's beskyttelsesniveau var dermed ikke noget som »i det væsentlige svarer til« de grundlæggende rettigheder og frihedsrettigheder, der sikres ved EU-retten ([680]). EU-Domstolen argumenterede, at flere artikler i Den Europæiske Unions charter om grundlæggende rettigheder var overtrådt. For det første var det væsentligste indhold af artikel 7 tilsidesat, da USA's lovgivning »gør det muligt for de offentlige myndigheder på generel vis at få adgang til indholdet af elektronisk kommunikation«. For det andet var det væsentligste indhold af artikel 47 også overtrådt, da lovgivningen ikke tildelte enkeltpersoner retsmidler vedrørende adgang til personoplysninger eller berigtigelse eller sletning af personoplysninger. Endelig var behandlingen af personoplysninger ikke længere lovlig, da safe harbour-ordningen overtrådte de ovennævnte artikler, hvilket resulterede i en overtrædelse af artikel 8.

Efter at EU-Domstolen erklærede safe harbour-ordningen for ugyldig, blev Kommissionen og USA enige om nye lovrammer: EU's og USA's værn om privatlivets fred. Den 12. juli 2016 vedtog Kommissionen en afgørelse, som erklærede, at USA sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger overført fra Unionen til organisationer i USA under værnet om privatlivets fred ([681]).

([678]) *Ibid.*, præmis 91-92.

([679]) *Ibid.*, præmis 96-97.

([680]) *Ibid.*, præmis 73-74 og 96.

([681]) Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred, EUT L 207 af 1. august 2016. Artikel 29-Gruppen glædede sig over de forbedringer, som kom med værnet om privatlivets fred sammenlignet med safe harbour-beslutningen, og roste Kommissionen og de amerikanske myndigheder for i den endelige udgave af dokumenterne om værnet om privatlivets fred at have taget hensyn til de bekymringer, som Artikel 29-Gruppen gav udtryk for i dennes udtalelse WP 238 om udkastet til beslutning om tilstrækkeligheden af beskyttelsesniveauet for EU's og USA's værn om privatlivets fred. Den fremhævede dog stadig en række udestående betænkeligheder. For flere detaljer se Artikel 29-Gruppen, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, vedtaget den 13. april 2016, 16/EN WP 238.

Ligesom safe harbour-ordningen er EU's og USA's værn om privatlivets fred rettet mod at beskytte personoplysninger, som overføres fra EU til USA til kommercielle formål ([682]). Amerikanske virksomheder kan frivilligt selvcertificere deres overholdelse af listen over deltagere i værnet om privatlivets fred ved at opfylde ordningens databeskyttelsesstandarder. De kompetente amerikanske myndigheder overvåger og bekræfter de certificerede virksomheders overholdelse af disse standarder.

Ordningen for værnet om privatlivets fred fastlægger især:

- databeskyttelsesforpligtelser for virksomheder, som modtager personoplysninger fra EU

- beskyttelse og klagemuligheder for fysiske personer, navnlig oprettelse af en ombudsmandsmekanisme, som er uafhængig fra de amerikanske efterretningstjenester og håndterer klager fra fysiske personer, som mener, at deres personoplysninger er blevet anvendt på en ulovlig måde af de amerikanske myndigheder på området for national sikkerhed

- en årlig fælles gennemgang for at overvåge ordningens implementering ([683]). Den første gennemgang fandt sted i september 2017 ([684]).

Den amerikanske regering har udfærdiget forpligtelser og forsikringer, som ledsager beslutningen om værnet om privatlivets fred. Disse fastlægger begrænsninger og garantier for den amerikanske regerings adgang til personoplysninger med henblik på retshåndhævelse og national sikkerhed.

7.3.2. Overførsler omfattet af fornødne garantier

Både **EU-retten** og **Europarådets retsorden** anerkender, at passende garantier mellem den dataansvarlige, som eksporterer oplysninger, og modtageren i tredjelandet eller den internationale organisation kan være en måde at sikre et tilstrækkeligt niveau af databeskyttelse for modtageren.

([682]) Der er flere oplysninger i faktaarket om EU's og USA's værn om privatlivets fred.

([683]) Der er flere oplysninger på Europa-Kommissionens websted om EU's og USA's værn om privatlivets fred.

([684]) Europa-Kommissionen, rapport fra Kommissionen til Europa-Parlamentet og Rådet om den første årlige evaluering af EU's og USA's værn om privatlivets fred, COM(2017) 611 final, 18. oktober 2017. Se også Artikel 29-Gruppen, *EU – U.S. Privacy Shield – First annual Joint Review*, vedtaget den 28. november 2017, 17/EN WP 255.

Under **EU-retten** tillades overførsler af personoplysninger til et tredjeland eller en international organisation, hvis den dataansvarlige eller databehandleren giver de fornødne garantier og rettigheder, som kan håndhæves, og hvis effektive retsmidler for registrerede er tilgængelige ([685]). Listen over acceptable »fornødne garantier« er udelukkende fastlagt i europæisk databeskyttelseslovgivning. Fornødne garantier kan fastlægges ved:

- et retligt bindende instrument, som kan håndhæves, mellem offentlige myndigheder eller organer
- bindende virksomhedsregler
- standardbestemmelser om databeskyttelse vedtaget af enten Europa-Kommissionen eller en tilsynsmyndighed
- adfærdskodekser
- certificeringsmekanismer ([686]).

Skræddersyede kontraktbestemmelser mellem den dataansvarlige eller databehandleren i EU og datamodtageren i et tredjeland er en anden måde at give de fornødne garantier på. Disse kontraktbestemmelser skal dog godkendes af den kompetente tilsynsmyndighed, inden de kan benyttes som et værktøj til overførsel af personoplysninger. På samme måde kan offentlige myndigheder gøre brug af databeskyttelsesbestemmelser i deres administrative ordninger, hvis tilsynsmyndigheden har godkendt disse ([687]).

Under Europarådets retsorden tillades overførsler af oplysninger til en stat eller international organisation, som ikke er part i den moderniserede konvention 108, hvis et passende beskyttelsesniveau sikres. Dette kan opnås ved:

- statens eller en international organisations lovgivning, eller
- ad hoc- eller standardgarantier, der er indbygget i et retligt bindende dokument ([688]).

([685]) Generel forordning om databeskyttelse, artikel 46.

([686]) Generel forordning om databeskyttelse, artikel 46, stk. 1, litra c) og d), og stk. 2, litra a), b), e) og f), og artikel 47.

([687]) *Ibid.*, artikel 46, stk. 3.

([688]) Den moderniserede konvention 108, artikel 14, stk. 3, litra b).

Overførsler omfattet af kontraktbestemmelser

Både **Europarådets retsorden** og **EU-retten** anerkender, at kontraktbestemmelser mellem den dataansvarlige, som eksporterer oplysninger, og modtageren i tredjelandet kan være en måde at garantere et tilstrækkeligt niveau af databeskyttelse for modtageren ([689]).

På **EU-plan** udviklede Europa-Kommissionen, med hjælp fra Artikel 29-Gruppen, standardbestemmelser om databeskyttelse, som blev officielt certificeret ved en afgørelse fra Kommissionen som bevis på tilstrækkelig databeskyttelse ([690]). Da Kommissionens afgørelser er bindende i deres helhed i medlemsstaterne, skal de nationale myndigheder, som overvåger dataoverførsler, anerkende disse standardkontraktbestemmelser i deres procedurer ([691]). Hvis den dataansvarlige, som eksporterer oplysninger, og modtageren i tredjelandet indgår en aftale og underskriver disse bestemmelser, burde det give tilsynsmyndigheden tilstrækkelig dokumentation for, at tilstrækkelige garantier er på plads. I *Schrems*-sagen fastholdt EU-Domstolen dog, at Europa-Kommissionen ikke har kompetencen til at begrænse beføjelserne for de nationale tilsynsmyndigheder til at overvåge overførslen af personoplysninger til et tredjeland, som har været genstand for en afgørelse om tilstrækkeligheden af beskyttelsesniveauet fra Kommissionen ([692]). De nationale tilsynsmyndigheder forhindres dermed ikke i at udøve deres beføjelser, inklusive beføjelsen til at suspendere eller forbyde en overførsel af personoplysninger, når overførslen udføres i strid med europæisk eller national databeskyttelseslovgivning, såsom når dataimportøren ikke overholder standardkontraktbestemmelser ([693]).

Tilstedeværelsen af standardbestemmelser om databeskyttelse i EU's lovrammer forhindrer ikke dataansvarlige i at udarbejde andre ad hoc- og individuelle kontraktbestemmelser, så længe tilsynsmyndigheden har godkendt disse

([689]) Generel forordning om databeskyttelse, artikel 46, stk. 3, og den moderniserede konvention 108, artikel 14, stk. 3, litra b).

([690]) *Ibid*., artikel 46, stk. 2, litra b), og artikel 46, stk. 5.

([691]) *Ibid*., artikel 46, stk. 2, litra c), og traktaten om Den Europæiske Unions funktionsmåde, artikel 288.

([692]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner*, [GC] 6. oktober 2015, præmis 96-98 og 102-105.

([693]) For at tage hensyn til EU-Domstolens holdning i *Schrems*-sagen ændrede Kommissionen sin afgørelse om standardkontraktbestemmelser. Kommissionens gennemførelsesafgørelse (EU) 2016/2297 af 16. december 2016 om ændring af beslutning 2001/497/EF og afgørelse 2010/87/EU om standardkontraktbestemmelser for videregivelse af personoplysninger til tredjelande og registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF, EUT L 344 af 17. december 2016.

bestemmelser ([694]). De ville dog være nødt til at sikre det samme beskyttelsesniveau, som sikres ved standardkontraktbestemmelserne. Tilsynsmyndigheder skal ved godkendelse af ad hoc-bestemmelser anvende sammenhængsmekanismen, så en ensartet lovgivningsmæssig tilgang i EU sikres ([695]). Dette betyder, at den kompetente tilsynsmyndighed skal meddele sit udkast til afgørelse om bestemmelserne til EDPB. EDPB vil udstede en udtalelse herom, og tilsynsmyndigheden skal tage særligt hensyn til denne udtalelse, når den gennemfører sin afgørelse. Hvis den ikke har tænkt sig at følge EDPB's udtalelse, aktiveres mekanismen til bilæggelse af tvister inden for EDPB, og Databeskyttelsesrådet vedtager en bindende afgørelse ([696]).

De vigtigste elementer i en standardkontraktbestemmelse er:

- en bestemmelse om tredjepartsløfte, som giver registrerede mulighed for at udøve kontraktlige rettigheder, selvom de ikke er part i kontrakten

- at modtageren eller importøren af data er enige i at være underlagt den nationale tilsynsmyndighed og/eller de nationale domstole for den dataeksporterende dataansvarlige i tilfælde af en tvist.

Der er nu to tilgængelige sæt af standardbestemmelser for overførsler mellem dataansvarlige, som den dataeksporterende dataansvarlige kan vælge imellem ([697]). Ved overførsler fra en dataansvarlig til en databehandler er der kun et sæt af standardkontraktbestemmelser ([698]). Disse standardkontraktbestemmelser er dog i øjeblikket genstand for retslige procedurer.

([694]) Generel forordning om databeskyttelse, artikel 46, stk. 3, litra a).

([695]) *Ibid.*, artikel 63 og 64, stk. 1, litra e).

([696]) *Ibid.*, artikel 64 og 65.

([697]) Sæt I er indeholdt i bilaget til Europa-Kommissionen (2001), Kommissionens beslutning af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF, EFT L 181 af 4. juli 2001. Sæt II er indeholdt i bilaget til Europa-Kommissionen (2004), Kommissionens beslutning af 27. december 2004 om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontrakt om overførsel af personoplysninger til tredjelande, EUT L 385 af 29. december 2004.

([698]) Europa-Kommissionen (2010), Kommissionens afgørelse 2010/87 af 5. februar 2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF, EUT L 39 af 12. februar 2010. På tidspunktet for håndbogens udarbejdelse var brugen af standardkontraktbestemmelser som et grundlag for overførsel af personoplysninger til USA under retslig behandling ved den irske højesteret High Court.

Eksempel: Efter EU-Domstolen erklærede safe harbour-beslutningen for ugyldig, kunne overførsler af personoplysninger til USA ikke længere baseres på den afgørelse om tilstrækkeligheden af beskyttelsesniveauet ([699]). Da forhandlinger med de amerikanske myndigheder var igangværende og inden vedtagelsen af en ny afgørelse om tilstrækkeligheden af beskyttelsesniveauet (som endelig blev vedtaget den 12. juli 2016) ([700]), kunne overførsler kun udføres under andre lovgrundlag, såsom standardkontraktbestemmelser eller bindende virksomhedsregler. Flere virksomheder, herunder Facebook Ireland (som sagen, der førte til ugyldighedserklæringen af safe harbour-beslutningen, blev anlagt imod), skiftede til standardkontraktbestemmelser for at fortsætte deres overførsler af oplysninger imellem EU og USA.

Maximillian Schrems indsendte en klage til den irske tilsynsmyndighed, hvor han anmodede denne om at suspendere dataoverførsler til USA på baggrund af standardkontraktbestemmelser. Overordnet påstod han, at der ikke var nogen garanti for, at hans personoplysninger ville være beskyttet, når de blev overført fra Facebooks irske datterselskab til Facebook Inc. og til servere, som befinder sig i USA. Facebook Inc. er bundet af amerikanske love, som forpligter virksomheden til at udlevere personoplysninger til amerikanske retshåndhævende myndigheder, og europæiske enkeltpersoner har ingen retsmidler til at bestride denne praksis ([701]). Af disse årsager konkluderede EU-Domstolen, at safe harbour-beslutningen var ugyldig, og selvom Domstolens dom var begrænset til at undersøge denne beslutning, mente sagsøgeren, at de fremhævede problemstillinger er ligeså relevante, når overførslen er baseret på kontraktbestemmelser. I skrivende stund behandles sagen ved den irske højesteret. Sagsøgeren har tilsyneladende tænkt sig at fremlægge sagen for EU-Domstolen, hvor hans mål er at anfægte gyldigheden af Europa-Kommissionens afgørelse om standardkontraktbestemmelser. Som beskrevet i kapitel 5 er det kun EU-Domstolen, som har beføjelser til at erklære et EU-instrument for ugyldigt.

([699]) EU-Domstolen, C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015.

([700]) Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred, EUT L 207 af 1. august 2016.

([701]) Der findes flere oplysninger i den reviderede klage mod Facebook Ireland Ltd, som blev indsendt til den irske tilsynsførende for databeskyttelse af Maximilian Schrems den 1. december 2015.

Overførsler omfattet af bindende virksomhedsregler

EU-retten tillader også overførsler af personoplysninger på baggrund af bindende virksomhedsregler for internationale overførsler, som finder sted inden for samme koncern eller gruppe af foretagender, der er del af en fælles økonomisk aktivitet ([702]). Inden bindende virksomhedsregler kan benyttes som et værktøj til overførsel af personoplysninger, skal den kompetente tilsynsmyndighed godkende disse i medfør af bindende virksomhedsregler, hvor denne gør brug af sammenhængsmekanismen.

Bindende virksomhedsregler skal, for at de kan godkendes, være juridisk bindende, omfatte alle vigtige databeskyttelsesprincipper og gælde for – og håndhæves af – alle gruppens medlemmer. De skal udtrykkeligt tillægge registrerede rettigheder, som kan håndhæves, omfatte alle vigtige databeskyttelsesprincipper og overholde visse formelle krav, såsom fastlæggelse af virksomhedens struktur, hvor overførsler, og hvordan databeskyttelsesprincipper vil blive benyttet, beskrives. Dette omfatter levering af sådanne informationer til registrerede. Bindende virksomhedsregler skal blandt andet angive registreredes rettigheder og bestemmelser om ansvar ved brud på reglerne ([703]). Ved godkendelse af bindende virksomhedsregler aktiveres sammenhængsmekanismen for samarbejdet mellem tilsynsmyndighederne (beskrevet i kapitel 5).

Inden for rammerne af sammenhængsmekanismen gennemgår den ledende tilsynsmyndighed de foreslåede bindende virksomhedsregler, vedtager et udkast til afgørelse og meddeler det til EDPB. Databeskyttelsesrådet udsteder en udtalelse herom, og den ledende tilsynsmyndighed kan formelt godkende de bindende virksomhedsregler, mens denne tager »særligt hensyn« til Databeskyttelsesrådets udtalelse. Denne udtalelse er ikke juridisk bindende, men hvis tilsynsmyndigheden planlægger at se bort fra udtalelsen, så aktiveres mekanismen til bilæggelse af tvister, og Databeskyttelsesrådet vil blive anmodet om at vedtage en juridisk bindende afgørelse ved et to tredjedeles flertal blandt dets medlemmer ([704]).

Under **Europarådets retsorden** omfatter ad hoc- eller standardgarantier, der er indbygget i et retligt bindende dokument ([705]), også bindende virksomhedsregler.

([702]) Generel forordning om databeskyttelse, artikel 47.

([703]) Se generel forordning om databeskyttelse, artikel 47, for en mere detaljeret beskrivelse.

([704]) *Ibid.*, artikel 57, stk. 1, litra s), artikel 58, stk. 1, litra j), artikel 64, stk. 1, litra f), artikel 65, stk. 1 og 2.

([705]) Den moderniserede konvention 108, artikel 14, stk. 3, litra b).

7.3.3. Undtagelser i særlige situationer

Under EU-retten kan overførsler af personoplysninger til et tredjeland begrundes, selv hvis en afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller garantier mangler, såsom standardkontraktbestemmelser eller bindende virksomhedsregler, under en af følgende omstændigheder:

- Den registrerede giver udtrykkeligt samtykke til dataoverførslen.
- Den registrerede indgår – eller gør klar til at indgå – en kontrakt, hvor overførsel af oplysninger til udlandet er nødvendig.
- Indgåelsen af en kontrakt mellem en dataansvarlig og en tredjepart med henblik på den registreredes interesser.
- Ud fra vigtige hensyn i offentlighedens interesse.
- Til at fastlægge, forsvare eller gøre retskrav gældende.
- Til at beskytte den registreredes vitale interesser.
- Til overførsel af oplysninger fra offentlige registre. Dette er et eksempel på, at den brede offentlighed har en vigtig interesse i at tilgå oplysninger lagret i offentlige registre ([706]).

Når ingen af disse betingelser finder anvendelse, og når overførslerne ikke kan baseres på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller fornødne garantier, må en overførsel kun finde sted, når den ikke gentages, vedrører et begrænset antal registrerede og er nødvendig på baggrund af den dataansvarliges vægtige legitime interesser, medmindre den registreredes rettigheder vejer tungere end disse ([707]). I disse tilfælde skal den dataansvarlige vurdere omstændighederne for overførslen og give garantier. Den skal også oplyse tilsynsmyndigheden og de påvirkede registrerede om både overførslen og den legitime interesse, som begrunder denne.

([706]) Generel forordning om databeskyttelse, artikel 49.

([707]) *Ibid*.

Det faktum, at undtagelser er en sidste udvej for lovlige overførsler ([708]) (de benyttes kun, hvis en afgørelse om tilstrækkeligheden af beskyttelsesniveauet mangler, og hvis ingen andre garantier er på plads), understreger deres ekstraordinære karakter og fremhæves yderligere i GDPR's betragtninger ([709]). Undtagelser accepteres derfor som en mulighed for overførsler »under visse omstændigheder« på baggrund af samtykke, og »hvor overførsel er lejlighedsvis og nødvendig i forbindelse med en kontrakt eller et retskrav« ([710]).

Derudover skal påberåbelse af undtagelser i særlige situationer, i medfør af vejledning fra Artikel 29-Gruppen, finde sted ekstraordinært, baseret på enkelte sager og må ikke benyttes til massive eller gentagne overførsler ([711]). Den Europæiske Tilsynsførende for Databeskyttelse understregede også den ekstraordinære karakter af undtagelser som et retsgrundlag for overførsler under forordning (EF) nr. 45/2001, hvor denne bemærkede, at denne løsning bør benyttes i begrænsede tilfælde og til lejlighedsvise overførsler ([712]).

Eksempel: En virksomhed, som leverer globale distributionssystemer (GDS), med hovedkvarter i USA forsyner et online reservationssystem til flere flyselskaber, hoteller og krydstogter over hele verden, hvor oplysninger om millionvis af personer i EU behandles. GDS-virksomheden gør brug af en undtagelse som retsgrundlaget for den indledende overførsel af oplysninger til deres servere i USA, nemlig kravet om indgåelse af en kontrakt. Den fremlægger dermed ingen andre garantier for de personoplysninger, som oprinder i Europa, overføres til USA og derefter sendes ud til hoteller over hele verden (hvilket betyder, at der heller ikke er nogen garantier for videreoverførsler). GDS-virksomheden overholder ikke GDPR's krav til lovlige internationale dataoverførsler, da den gør brug af en undtagelse som retsgrundlag for massive overførsler.

Medmindre en afgørelse om tilstrækkeligheden af beskyttelsesniveauet er på plads, er EU eller dens medlemsstater bemyndiget til at fastlægge begrænsninger for

([708]) *Ibid.*, artikel 49, stk. 1.

([709]) Se generel forordning om databeskyttelse, artikel 49, stk. 1, litra a), b) og e), og betragtning 113.

([710]) *Ibid.*, artikel 49, stk. 1.

([711]) Artikel 29-Gruppen (2005), *Arbejdsdokument om en ensartet fortolkning af artikel 26, stk. 1, i direktiv 95/46/EF af 24. oktober 1995*, WP 114, Bruxelles, 25. november 2005.

([712]) Den Europæiske Tilsynsførende for Databeskyttelse, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, holdningspapir, Bruxelles, 14. juli 2014, s. 15.

overførsel af særlige kategorier af personoplysninger til et tredjeland, på trods af at andre betingelser for sådanne overførsler opfyldes, ud fra vigtige hensyn i offentlighedens interesse. Disse begrænsninger bør betragtes som ekstraordinære, og medlemsstater skal meddele de relevante bestemmelser til Kommissionen ([713]).

Europarådets retsorden tillader overførsler af oplysninger til områder, som ikke har passende databeskyttelse, i tilfælde, hvor:

- den registrerede har givet samtykke
- den registreredes interesser kræver en sådan overførsel
- loven har fastsat tungtvejende legitime interesser, navnlig vigtige offentlige interesser
- det udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund ([714]).

7.3.4. Overførsler baseret på internationale aftaler

EU kan indgå internationale aftaler med tredjelande, som regulerer overførslen af personoplysninger til bestemte formål. Disse aftaler skal indeholde passende garantier til at sikre beskyttelsen af personoplysningerne for de pågældende enkeltpersoner. GDPR berører ikke disse internationale aftaler ([715]).

Medlemsstater kan også indgå internationale aftaler med tredjelande eller internationale organisationer, som giver et passende beskyttelsesniveau af enkeltpersoners grundlæggende rettigheder og frihedsrettigheder, såfremt disse aftaler ikke påvirker anvendelsen af GDPR.

En lignende regel er givet i artikel 12, stk. 3, litra a), i den moderniserede konvention 108.

Eksempler på internationale aftaler, som omfatter overførsel af personoplysninger, er aftaler om passagerlisteoplysninger (PNR).

([713]) Se generel forordning om databeskyttelse, artikel 49, stk. 5.

([714]) Den moderniserede konvention 108, artikel 14, stk. 4.

([715]) Generel forordning om databeskyttelse, betragtning 102.

Passagerlisteoplysninger (PNR)

PNR-oplysninger indsamles af flyselskaber under reservationsproceduren og omfatter, bl.a., flypassagerernes navne, adresser, kreditkortoplysninger og flysæder. Flyselskaber indsamler også disse oplysninger til deres egne kommercielle formål. EU har indgået aftaler med bestemte tredjelande (Australien, Canada og USA) for overførslen af PNR-oplysninger for at forebygge, opdage, efterforske og retsforfølge terrorhandlinger eller grov kriminalitet på tværs af grænserne. Derudover vedtog Unionen direktiv (EU) 2016/861 – der er kendt som EU-direktivet om PNR-oplysninger – i 2016 ([716]). Dette direktiv fastlægger en lovramme for, at EU-medlemsstater kan overføre PNR-oplysninger til kompetente myndigheder i andre tredjelande for på tilsvarende vis at forebygge, opdage, efterforske eller retsforfølge terrorhandlinger og grov kriminalitet. Overførsler af PNR-oplysninger til myndigheder i tredjelande foregår ud fra et individuelt grundlag og er underlagt en individuel vurdering af, om overførslen er nødvendig til formålene angivet i direktivet og grundlæggende rettigheder overholdes.

I forbindelse med PNR-aftaler mellem EU og tredjelande er deres forenelighed med de grundlæggende rettigheder til privatlivets fred og databeskyttelse fastlagt i Den Europæiske Unions charter om grundlæggende rettigheder blevet anfægtet. Da EU – efter forhandlinger med Canada – underskrev en aftale om overførsel og behandling af PNR-oplysninger i 2014, besluttede Europa-Parlamentet at henvise sagen til EU-Domstolen for at vurdere aftalens lovlighed under EU-retten, og navnlig artikel 7 og 8 i chartret.

Eksempel: I sin udtalelse om lovligheden af PNR-aftalen mellem EU og Canada ([717]) fastholdt EU-Domstolen, at den planlagte aftale i sin nuværende form ikke var forenelig med de grundlæggende rettigheder anerkendt i chartret og derfor ikke kunne indgås. Aftalen overtrådte retten til beskyttelse af personoplysninger, som er sikret under chartrets artikel 8, da den involverede behandling af personoplysninger. På samme tid repræsenterer den også en begrænsning af retten til respekt for privatlivets fred, som er sikret i artikel 7, da PNR-oplysninger i stort omfang kan

([716]) Europa-Parlamentets og Rådets direktiv (EU) 2016/681 af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (EUT L 119 af 4.5.2016).

([717]) EU-Domstolen, *domstolens udtalelse 1/15 (Store Afdeling)*, 26. juli 2017.

samles og analyseres på en måde, som afslører rejsevaner, forhold mellem forskellige enkeltpersoner og oplysninger om deres økonomiske situation, kostvaner og sundhedstilstand, hvilket dermed krænker deres privatliv.

Indgrebet i de grundlæggende rettigheder, som den planlagte aftale medførte, forfulgte et mål af almen interesse, navnlig offentlig sikkerhed og bekæmpelse af terrorisme og grov kriminalitet på tværs af grænserne. EU-Domstolen gentog dog, at et indgreb, for at det kan være begrundet, skal begrænses til det strengt nødvendige for at opnå det forfulgte mål. Efter en analyse af den planlagte aftales bestemmelser konkluderede EU-Domstolen, at den ikke opfyldte kriteriet om at være »strengt nødvendigt«. EU-Domstolen overvejede bl.a. følgende faktorer under udarbejdelsen af sin konklusion:

- Det faktum, at den planlagte aftale indebar overførsel af følsomme oplysninger. PNR-oplysningerne indsamlet i medfør af den planlagte aftale kunne omfatte følsomme oplysninger, såsom oplysninger, der afslører en passagers racemæssige eller etniske oprindelse, religiøse overbevisning eller sundhedstilstand. De canadiske myndigheders overførsel og behandling af følsomme oplysninger kunne udgøre en risiko for princippet om forbud mod forskelsbehandling og kræver derfor en nøjagtig og solid begrundelse, som ikke er offentlig sikkerhed og bekæmpelse af grov kriminalitet. Den planlagte aftale indeholdt ikke en sådan begrundelse ([718]).

- Den fortsatte opbevaring af PNR-oplysninger for alle passagerer i en periode på fem år, selv efter passagererne har forladt Canada, blev også anset for at overskride grænserne for streng nødvendighed. EU-Domstolen mente, at det ville være tilladt for de canadiske myndigheder at lagre oplysninger over passagerer, som objektiv dokumentation antyder kan udgøre en risiko mod den offentlige sikkerhed, selv efter disse personer har forladt Canada. I modsætning hertil er der intet grundlag for at opbevare personoplysninger for *alle* passagerer, for hvem der ikke engang er indirekte beviser for, at de udgør en risiko mod den offentlige sikkerhed ([719]).

([718]) *Ibid.*, præmis 165.

([719]) *Ibid.*, præmis 204-207.

Det rådgivende udvalg for konvention 108 har afgivet en udtalelse om PNR-aftalers konsekvenser for databeskyttelse under Europarådets retsorden ([720]).

Meddelelsesdata

Det i Belgien baserede Society for Worldwide Interbank Financial Telecommunication (SWIFT), som behandler de fleste globale pengeoverførsler fra europæiske banker og har et »spejlings«-center i USA, modtog en anmodning om at videregive oplysninger til det amerikanske finansministerium med henblik på efterforskning af terrorisme under dets program til sporing af finansiering af terrorisme ([721]).

EU fandt, at der ikke var tilstrækkeligt retsgrundlag til at videregive disse overvejende europæiske oplysninger, som kun var tilgængelige i USA, fordi ét af SWIFT's databehandlingscentre var beliggende i USA.

En særlig aftale mellem EU og USA, kendt som SWIFT-aftalen, blev indgået i 2010 for at tilvejebringe det nødvendige retsgrundlag og sikre tilstrækkelige databeskyttelsesstandarder ([722]).

Under denne aftale bliver finansielle oplysninger, som lagres af SWIFT, fortsat videregivet til det amerikanske finansministerium med henblik på at forebygge, efterforske, afsløre eller retsforfølge terrorisme eller finansiering af terrorisme. Det amerikanske finansministerium kan anmode om finansielle oplysninger fra SWIFT, hvis anmodningen:

- så tydeligt som muligt identificerer de finansielle data
- klart begrunder nødvendigheden af de finansielle data

([720]) Europarådet, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19. august 2016.

([721]) Se i denne sammenhæng, Artikel 29-Gruppen 2011, *Udtalelse 14/2011 om databeskyttelsesproblemer i forbindelse med forebyggelse af hvidvaskning af penge og finansiering af terrorisme*, WP 186, Bruxelles, 13. juni 2011; Artikel 29-Gruppen (2006), *Udtalelse 10/2006 om behandling af personoplysninger i Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Bruxelles, 22. november 2006; Belgiens kommission for beskyttelse af privatlivets fred (*Commission de la protection de la vie privée*) (2008), »*Control and recommendation procedure initiated with respect to the company SWIFT scrl*«, afgørelse, 9. december 2008.

([722]) Rådets afgørelse 2010/412/EU af 13. juli 2010 om indgåelse af aftalen mellem Den Europæiske Union og Amerikas Forenede Stater om behandling og overførsel af finansielle betalingsdata fra Den Europæiske Union til USA til brug for programmet til sporing af finansiering af terrorisme, EUT L 195 af 27. juli 2010, s. 3 og 4. Aftalens tekst er vedhæftet som bilag til denne afgørelse, EUT L 195, s. 5-14.

- i så høj grad som muligt er skræddersyet, så den omhandlede mængde af data er så lille som muligt

- ikke omhandler data vedrørende det fælles eurobetalingsområde (SEPA) ([723]).

Europol skal have en kopi af hver anmodning fra det amerikanske finansministerium og skal kontrollere, om principperne i SWIFT-aftalen overholdes ([724]). Hvis det bekræftes, at de overholdes, skal SWIFT videregive de finansielle data direkte til det amerikanske finansministerium. Finansministeriet skal opbevare de finansielle data i et sikkert fysisk miljø, hvor kun personer, der efterforsker terrorisme eller finansiering heraf, kan få adgang til dem, og de finansielle data må ikke være forbundet med en anden database. Generelt skal de finansielle data, ministeriet modtager fra SWIFT, slettes senest fem år efter modtagelsen. Finansielle data, som er relevante for specifikke undersøgelser eller retssager, kan opbevares så længe, det er nødvendigt for disse undersøgelser eller retssager.

Det amerikanske finansministerium kan overføre information fra de data, der er modtaget fra SWIFT, til specifikke håndhævelses-, sikkerheds- eller antiterrormyndigheder i eller uden for USA alene med henblik på at efterforske, afsløre, forebygge eller retsforfølge terrorisme og finansiering heraf. Når overførslen af finansielle data involverer en borger eller person med bopæl i en EU-medlemsstat, skal udvekslingen af oplysninger med myndigheder i et tredjeland på forhånd godkendes af de kompetente myndigheder i den pågældende medlemsstat. Undtagelser kan gøre sig gældende, hvis udvekslingen af oplysninger er nødvendig for at forebygge en umiddelbar og alvorlig trussel mod den offentlige sikkerhed.

Uafhængige tilsynsmyndigheder, herunder en person udpeget af Europa-Kommissionen, overvåger overholdelsen af principperne i SWIFT-aftalen. De har i realtid og med tilbagevirkende kraft mulighed for at gennemgå alle søgninger i de leverede oplysninger, anmode om en yderligere begrundelse for forbindelsen med terrorisme, og myndigheden kan stille spørgsmålstegn ved alle søgninger, som kan være i strid med beskyttelsesforanstaltningerne fastlagt i aftalen.

Registrerede har ret til fra den kompetente EU-databeskyttelsesmyndighed at få bekræftet, at deres ret til beskyttelse af personoplysninger er blevet

([723]) *Ibid.*, artikel 4, stk. 2.

([724]) Den fælles kontrolinstans for Europol har gennemført audit vedrørende Europols aktiviteter på dette område.

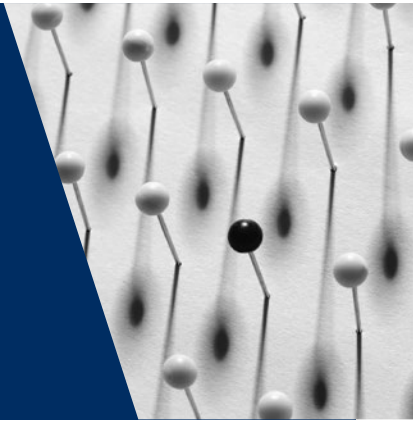
respekteret. Registrerede har også ret til at få deres data, som det amerikanske finansministerium har indsamlet og lagret i medfør af SWIFT-aftalen, berigtiget, slettet eller blokeret. Registreredes ret til indsigt er dog med forbehold for visse juridiske begrænsninger. Hvis indsigt afvises, skal den registrerede underrettes om afvisningen skriftligt og have oplysninger om administrativ klageadgang og adgang til domstolsprøvelse i USA.

SWIFT-aftalen er gyldig i fem år, og dens første gyldighedsperiode varede indtil august 2015. Aftalen forlænges automatisk med efterfølgende perioder på et år, medmindre den ene af parterne skriftligt meddeler den anden part senest seks måneder før om, at den pågældende part ønsker at opsige aftalen. Den automatiske forlængelse blev benyttet i august 2015, 2016 og 2017 og sikrer, at SWIFT-aftalen er gyldig indtil mindst august 2018 ([725]).

([725]) *Ibid.*, artikel 23, stk. 2.

8

Databeskyttelse i forbindelse med politi og strafferetten



EU	Omhandlede emner	Europarådet
Databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder	**Generelt**	Den moderniserede konvention 108
	Politi	Henstilling om politiets brug af personoplysninger Practical Guide on the use of personal data in the police sector
	Overvågning	EMD, *B.B. mod Frankrig*, nr. 5335/06, 2009 EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 2008 EMD, *Allan mod Det Forenede Kongerige*, nr. 48539/99, 2002 EMD, *Malone mod Det Forenede Kongerige*, nr. 8691/79, 1984 EMD, *Klass m.fl. mod Tyskland*, nr. 5029/71, 1978 EMD, *Szabo og Vissy mod Ungarn*, nr. 37138/14, 2016 EMD, *Vetter mod Frankrig*, nr. 59842/00, 2005
	Cyberkriminalitet	Konventionen om cyberkriminalitet

EU	Omhandlede emner	Europarådet
Andre specifikke retlige instrumenter		
Prümafgørelsen	**Vedrørende særlige data: fingeraftryk, DNA, hooliganisme, oplysninger om luftpassagerer, telekommunikations-oplysninger osv.**	Den moderniserede konvention 108, artikel 6 Henstilling om politiets brug af personoplysninger, Practical Guide on the use of personal data in the police sector
Det svenske initiativ (Rådets rammeafgørelse 2006/960/RIA)	**Forenkling af udvekslingen af oplysninger og efterretninger mellem retshåndhævende myndigheder**	EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 2008
Direktiv (EU) 2016/681 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 2014 EU-Domstolen, forenede sager C-203/15 og C-698/15, *Tele2 Sverige* og *Home Department mod Tom Watson m.fl.* [GC], 2016	**Opbevaring af personoplysninger**	EMD, *B.B. mod Frankrig*, nr. 5335/06, 2009
Europolforordningen Eurojust-afgørelsen	**Af særlige agenturer**	Henstilling om politiets brug af personoplysninger
Schengen II-afgørelsen VIS-forordningen Eurodacforordningen CIS-afgørelsen	**Af særlige fælles informationssystemer**	Henstilling om politiets brug af personoplysninger EMD, *Dalea mod Frankrig*, nr. 964/07, 2010

For at sikre balance mellem den enkeltes interesse i databeskyttelse og samfundets interesse i dataindsamling med henblik på at bekæmpe kriminalitet og garantere den nationale og offentlige sikkerhed har Europarådet og EU vedtaget specifikke

retlige instrumenter. Dette afsnit giver et overblik over Europarådets retsorden (afsnit 8.1.) og EU-retten (afsnit 8.2.) vedrørende databeskyttelse i forbindelse med politi og strafferetlige sager.

8.1. Europarådets retsorden vedrørende databeskyttelse og national sikkerhed, politi og strafferetlige sager

Hovedpunkter

- Den moderniserede konvention 108 og Europarådets henstilling om politiets brug af personoplysninger omhandler databeskyttelse i forbindelse med alt politiarbejde.
- Konventionen om cyberkriminalitet (Budapestkonventionen) er et bindende internationalt retligt instrument, som omhandler kriminalitet, der begås mod og ved hjælp af elektroniske netværk. Den er også relevant for efterforskning af kriminalitet, som ikke er cyberkriminalitet, men omfatter elektronisk bevismateriale.

En vigtig forskel mellem Europarådets retsorden og EU-retten er, at **Europarådets retsorden** også er gældende på det nationale sikkerhedsområde, hvilket EU-retten ikke er. Dette betyder, at kontraherende parter skal holde sig inden for rammerne af artikel 8 i EMRK, selv ved aktiviteter vedrørende national sikkerhed. Flere domme ved EMD har omhandlet statslige aktiviteter inden for de følsomme områder med lovgivning og praksis for national sikkerhed ([726]).

Vedrørende politi og strafferetten på europæisk plan dækker den moderniserede konvention 108 alle områder af behandlingen af personoplysninger, og dens bestemmelser har til formål at regulere behandlingen af personoplysninger generelt. Konvention 108 gælder derfor for databeskyttelse i forbindelse med politiets og strafferettens arbejde. Behandling af genetiske data, personoplysninger vedrørende lovovertrædelser, straffesager og -domme og alle relaterede sikkerhedsforanstaltninger, biometriske oplysninger, som identificerer én bestemt fysisk person, samt alle følsomme personoplysninger er kun tilladt, når fornødne garantier er tilstede mod de risici, som behandlingen af sådanne oplysninger

([726]) Se for eksempel: EMD, *Klass m.fl. mod Tyskland*, nr. 5029/71, 6. september 1978; EMD, *Rotaru mod Rumænien* [GC], nr. 28341/95, 4. maj 2000 og EMD, *Szabó og Vissy mod Ungarn*, nr. 37138/14, 12. januar 2016.

kan udgøre for den registreredes interesser, rettigheder og grundlæggende frihedsrettigheder, navnlig risikoen for diskrimination ([727]).

Politiets og strafferetlige myndigheders opgaver kræver ofte behandling af personoplysninger, som kan have alvorlige følger for de involverede personer. Henstillingen om politiets brug af personoplysninger, som Europarådet vedtog i 1987, giver Europarådets medlemsstater en rettesnor for, hvordan de bør gennemføre principperne i konvention 108 i forbindelse med politiets behandling af personoplysninger ([728]). Henstillingen blev suppleret af en praktisk vejledning i politiets brug af personoplysninger, som blev vedtaget af det rådgivende udvalg for konvention 108 ([729]).

Eksempel: I sagen *D.L. mod Bulgarien* ([730]) anbragte sociale myndigheder sagsøgeren i en lukket uddannelsesinstitution i medfør af en retskendelse. Alle skriftlige korrespondancer og telefonopkald blev overvåget af institutionen i omfattende og vilkårlig grad. EMD fastholdt, at artikel 8 var blevet overtrådt, da den pågældende foranstaltning ikke var nødvendig i et demokratisk samfund. Domstolen fastlagde, at man så vidt muligt skulle sørge for, at mindreårige anbragt i en institution havde tilstrækkelig kontakt med omverden, da dette var en integreret del af deres ret til en værdig behandling og var af altafgørende betydning for deres reintegration i samfundet. Dette var både gældende for besøg og skriftlig korrespondance eller telefonopkald. Derudover skelnede overvågningen ikke mellem kommunikation med familiemedlemmer og ikke-statslige organisationer, som repræsenterer børns rettigheder, eller advokater. Desuden var beslutningen om at opfange kommunikationen ikke baseret på en individuel risikoanalyse i den enkelte sag.

Eksempel: I *Dragojević mod Kroatien* ([731]), var sagsøgeren mistænkt for at være indblandet i narkotikahandel. Han blev dømt skyldig, efter at undersøgelsesdommeren godkendte brugen af hemmelige overvågningsforanstaltninger til at aflytte sagsøgerens telefonopkald. EMD fastholdt, at

([727]) Den moderniserede konvention 108, artikel 6.

([728]) Europarådet, Ministerkomité (1987), Henstilling Rec(87)15 til medlemsstaterne om politiets brug af personoplysninger, 17. september 1987.

([729]) Europarådet (2018), det rådgivende udvalg for konvention 108, Practical Guide on the use of personal data in the police sector, T-PD(2018)1.

([730]) EMD, *D.L. mod Bulgarien*, nr. 7472/14, 19. maj 2016.

([731]) EMD, *Dragojević mod Kroatien*, nr. 68955/11, 15. januar 2015.

foranstaltningen, som var genstand for klagen, udgjorde et indgreb i retten til respekt for privatlivets fred og korrespondance. Godkendelsen givet af undersøgelsesdommeren var udelukkende baseret på anklagemyndighedens udtalelse om, at undersøgelsen ikke kunne udføres på andre måder. EMD bemærkede også, at straffedomstolene havde begrænset deres vurdering vedrørende brugen af overvågningsforanstaltninger, og at regeringen ikke fremlagde de tilgængelige midler. Artikel 8 var derfor blevet overtrådt.

8.1.1. Henstillingen om politiets brug af personoplysninger

EMD har konsekvent fastholdt, at politiets eller nationale sikkerhedsmyndigheders opbevaring og lagring af personoplysninger udgør et indgreb i artikel 8, stk. 1, i EMRK. Mange af EMD's domme omhandler begrundelsen bag et sådant indgreb ([732]).

Eksempel: I *B.B. mod Frankrig* ([733]) var sagsøgeren blevet dømt for at have begået seksuelle overgreb mod 15-årige mindreårige, hvor vedkommende var i en tillidsposition. Han fuldendte sin fængselsstraf i 2000. Et år senere anmodede han om at få fjernet denne dom fra hans straffeattest, men anmodningen blev afvist. I 2004 fastlagde en fransk lov en national retsdatabase over sexforbrydere, og sagsøgeren blev oplyst omkring hans optagelse heri. EMD fastholdt at registreringen af en dømt sexforbryder i en national retsdatabase var omfattet af artikel 8 i EMRK. Eftersom tilstrækkelig databeskyttelse var garanteret, f.eks. den registreredes ret til at anmode om at få oplysningerne slettet, den begrænsede opbevaringsperiode og begrænset adgang til sådanne oplysninger, havde man sikret en rimelig balance mellem de involverede og modstridende private og offentlige interesser. Domstolen konkluderede, at EMRK's artikel 8 ikke var blevet overtrådt.

([732]) Se for eksempel EMD, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987; EMD, *M.M. mod Det Forenede Kongerige*, nr. 24029/07, 13. november 2012; EMD, *M.K. mod Frankrig*, nr. 19522/09, 18. april 2013 eller EMD, *Aycaguer mod Frankrig*, nr. 8806/12, 22. juni 2017.

([733]) EMD, *B.B. mod Frankrig*, nr. 5335/06, 17. december 2009.

Eksempel: I sagen *S. og Marper mod Det Forenede Kongerige* ([734]) var begge sagsøgere blevet tiltalt, men ikke dømt for overtrædelse af straffeloven. Alligevel beholdt og opbevarede politiet deres fingeraftryk, DNA-profiler og celleprøver. Den ubegrænsede opbevaring af de førnævnte biometriske data var tilladt, hvis en person var mistænkt for en strafbar handling, selv om den mistænkte senere blev frikendt eller løsladt. EMD fastslog, at den generelle og vilkårlige opbevaring af personoplysninger, som ikke var tidsbegrænset, og hvor de frikendte enkeltpersoner kun havde begrænset mulighed for at anmode om sletning, udgjorde et uforholdsmæssigt indgreb i sagsøgernes ret til respekt for privatlivet. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Et vigtigt spørgsmål i forbindelse med elektronisk kommunikation er offentlige myndigheders indgreb i retten til privatlivets fred og databeskyttelse. Metoder til overvågning eller opfangelse af kommunikation, som f.eks. aflytningsudstyr, er kun tilladt, hvis dette er fastsat ved lov, og hvis det udgør en nødvendig foranstaltning i et demokratisk samfund af hensyn til:

- beskyttelse af national sikkerhed
- offentlig sikkerhed
- statens økonomiske interesser
- bekæmpelse af strafbare handlinger, eller
- beskyttelse af den registreredes eller andres rettigheder og frihedsrettigheder.

Mange andre EMD-domme omhandler begrundelsen for indgreb i retten til privatlivets fred igennem gennemførelse af overvågning.

Eksempel: I sagen *Allan mod Det Forenede Kongerige* ([735]) havde myndighederne i hemmelighed optaget en indsats private samtaler med en ven i fængslets besøgsområde og med en medanklaget i en

([734]) EMD, *S. og Marper mod Det Forenede Kongerige* [GC], nr. 30562/04 og 30566/04, 4. december 2008, præmis 119 og 125.

([735]) EMD, *Allan mod Det Forenede Kongerige*, nr. 48539/99, 5. november 2002.

fængselscelle. Menneskerettighedsdomstolen fastslog, at brugen af lyd- og videooptagelsesudstyr i sagsøgerens celle, fængslets besøgsområde og på en medindsat udgjorde et indgreb i sagsøgerens ret til respekt for privatlivet. Da der på daværende tidspunkt ikke var fastlagt bestemmelser vedrørende politiets skjulte brug af optageudstyr, var det pågældende indgreb ikke i overensstemmelse med loven. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Eksempel: I sagen *Roman Zakharov mod Rusland* ([736]) anlagde sagsøgeren retssager mod tre mobilnetoperatører. Han argumenterede for, at hans ret til privatlivets fred i forbindelse med hans telefoniske kommunikation var blevet krænket, da operatørerne havde monteret udstyr, som gjorde det muligt for den føderale sikkerhedstjeneste at opfange hans telefoniske kommunikation uden forudgående retskendelse. EMD fastholdt, at den nationale lovgivning, som regulerer opfangelse af kommunikationer, ikke gav tilstrækkelige og effektive garantier mod vilkårlig behandling og risikoen for misbrug. Den nationale lovgivning krævede navnlig ikke, at de lagrede oplysninger blev slettet, efter lagringsformålet var opnået. Desuden var det retlige tilsyn begrænset, selvom retskendelse var påkrævet.

Eksempel: I sagen *Szabó og Vissy mod Ungarn* ([737]) påstod sagsøgerne, at den ungarske lovgivning var i strid med EMRK's artikel 8, da den ikke var tilstrækkelig detaljeret eller nøjagtig. Derudover blev det argumenteret, at lovgivningen ikke sikrede tilstrækkelige garantier mod misbrug og vilkårlig behandling. EMD fastholdt, at den ungarske lovgivning ikke krævede, at overvågning var underlagt godkendelse ved en domstol. Ikke desto mindre bemærkede Domstolen, at selvom den var underlagt godkendelse fra justitsministeren, var denne overvågning særdeles politisk og opfyldte ikke den krævede vurdering af strengt nødvendigt. Desuden fastlagde den nationale lovgivning ikke en domstolsprøvelse, da de registrerede ikke tilsendes nogen underretning. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Da politiets behandling af personoplysninger kan have betydelige følger for de berørte personer, er der et særligt behov for detaljerede databeskyttelsesregler i forbindelse med behandlingen af personoplysninger på dette område.

([736]) EMD, *Roman Zakharov mod Rusland* [GC], nr. 47143/06, 4. december 2015.

([737]) EMD, *Szabo og Vissy mod Ungarn*, nr. 37138/14, 12. januar 2016.

Europarådets henstilling om politiets brug af personoplysninger omhandler dette spørgsmål og indeholder retningslinjer for, hvordan personoplysninger bør indsamles i forbindelse med politiets arbejde; hvordan sådanne arkiver bør opbevares; hvem der bør have adgang til disse arkiver, herunder betingelserne for videregivelse af personoplysninger til udenlandske politimyndigheder; hvordan registrerede bør have mulighed for at udøve deres ret til databeskyttelse og hvordan uafhængig myndighedskontrol bør gennemføres. Forpligtelsen til at garantere tilstrækkelig datasikkerhed blev også taget under overvejelse.

I henhold til henstillingen har politiet ikke ubegrænset og vilkårlig mulighed for at indsamle personoplysninger. Den begrænser politiets indsamling af personoplysninger til det, der er nødvendigt for at forebygge en reel fare eller retsforfølge en specifik strafbar handling. Yderligere dataindsamling skal baseres på specifik national lovgivning. Behandling af følsomme oplysninger bør begrænses til det, der er absolut nødvendigt i forbindelse med en bestemt sag.

Hvis personoplysninger indsamles uden den registreredes viden, bør den registrerede informeres om dataindsamlingen, så snart en sådan oplysning ikke længere er til hinder for efterforskningen. Indsamling af oplysninger ved teknisk overvågning eller andre automatiske midler skal have et specifikt retsgrundlag.

Eksempel: I sagen *Versini-Campinchi og Crasnianski mod Frankrig* ([738]) havde sagsøgeren, en advokat, en telefonsamtale med en klient, hvis telefonlinje blev aflyttet efter anmodning fra en undersøgelsesdommer. Transskriptionen over samtalen viste, at hun havde afsløret oplysninger omfattet af fortroligheden i korrespondancen mellem advokater og klienter. Anklageren sendte disse oplysninger til advokatrådet, som pålagde sagsøgeren en sanktion. EMD anerkendte eksistensen af et indgreb i retten til respekt for privatlivets fred og korrespondance - ikke kun for den person, hvis telefon var blevet aflyttet, men også for sagsøgeren, hvis kommunikation var blevet aflyttet og transskriberet. Indgrebet var foretaget i henhold til loven og havde et legitimt mål om at forebygge uro. Sagsøgeren havde fået fat på en gennemgang af, om indsendelsen af transskriptionen over telefonaflytningsoptagelserne i forbindelse med disciplinærsagen, som blev indledt mod hende, var lovlig. Selvom hun ikke havde haft mulighed for at anmode om at annullere transskriptionen for telefonsamtalen, mente EMD, at der havde været en effektiv kontrol, som havde været i stand til at holde det indgreb,

([738]) EMD, *Versini-Campinchi og Crasnianski mod Frankrig*, nr. 49176/11, 16. juni 2016.

der klages over, inden for et niveau, der var nødvendigt i et demokratisk samfund. EMD fastholdt, at argumentet om, at muligheden for straffesager mod en advokat på baggrund af en transskription kunne have en negativ virkning på kommunikationsfriheden mellem en advokat og dennes klient og dermed sidstnævntes ret til forsvar, ikke er troværdigt, når offentliggørelsen foretaget af advokaten i sig selv var ulovlig adfærd. Der blev derfor ikke konstateret nogen overtrædelse af artikel 8.

Europarådets henstilling om politiets brug af personoplysninger fastlægger, at der ved lagring af personoplysninger klart skal adskilles mellem administrative oplysninger, politioplysninger (personoplysninger for forskellige typer af registrerede, såsom mistænkte, dømte personer, ofre og vidner), oplysninger, der betragtes som konkrete kendsgerninger, og dem, som er baseret på mistanker eller spekulation.

Formålet med anvendelsen af politioplysninger skal være begrænset til det strengt nødvendige. Dette har konsekvenser for offentliggørelse af politioplysninger til tredjeparter: Overførsel eller offentliggørelse af sådanne oplysninger inden for politisektoren skal være reguleret efter, hvorvidt en legitim interesse ligger til grund for deling af oplysningerne. Overførsel eller offentliggørelse af sådanne oplysninger uden for politisektoren skal kun tillades, når der er en tydelig retlig forpligtelse eller tilladelse.

Eksempel: I sagen *Karabeyoğlu mod Tyrkiet* ([739]) fik sagsøgeren, en dommer, aflyttet sine telefonlinjer i forbindelse med en efterforskning af en kriminalsag vedrørende en ulovlig organisation, som han var mistænkt for at høre til, eller som man mente, at han ydede bistand og hjælp til. Efter det blev besluttet, at ingen skulle retsforfølges, ødelagde den offentlige anklager med ansvar for efterforskningen de pågældende optagelser. De retlige efterforskere beholdt dog en kopi, og de brugte det relevante materiale i forbindelse med en disciplinærundersøgelse af sagsøgeren. EMD fastholdt, at den pågældende lovgivning var overtrådt, da oplysningerne var blevet anvendt til andre formål end det, som de var indsamlet til, og de var ikke blevet ødelagt inden for en lovbestemt tidsfrist. Indgrebet i sagsøgerens ret til respekt for hans privatliv var, i forbindelse med disciplinærsagen mod vedkommende, i strid med loven.

([739]) EMD, *Karabeyoğlu mod Tyrkiet*, nr. 30083/10, 7. juni 2016.

International videregivelse eller offentliggørelse bør kun være tilladt til udenlandske politimyndigheder og bør være baseret på særlige lovbestemmelser, eventuelt internationale aftaler, medmindre det er nødvendigt for at forebygge alvorlige og umiddelbart forestående farer.

Politiets databehandling skal være underlagt uafhængigt tilsyn for at sikre overholdelse af national databeskyttelseslovgivning. Registrerede skal have alle adgangsrettighederne anført i den moderniserede konvention 108. Hvis registreredes ret til indsigt har været begrænset i medfør af artikel 9 i konvention 108 af hensyn til politiets effektive efterforskning og fuldbyrdelse af strafferetlige sanktioner, skal den registrerede have ret til i henhold til national lovgivning at klage til den nationale databeskyttelsesmyndighed eller et andet uafhængigt organ.

8.1.2. Budapestkonventionen om cyberkriminalitet

Da kriminelle aktiviteter i stigende grad anvender og påvirker elektroniske databehandlingssystemer, er der behov for nye strafferetlige bestemmelser for at imødegå denne udfordring. Europarådet vedtog derfor et internationalt retligt instrument, konventionen om cyberkriminalitet – også kaldt Budapestkonventionen – som omhandler kriminalitet, der begås mod og ved hjælp af elektroniske netværk ([740]). Denne konvention kan også tiltrædes af lande, som ikke er medlem af Europarådet. Siden begyndelsen af 2018 har 14 stater uden for Europarådet ([741]) været parter i konventionen, mens syv andre ikkemedlemmer er blevet opfordret til at tiltræde den.

Konventionen om cyberkriminalitet er stadig den mest indflydelsesrige internationale traktat vedrørende lovovertrædelser, der begås via internettet eller andre informationsnetværk. Den kræver, at parterne ajourfører og harmoniserer deres straffelovgivning mod hacking og andre sikkerhedskrænkelser, herunder krænkelse af ophavsret, IT-bedrageri, børnepornografi og andre ulovlige cyberaktiviteter. Ved konventionen fastlægges der også processuelle rettigheder, som omfatter søgning på computernetværk og overvågning af kommunikation i forbindelse med bekæmpelse af cyberkriminalitet. Endelig muliggør den effektivt internationalt samarbejde.

([740]) Europarådet, Ministerudvalget (2001), konvention om cyberkriminalitet, CETS nr. 185, Budapest, 23. november 2001, ikrafttrædelse den 1. juli 2004.

([741]) Australien, Canada, Chile, Colombia, Den Dominikanske Republik, Israel, Japan, Mauritius, Panama, Senegal, Sri Lanka, Tonga, Tunesien og USA. Se Chart of signatures and ratifications of Treaty 185, status as of July 2017.

En tillægsprotokol til konvention omhandler kriminaliseringen af racistisk og xenofobisk propaganda på computernetværk.

Konventionen er ikke et egentligt instrument til fremme af databeskyttelse, men kriminaliserer aktiviteter, der med sandsynlighed kan krænke en registrerets ret til beskyttelse af vedkommendes personoplysninger. Derudover kræver den, at kontraherende parter vedtager lovmæssige foranstaltninger, som gør det muligt for nationale myndigheder at opfange trafik og indholdsdata ([742]). Den forpligter også de kontraherende parter til ved gennemførelsen af konventionen at sikre tilstrækkelig beskyttelse af menneskerettigheder og frihedsrettigheder, herunder rettigheder garanteret i medfør af EMRK, som f.eks. retten til databeskyttelse ([743]). Det er ikke et krav, at kontraherende parter slutter sig til konvention 108 for at tiltræde Budapestkonventionen om cyberkriminalitet.

8.2. EU-retten vedrørende databeskyttelse i forbindelse med politi- og strafferetlige sager

Hovedpunkter

- På EU-plan reguleres databeskyttelse inden for politisektoren og strafferetten i forbindelse med både national og grænseoverskridende behandling hos medlemsstaters politi og strafferetlige myndigheder og EU-aktører.
- På medlemsstatsniveau skal databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder gennemføres i national lovgivning.
- Særlige retlige instrumenter regulerer databeskyttelse for grænseoverskridende samarbejde mellem politi og retshåndhævende myndigheder, navnlig i forbindelse med bekæmpelse af terrorisme og grænseoverskridende kriminalitet.
- Der findes særlige databeskyttelsesregler for Europol, Eurojust (Den Europæiske Unions Agentur for Strafferetligt Samarbejde) og Den Europæiske Anklagemyndighed, der er oprettet for nylig, som er EU-organer, der medvirker til og fremmer grænseoverskridende retshåndhævelse.

([742]) Europarådet, Ministerudvalget (2001), konvention om cyberkriminalitet, CETS nr. 185, Budapest, 23. november 2001, artikel 20 og 21.

([743]) *Ibid*., artikel 15, stk. 1.

- Der findes også særlige databeskyttelsesregler for de fælles informationssystemer, der er oprettet på EU-plan for grænseoverskridende informationsudveksling mellem kompetente politi- og retsmyndigheder. Vigtige eksempler er SIS II (Schengeninformationssystemet II), VIS (visuminformationssystemet) og Eurodac, et centralt system, der indeholder fingeraftryksoplysninger om tredjelandsstatsborgere og statsløse personer, der søger om asyl i en EU-medlemsstat.
- EU er i gang med at ajourføre databeskyttelsesbestemmelserne fastlagt i ovenstående, så de er i overensstemmelse med databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder.

8.2.1. Databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder

Direktiv (EU) 2016/680 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger (databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder) ([744]) er rettet mod at beskytte personoplysninger, der indsamles og behandles med henblik på strafferetlige formål, der spænder fra:

- forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed
- fuldbyrdelse af en strafferetlig sanktion
- tilfælde, hvor politi eller andre retshåndhævende myndigheder håndhæver loven og beskytter mod og forebygger trusler mod den offentlige sikkerhed og samfundets grundlæggende rettigheder, som kunne udgøre en strafbar handling.

([744]) Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA, EUT L 119 af 4. maj 2016, s. 89 (databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder).

Databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder beskytter personoplysningerne for forskellige kategorier af enkeltpersoner, som er involveret i straffesager, såsom vidner, kilder, ofre, mistænkte og medskyldige. Politi og strafferetlige myndigheder er forpligtet til at overholde direktivets bestemmelser, når de behandler sådanne oplysninger i forbindelse med retshåndhævelse, både inden for direktivets personelle og materielle anvendelsesområde ([745]).

Det er dog også tilladt at benytte oplysninger til andre formål under visse betingelser. Databehandling til et andet retshåndhævende formål end det, som dataene blev indsamlet til, tillades kun, hvis det er lovligt, nødvendigt og forholdsmæssigt i medfør af national lovgivning eller EU-ret ([746]). For andre formål finder reglerne i den generelle forordning om databeskyttelse anvendelse. Registrering og dokumentering af datadeling er én af de kompetente myndigheders særlige pligter, som skal hjælpe med at præcisere de ansvarsområder, der opstår som følge af klager.

Kompetente myndigheder, som arbejder inden for politi- og strafferetsområdet, er offentlige myndigheder eller myndigheder, der er bemyndiget af national lovgivning og offentlige beføjelser til at udføre en offentlig myndigheds funktioner ([747]), f.eks. private fængsler ([748]). Direktivets annvendelsesområde omfatter både databehandling på nationalt plan og grænseoverskridende behandling mellem medlemsstaters politi- og retsmyndigheder samt de kompetente myndigheders internationale overførsler til tredjelande og internationale organisationer ([749]). Det omfatter ikke national sikkerhed eller behandling af personoplysninger ved EU's institutioner, organer, kontorer og agenturer ([750]).

Direktivet henviser i stor grad til principper og definitioner i den generelle forordning om databeskyttelse, hvor der tages hensyn til, at politiets og strafferettens område er af en særlig karakter. Tilsyn kan udføres af de samme myndigheder

([745]) Databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder, artikel 2, stk. 1.

([746]) *Ibid*., artikel 4, stk. 2.

([747]) *Ibid*., artikel 3, stk. 7.

([748]) Europa-Kommissionen (2016), Meddelelse fra Kommissionen til Europa-Parlamentet i henhold til artikel 294, stk. 6, i traktaten om Den Europæiske Unions funktionsmåde vedrørende Rådets holdning med henblik på vedtagelse af Europa-Parlamentets og Rådets direktiv om beskyttelse af fysiske personer i forbindelse med de kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, opdage eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA, COM(2016) 213 final, Bruxelles, 11. april 2016.

([749]) Databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder, kapitel V.

([750]) *Ibid*., artikel 2, stk. 3.

i medlemsstaten, som også udfører det i henhold til den generelle forordning om databeskyttelse. Udpegelse af databeskyttelsesrådgivere og udførelse af konsekvensanalyser vedrørende databeskyttelse er indført i direktivet som nye forpligtelser for politi- og strafferetlige myndigheder ([751]). Selvom disse begreber er inspireret af den generelle forordning om databeskyttelse, er direktivet rettet mod politi- og strafferetlige myndigheders særlige karakter. Sammenlignet med databehandling til kommercielle formål, som reguleres af forordningen, kan sikkerhedsrelateret behandling kræve et vist fleksibilitetsniveau. For eksempel kan levering af det samme beskyttelsesniveau til registrerede i forbindelse med rettighederne til information, adgang til eller sletning af deres personoplysninger som i den generelle forordning om databeskyttelse betyde, at alle overvågningsaktiviteter, som udføres med henblik på retshåndhævende formål, ville være ineffektivt i forbindelse med retshåndhævelse. Direktivet indeholder derfor ikke princippet om gennemsigtighed. På tilsvarende vis skal principperne om dataminimering og formålsbegrænsning, som kræver, at personoplysninger begrænses til det, der er nødvendigt til de formål, som oplysningerne behandles til, og at de behandles til udtrykkeligt angivne formål, også finde anvendelse på en fleksibel måde ved sikkerhedsrelateret behandling. De oplysninger, som indsamles og lagres af kompetente myndigheder til en bestemt sag, kan være ekstremt nyttige til opklaringen af fremtidige sager.

Principper for behandling

Databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder fastlægger nogle nøglegarantier for brugen af personoplysninger. Det fastlægger også de principper, som vejleder behandlingen af disse oplysninger. Medlemsstater skal sikre, at personoplysninger:

- behandles lovligt og rimeligt
- indsamles til udtrykkeligt angivne og legitime formål og ikke behandles på en måde, der er uforenelig med disse formål
- er tilstrækkelige, relevante og ikke omfatter mere end, hvad der kræves til opfyldelse af de formål, hvortil de behandles

([751]) *Ibid.*, henholdsvist artikel 32 og 27.

- er korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt til at sikre, at personoplysninger, der er urigtige hvad angår de formål, hvortil de behandles, omgående slettes eller berigtiges

- opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de behandles

- behandles på en måde, der sikrer en tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger ([752]).

Under direktivet er behandling kun lovlig, når det finder sted i det omfang, som er nødvendigt til at udføre den pågældende opgave. Desuden skal behandling udføres af en kompetent myndighed for at nå målene angivet i direktivet og være baseret på EU-retten eller national lovgivning ([753]). Oplysninger må ikke opbevares i længere tid end nødvendigt, og de skal slettes eller periodisk revideres inden for fastlagte tidsfrister. De må kun benyttes af en kompetent myndighed og til de formål, som oplysningerne blev indsamlet, overført eller gjort tilgængelige til.

Den registreredes rettigheder

Direktivet fastlægger også den registreredes rettigheder. Disse omfatter:

- Retten til at modtage oplysninger. Medlemsstater skal kræve, at dataansvarlige stiller til rådighed for den registrerede: 1) identitet på og kontaktoplysninger for den dataansvarlige, 2) kontaktoplysninger for en eventuel databeskyttelsesrådgiver, 3) formålene med den behandling, som personoplysningerne skal bruges til, 4) retten til at indgive en klage til en tilsynsmyndighed og kontaktoplysningerne for tilsynsmyndigheden og 5) retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger og begrænsning af behandling af personoplysningerne vedrørende den registrerede ([754]). Udover disse generelle oplysningskrav fastlægger direktivet, at dataansvarlige i specifikke tilfælde og for at muliggøre udøvelsen af deres rettigheder skal give de

([752]) *Ibid*., artikel 4, stk. 1.

([753]) *Ibid*., artikel 8.

([754]) *Ibid*., artikel 13, stk. 1.

registrerede oplysninger om retsgrundlaget for behandlingen, og om i hvor lang tid oplysningerne opbevares. Hvis personoplysninger skal overføres til andre modtagere, herunder i tredjelande eller internationale organisationer, skal registrerede oplyses om kategorierne for sådanne modtagere. Endelig skal dataansvarlige forsyne alle supplerende oplysninger under hensyntagen til de specifikke omstændigheder, hvorunder oplysningerne behandles – for eksempel når personoplysninger indsamles i forbindelse med skjult overvågning, dvs. uden den registreredes viden. Dette garanterer rimelig behandling for den registrerede ([755]).

- Retten til indsigt i personoplysninger. Medlemsstater skal sikre registreredes ret til at vide, om vedkommendes personoplysninger behandles. Gør de det, bør den registrerede have adgang til visse oplysninger, såsom datakategorierne, som behandles ([756]). Denne ret kan dog begrænses – for eksempel for at undgå hindring af undersøgelser, eller at retsforfølgning af kriminalitet skades, eller for at beskytte offentlig sikkerhed og andres rettigheder og frihedsrettigheder ([757]).

- Retten til berigtigelse af personoplysninger. Medlemsstater er forpligtede til at sikre, at en registreret uden unødig forsinkelse kan få ukorrekte personoplysninger berigtiget. Derudover har den registrerede også ret til at få fuldstændiggjort ufuldstændige personoplysninger ([758]).

- Retten til sletning af personoplysninger og begrænsning af behandling. I visse tilfælde skal den dataansvarlige slette personoplysninger. Desuden kan den registrerede sikre sletningen af deres personoplysninger, men kun når de ulovligt behandles ([759]). I visse situationer kan behandlingen af personoplysninger begrænses i stedet for, at disse slettes. Dette kan finde sted i tilfælde, hvor 1) nøjagtigheden af personoplysningerne er anfægtet, men uden mulighed for at fastslå dette, eller 2) når personoplysningerne er nødvendige til brug som bevismateriale ([760]).

([755]) *Ibid.*, artikel 13, stk. 2.
([756]) *Ibid.*, artikel 14.
([757]) *Ibid.*, artikel 15.
([758]) *Ibid.*, artikel 16, stk. 1.
([759]) *Ibid.*, artikel 16, stk. 2.
([760]) *Ibid.*, artikel 16, stk. 3.

Når den dataansvarlige nægter at berigtige eller slette personoplysninger eller begrænse behandlingen af oplysninger, skal den registrerede skriftligt oplyses herom. Medlemsstater kan begrænse denne ret til at blive underrettet for, blandt andet, at beskytte offentlig sikkerhed eller andres rettigheder og frihedsrettigheder på baggrund af de samme årsager, der ligger til grund for retten til indsigt ([761]).

Den registrerede er normalt berettiget til oplysninger om behandlingen af vedkommendes personoplysninger og har ret til indsigt i, berigtigelse af eller sletning af begrænsningen af behandling, som denne kan udøve direkte hos den dataansvarlige. Som et alternativ er den indirekte udøvelse af den registreredes rettigheder igennem dennes tilsynsmyndighed for databeskyttelse også mulig under databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder, og det træder i kraft, når den dataansvarlige begrænser den registreredes rettigheder ([762]). Artikel 17 i direktivet kræver, at medlemsstater vedtager foranstaltninger, som sikrer, at registreredes rettigheder også kan udøves igennem deres tilsynsmyndighed. Dette er grunden til, at den dataansvarlige skal oplyse den registrerede om muligheden for indirekte adgang.

Forpligtelser for den dataansvarlige og databehandleren

I forbindelse med databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder er dataansvarlige kompetente offentlige myndigheder eller andre organer med relevante offentlige beføjelser og offentlig myndighed, som bestemmer formålene med og metoderne for personoplysningers behandling. Direktivet fastlægger flere forpligtelser for dataansvarlige om at sikre et højt beskyttelsesniveau for personoplysninger, som behandles til retshåndhævende formål.

Kompetente myndigheder skal foretage logning over de behandlingsaktiviteter, de udfører i automatiske databehandlingssystemer. Der skal som minimum foretages logning over indsamling, ændring, søgning, videregivelse, herunder overførsel, samkøring og sletning af personoplysningerne ([763]). Direktivet fastsætter, at logning af søgning og videregivelse skal gøre det muligt at fastlægge begrundelsen, datoen og tidspunktet for sådanne aktiviteter og i videst muligt omfang identifikation af den person, som har søgt eller videregivet personoplysninger, og identiteten på modtagerne af sådanne personoplysninger. Loggene anvendes udelukkende til at

([761]) *Ibid.*, artikel 16, stk. 4.

([762]) *Ibid.*, artikel 17.

([763]) *Ibid.*, artikel 25, stk. 1.

kontrollere, om behandling er lovlig, til egenkontrol, til at sikre integriteten og sikkerheden af personoplysningerne og i forbindelse med straffesager ([764]). Den dataansvarlige og databehandleren skal efter anmodning stille loggene til rådighed for tilsynsmyndigheden.

Navnlig er der en generel forpligtelse om, at dataansvarlige implementerer passende tekniske og organisatoriske foranstaltninger til at sikre, at behandling udføres i medfør af direktivet, og for at påvise lovligheden af en sådan behandling ([765]). Ved udformningen af disse foranstaltninger skal de tage hensyn til behandlingens karakter, omfang, sammenhæng og, vigtigst af alt, alle potentielle risici for enkeltpersoners rettigheder og frihedsrettigheder. Dataansvarlige bør vedtage interne politikker og implementere foranstaltninger, som fremmer overholdelse af principperne for databeskyttelse, navnlig princippet om databeskyttelse gennem design og standardindstillinger ([766]). Når behandling med sandsynlighed kan resultere i en høj risiko for enkeltpersoners rettigheder – for eksempel på grund af brugen af nye teknologier – skal dataansvarlige udføre en konsekvensanalyse vedrørende databeskyttelse, inden behandlingen påbegyndes ([767]). Direktivet angiver også de foranstaltninger, som skal implementeres af de dataansvarlige for at sikre behandlingens sikkerhed. Disse omfatter foranstaltninger til at forhindre uautoriseret adgang til de personoplysninger, som behandles af dem, og til at sikre, at uautoriserede personer kun har adgang til de personoplysninger, som er omfattet af deres adgangstilladelse, at behandlingssystemets funktioner fungerer korrekt, og at lagrede personoplysninger ikke kan blive ødelagt som følge af fejlfunktioner i systemet ([768]). Hvis et brud på persondatasikkerheden finder sted, skal dataansvarlige underrette tilsynsmyndigheden inden for tre dage, hvor denne beskriver bruddets karakter, dets sandsynlige konsekvenser, kategorierne af personoplysninger og det omtrentlige antal berørte registrerede. Bruddet på persondatasikkerheden skal også meddeles til den registrerede uden »unødig forsinkelse«, når bruddet på persondatasikkerheden med sandsynlighed udgør en stor risiko for vedkommendes rettigheder og frihedsrettigheder ([769]).

([764]) *Ibid.*, artikel 25, stk. 2.
([765]) *Ibid.*, artikel 19.
([766]) *Ibid.*, artikel 20.
([767]) *Ibid.*, artikel 27.
([768]) *Ibid.*, artikel 29.
([769]) *Ibid.*, artikel 30 og 31.

Direktivet indeholder ansvarlighedsprincippet, som forpligter dataansvarlige til at implementere foranstaltninger, der sikrer overholdelse af dette princip. Dataansvarlige skal føre fortegnelser over alle de kategorier af behandlingsaktiviteter, som de er ansvarlige for. Det detaljerede indhold af sådanne fortegnelser er angivet i direktivets artikel 24. Fortegnelserne skal efter anmodning gøres tilgængelige for tilsynsmyndigheden, så de kan overvåge den dataansvarliges behandlingsaktiviteter. En anden vigtig foranstaltning for at forbedre ansvarlighed er at udpege en databeskyttelsesrådgiver (DPO). Dataansvarlige skal udpege en DPO, selvom direktivet tillader, at medlemsstater fritager domstole og andre uafhængige judicielle myndigheder fra denne forpligtelse ([770]). DPO'ens forpligtelser minder om dem i den generelle forordning om databeskyttelse. Vedkommende kontrollerer overensstemmelse med direktivet, videregiver oplysninger og rådgiver medarbejdere, som udfører databehandling, om deres forpligtelser under databeskyttelseslovgivningen. DPO'en udsteder også rådgivning om behovet for at udføre en konsekvensanalyse vedrørende databeskyttelse og fungerer som kontaktpunkt for tilsynsmyndigheden.

Overførsler til tredjelande eller internationale organisationer

Ligesom den generelle forordning om databeskyttelse fastlægger direktivet betingelser for overførsel af personoplysninger til tredjelande eller internationale organisationer. Hvis personoplysninger blev frit overført uden for EU's jurisdiktion, kan garantierne og den stærke beskyttelse, som sikres under EU-retten, undermineres. Selve betingelserne er dog meget anderledes end dem i den generelle forordning om databeskyttelse. Overførsler af personoplysninger til tredjelande eller internationale organisationer tillades, hvis ([771]):

- Overførslen er nødvendig for at nå direktivets mål.
- Personoplysningerne overføres til en kompetent myndighed, i overensstemmelse med direktivet, i tredjelandet eller den internationale organisation – selvom der i enkeltstående og specifikke tilfælde er en undtagelse fra denne regel ([772]).
- Overførsler til tredjelande eller internationale organisationer af personoplysninger, som er modtaget i forbindelse med grænseoverskridende samarbejde,

([770]) *Ibid.*, artikel 32.

([771]) *Ibid.*, artikel 35.

([772]) *Ibid.*, artikel 39.

kræver godkendelse fra medlemsstaten, hvorfra oplysningerne oprinder. Dog er der undtagelser ved hastesager.

- En afgørelse om tilstrækkeligheden af beskyttelsesniveauet er vedtaget af Europa-Kommissionen, passende garantier er etableret, eller undtagelsen for overførsler i særlige situationer finder anvendelse.

- Videreoverførsler af personoplysninger til et andet tredjeland eller en international organisation kræver den kompetente myndighed fra oprindelsesstedets forudgående godkendelse, der bl.a. tager hensyn til overtrædelsens alvor og niveauet af databeskyttelse i destinationslandet for den anden internationale overførsel ([773]).

Under direktivet må overførsler af personoplysninger finde sted, hvis én af tre betingelser er opfyldt. Den første er, når Europa-Kommissionen har udstedt en afgørelse om tilstrækkeligheden af beskyttelsesniveauet under direktivet. Afgørelsen kan finde anvendelse i hele tredjelandets område, i bestemte sektorer i et tredjeland eller for en international organisation. Dette kan dog kun gøres, hvis et tilstrækkeligt beskyttelsesniveau sikres, og betingelserne defineret i direktivet opfyldes ([774]). I sådanne tilfælde er overførslen af personoplysninger ikke underlagt medlemsstatens godkendelse ([775]). Europa-Kommissionen skal overvåge udviklinger, der kan påvirke virkningen af afgørelser om tilstrækkeligheden af beskyttelsesniveauet. Derudover skal afgørelsen inkludere en mekanisme for regelmæssig revision. Kommissionen kan også ophæve, ændre eller suspendere en afgørelse, når tilgængelige oplysninger afslører, at betingelserne i tredjelandet eller den internationale organisation ikke længere sikrer et tilstrækkeligt beskyttelsesniveau. Er dette tilfældet, skal Kommissionen føre konsultationer med tredjelandet eller den internationale organisation med henblik på at afhjælpe situationen.

Ved mangel på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet kan overførsler baseres på fornødne garantier. De kan fastlægges i et retligt bindende instrument, eller den dataansvarlige kan udføre en selvvurdering af omstændighederne for overførslen af personoplysningerne og kan konkludere, at fornødne garantier er på plads. Selvvurderingen skal tage hensyn til

([773]) *Ibid.*, artikel 35, stk. 1.

([774]) *Ibid.*, artikel 36.

([775]) *Ibid.*, artikel 36, stk. 1.

eventuelle samarbejdsaftaler mellem Europol eller Eurojust og tredjelandet eller den internationale organisation, eksistensen af tavshedspligter og formålsbegrænsning samt afgivne garantier om, at oplysningerne ikke vil blive brugt til nogen form for grusom eller umenneskelig behandling, herunder dødsstraf ([776]). I sidstnævnte tilfælde skal den dataansvarlige oplyse den kompetente tilsynsmyndighed om overførselskategorierne under denne kategori ([777]).

Hvis ingen afgørelse om tilstrækkeligheden af beskyttelsesniveauet er vedtaget, eller ingen fornødne garantier er etableret, kan overførsler stadig tillades i specifikke situationer, som direktivet fastlægger. Disse omfatter bl.a. beskyttelse af den registreredes eller en anden persons vitale interesser og afværgelse af en umiddelbar og alvorlig trussel mod en medlemsstats eller et tredjelands offentlige sikkerhed ([778]).

I enkeltstående og specifikke tilfælde kan overførsler fra kompetente myndigheder til modtagere, der er etableret i tredjelande, som ikke er kompetente myndigheder, finde sted, hvis både én af de tre betingelser beskrevet i ovenstående samt yderligere betingelser fastlagt i direktivets artikel 39 opfyldes. Navnlig skal overførslen være strengt nødvendig til den overførende kompetente myndigheds udøvelse af en opgave, og denne myndighed er også ansvarlig for at vurdere, at ingen enkeltpersoners grundlæggende rettigheder eller frihedsrettigheder vejer tungere end den offentlige interesse, som begrunder overførslen. Sådanne overførsler skal dokumenteres, og den overførende kompetente myndighed skal underrette den kompetente tilsynsmyndighed ([779]).

I forhold til tredjelande og internationale organisationer kræver direktivet endelig også udviklingen af internationale samarbejdsmekanismer, som kan fremme den effektive håndhævelse af lovgivningen og dermed hjælpe tilsynsmyndigheder for databeskyttelse med at samarbejde med deres tilsvarende udenlandske organer ([780]).

([776]) *Ibid.*, betragtning 71.

([777]) *Ibid.*, artikel 37, stk. 1.

([778]) *Ibid.*, artikel 38, stk. 1.

([779]) *Ibid.*, artikel 37, stk. 3.

([780]) *Ibid.*, artikel 40.

Uafhængigt tilsyn og retsmidler for registrerede

Hver medlemsstat skal sikre, at én eller flere uafhængige nationale tilsynsmyndigheder er ansvarlige for at rådgive og overvåge anvendelsen af bestemmelserne, der er vedtaget i henhold til direktivet ([781]). Tilsynsmyndigheden, som er etableret til direktivets formål, kan være den samme som tilsynsmyndigheden, som er etableret under den generelle forordning om databeskyttelse, men medlemsstater kan dog selv udpege en anden myndighed, hvis den opfylder uafhængighedskriteriet. Tilsynsmyndigheder skal også behandle klager indgivet af personer vedrørende beskyttelsen af vedkommendes rettigheder og frihedsrettigheder i forbindelse med kompetente myndigheders behandling af personoplysninger.

Når udøvelsen af den registreredes rettigheder afvises ud fra en vægtig begrundelse, skal den registrerede have ret til at appellere til den kompetente nationale tilsynsmyndighed og/eller til en domstol. Hvis en person lider skade som følge af en overtrædelse af den nationale lovgivning, som implementerer direktivet, er vedkommende berettiget til erstatning fra den dataansvarlige eller en anden myndighed, der er kompetent i henhold til medlemsstaternes nationale ret ([782]). Generelt skal registrerede have adgang til retsmidler ved ethvert brud på deres rettigheder, der garanteres ved national ret, som gennemfører direktivet ([783]).

8.3. Andre specifikke retlige instrumenter om databeskyttelse i forbindelse med retshåndhævelse

Udover databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder reguleres udvekslingen af oplysninger i medlemsstaters besiddelse på bestemte områder af en række retslige instrumenter – såsom Rådets rammeafgørelse 2009/315/RIA om tilrettelæggelsen og indholdet af udvekslinger af oplysninger fra strafferegistre mellem medlemsstaterne, Rådets afgørelse 2000/642/RIA om samarbejdsordninger mellem medlemsstaternes finansielle efterretningsenheder for så vidt angår udveksling af oplysninger og Rådets rammeafgørelse 2006/960/RIA af

([781]) *Ibid.*, artikel 41.

([782]) *Ibid.*, artikel 56.

([783]) *Ibid.*, artikel 54.

18.december 2006 om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder ([784]).

Det er vigtigt at påpege, at grænseoverskridende samarbejde ([785]) mellem de kompetente myndigheder i stigende grad omfatter udveksling af immigrationsoplysninger. Dette lovområde anses ikke for at være en del af politi- og strafferetlige sager, men er på mange måder relevant for politiets og retsmyndigheders arbejde. Det samme gør sig gældende for oplysninger om varer, som importeres til eller eksporteres fra EU. Fjernelsen af de indre grænsekontroller i Schengenområdet har øget risikoen for bedrageri, hvilket har gjort det nødvendigt for medlemsstater at øge samarbejdet, navnlig ved at forbedre grænseoverskridende udvekslinger af oplysninger, så de mere effektivt er i stand til at opdage og retsforfølge overtrædelser af national og EU's toldlovgivning. Derudover har verden i senere år oplevet en stigning i grov og organiseret kriminalitet og terrorisme, som kan omfatte internationale rejser og i mange tilfælde har afsløret et behov for øget samarbejde mellem politi og retshåndhævende myndigheder på tværs af grænser ([786]).

Prümafgørelsen

Et vigtigt eksempel på institutionaliseret grænseoverskridende samarbejde ved udveksling af oplysninger, der opbevares af medlemsstaterne, er Rådets afgørelse 2008/615/RIA samt dennes gennemførelsesbestemmelser i afgørelse 2008/615/RIA om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (Prümafgørelsen), som gennemførte Prümaftalen i EU-retten i 2008 ([787]). Prümaftalen var en

([784]) Rådet for Den Europæiske Union (2009), Rådets rammeafgørelse 2009/315/RIA af 26. februar 2009 om tilrettelæggelsen og indholdet af udvekslinger af oplysninger fra strafferegistre mellem medlemsstaterne, EUT L 93 af 7. april 2009; Rådet for Den Europæiske Union (2000), Rådets afgørelse 2000/642/RIA af 17. oktober 2000 om samarbejdsordninger mellem medlemsstaternes finansielle efterretningsenheder for så vidt angår udveksling af oplysninger, EFT L 271 af 24. september 2000 og Rådets rammeafgørelse 2006/960/RIA af 18. december 2006 om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder, EUT L 386 af 29. december 2006.

([785]) Europa-Kommissionen (2012), *Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet – Styrkelse af samarbejdet om retshåndhævelse i EU: den europæiske informationsudvekslingsmodel (EIXM)*, COM(2012) 735 final, Bruxelles, 7. december 2012.

([786]) Se Europa-Kommissionen (2011), forslag til Europa-Parlamentets og Rådets direktiv om anvendelse af passagerlisteoplysninger til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet, KOM/2011/0032 endelig, Bruxelles, 2. februar 2011, s. 1.

([787]) Rådet for Den Europæiske Union (2008), Rådets afgørelse 2008/615/RIA af 23. juni 2008 om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet, EUT L 210 af 6. august 2008.

international aftale om politisamarbejde, som blev undertegnet af Belgien, Tyskland, Spanien, Frankrig, Luxembourg, Nederlandene og Østrig i 2005 ([788]).

Prümafgørelsen har til formål at hjælpe medlemsstaterne med at forbedre informationsudvekslingen med henblik på at forebygge og bekæmpe kriminalitet på tre områder, nemlig terrorisme, grænseoverskridende kriminalitet og ulovlig migration. Afgørelsen omfatter derfor bestemmelser vedrørende:

- elektronisk adgang til DNA-profiler, fingeraftryksoplysninger og oplysninger i nationale køretøjsregistre
- udveksling af oplysninger i forbindelse med større begivenheder på tværs af grænserne
- levering af oplysninger med henblik på at forebygge terrorisme
- andre foranstaltninger til intensivering af det grænseoverskridende politisamarbejde.

De databaser, der stilles til rådighed i medfør af Prümafgørelsen, er alene omfattet af national lovgivning, men udvekslingen af oplysninger er desuden underlagt afgørelsen, hvis kompatibilitet med databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder skal vurderes. De kompetente organer for tilsynet med sådanne dataudvekslinger er de nationale databeskyttelsesmyndigheder.

Rammeafgørelse 2006/960/RIA — det svenske initiativ

Rammeafgørelse 2006/960/RIA (det svenske initiativ) ([789]) er et andet eksempel på grænseoverskridende samarbejde i forbindelse med udveksling af oplysninger, som på nationalt niveau opbevares af retshåndhævende myndigheder. Det svenske initiativ fokuserer især på udveksling af efterretninger og oplysninger og fastlægger specifikke databeskyttelsesregler i artikel 8.

([788]) Aftale mellem Kongeriget Belgien, Forbundsrepublikken Tyskland, Kongeriget Spanien, Den Franske Republik, Storhertugdømmet Luxembourg, Kongeriget Nederlandene og Republikken Østrig om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme, grænseoverskridende kriminalitet og ulovlig migration.

([789]) Rådet for Den Europæiske Union (2006), Rådets rammeafgørelse 2006/960/RIA af 18. december 2006 om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder, EUT L 386/89 af 29. december 2006.

I medfør af dette instrument skal brugen af udvekslede oplysninger og efterretninger være underlagt de nationale databeskyttelsesbestemmelser i medlemsstaten, som modtager oplysningerne, og de samme regler, som hvis de var indsamlet i den medlemsstat. Artikel 8 går videre og fastslår, at kompetente retshåndhævende myndigheder ved levering af oplysninger og efterretninger kan pålægge betingelser, som er i overensstemmelse med deres nationale lovgivning, vedrørende den modtagende kompetente retshåndhævende myndigheds brug af disse oplysninger og efterretninger. Disse betingelser kan også finde anvendelse for rapportering af resultatet af kriminalefterforskninger eller kriminalefterretningsoperationer, hvor udvekslingen af oplysninger og efterretninger har været et krav. Men når national lovgivning fastlægger undtagelser for begrænsningerne i brugen af oplysningerne og efterretningerne (f.eks. for judicielle myndigheder, lovgivningsinstanser osv.), må disse kun benyttes efter forudgående høring af den medlemsstat, oplysningerne og efterretningerne stammer fra.

Meddelte oplysninger og efterretninger må benyttes:

- til de formål, hvortil de er meddelt, eller
- til at forebygge en umiddelbar og alvorlig trussel mod den offentlige sikkerhed.

Behandling til andre formål kan tillades, men kun efter forudgående høring af den medlemsstat, oplysningerne og efterretningerne stammer fra.

Det svenske initiativ fastsætter desuden, at behandlede personoplysninger skal beskyttes i henhold til internationale instrumenter, såsom:

- Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger ([790])
- Tillægsprotokol af 8. november 2001 til den konvention vedrørende tilsynsmyndigheder og grænseoverskridende dataudveksling ([791])

([790]) Europarådet (1981), konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, ETS nr. 108.

([791]) Europarådet (2001), tillægsprotokol til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger vedrørende tilsynsmyndigheder og grænseoverskridende videregivelse af personoplysninger, CETS nr. 108.

- Europarådets anbefaling nr. R (87) 15 om politiets brug af personoplysninger ([792]).

EU-direktivet om PNR-oplysninger

Passagerlisteoplysninger (PNR) omhandler oplysninger om luftpassagerer, som indsamles af og opbevares i flyselskabers reservations- og afgangskontrolsystemer til deres egne kommercielle formål. Disse data omfatter flere forskellige typer oplysninger, f.eks. rejsedatoer, rejseplan, billetoplysninger, kontaktoplysninger, det rejsebureau, som flyvningen blev reserveret igennem, betalingsmetode, sædenummer og bagageoplysninger ([793]). Behandling af PNR-oplysninger kan hjælpe retshåndhævende myndigheder med at identificere kendte eller potentielle mistænkte og udføre vurderinger på baggrund af rejsemønstre og andre indikatorer, som normalt er forbundet med kriminelle aktiviteter. En analyse af PNR-oplysninger tillader også efterfølgende sporing af rejseruter og kontakter for personer, som mistænkes for at være indblandet i kriminelle aktiviteter, hvilket kan gøre det muligt for retshåndhævende myndigheder at identificere kriminelle netværk ([794]). EU har indgået nogle aftaler med tredjelande vedrørende udveksling af PNR-oplysninger som forklaret i afsnit 7. Derudover har den indført behandling af PNR-oplysninger i EU igennem direktiv (EU) 2016/681 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (EU-direktivet om PNR-oplysninger) ([795]). Direktivet fastlægger forpligtelser for flyselskabers overførelse af PNR-oplysninger til de kompetente myndigheder og fastlægger strenge databeskyttelsesgarantier for behandling og indsamling af sådanne oplysninger. EU-direktivet om PNR-oplysninger er gældende for internationale flyvninger til og fra EU, men også for flyvninger inden for EU, hvis en medlemsstat beslutter dette ([796]).

([792]) Europarådet (1987), anbefaling nr. R (87) 15 fra Europarådets Ministerkomité til medlemsstaterne om politiets brug af personoplysninger (der blev vedtaget af Ministerkomitéen den 17. september 1987 på det 410. møde mellem ministerrepræsentanterne).

([793]) Europa-Kommissionen (2011), forslag til Europa-Parlamentets og Rådets direktiv om anvendelse af passagerlisteoplysninger til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet, KOM/2011/0032 endelig udg., Bruxelles, 2. februar 2011, s. 1.

([794]) Europa-Kommissionen (2015), Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives, (

([795]) Europa-Parlamentets og Rådets direktiv (EU) 2016/681 af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet, EUT L 119 af 4. maj 2016, s. 132.

([796]) PNR-direktivet, L 119, s. 132, artikel 1, stk. 1, og artikel 2, stk. 1.

Indsamlede PNR-oplysninger må kun indeholde de oplysninger, som er tilladt jf. EU-direktivet om PNR-oplysninger. De skal opbevares i en enkelt informationsenhed på en sikker placering i hver medlemsstat. PNR-oplysninger skal anonymiseres seks måneder efter deres overførelse fra flyselskabet og må maksimalt opbevares i en periode på fem år ([797]). PNR-oplysninger udveksles mellem medlemsstater, mellem medlemsstater og Europol og med tredjelande, men kun ud fra et individuelt grundlag.

Overførsel og behandling af PNR-oplysninger og registreredes garanterede rettigheder skal være i overensstemmelse med databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder og skal sikre det højeste beskyttelsesniveau af privatliv og personoplysninger, som kræves i chartret, den moderniserede konvention 108 og EMRK.

De uafhængige tilsynsmyndigheder, som er kompetente i medfør af databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder, er også ansvarlige for at rådgive om og overvåge anvendelsen af bestemmelserne vedtaget af medlemsstaterne i medfør af EU-direktivet om PNR-oplysninger.

Opbevaring af telekommunikationsoplysninger

Datalagringsdirektivet ([798]) — erklæret for ugyldig den 8. april 2014 i *Digital Rights Ireland* — forpligtede udbydere af kommunikationstjenester til at holde metadata tilgængelige til det specifikke formål at bekæmpe grov kriminalitet i mindst seks men højst 24 måneder, uanset om udbyderen stadig havde behov for disse oplysninger til fakturering eller for teknisk set at kunne levere tjenesten.

([797]) *Ibid*., artikel 12, stk. 1, og artikel 12, stk. 2.

([798]) Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF, EUT L 105 af 13. april 2006.

Opbevaring af telekommunikationsoplysninger overtræder klart retten til databeskyttelse ([799]). Flere retssager i EU-medlemsstater har anfægtet, hvorvidt dette indgreb er begrundet ([800]).

Eksempel: I sagen *Digital Rights Ireland* og *Kärntner Landesregierung m.fl.,* ([801]) anlagde Digital Rights-gruppen og Michael Seitlinger sag ved henholdsvist højesteretten i Irland og Østrigs forfatningsdomstol, hvor de rejste tvivl om lovligheden af nationale foranstaltninger, som tillod opbevaring af elektroniske telekommunikationsoplysninger. Digital Rights spurgte den irske domstol om at erklære direktiv 2006/24/EF og den del af den nationale strafferet, som vedrører terrorhandlinger, for ugyldig. På tilsvarende vis anfægtede Michael Seitlinger og mere end 11 000 andre sagsøgere en bestemmelse i den østrigske lovgivning om telekommunikationer, som gennemførte direktiv 2006/24/EF, og anmodede om annullering heraf.

Under behandling af disse anmodninger til præjudicielle afgørelser erklærede EU-Domstolen datalagringsdirektivet for ugyldigt. I medfør af EU-Domstolen indeholdt oplysninger, som kunne opbevares under direktivet, tilsammen præcise oplysninger om enkelte personer. Endvidere undersøgte EU-Domstolen alvoren af indgrebet i den grundlæggende rettighed til respekt for privatlivets fred og til beskyttelse af personoplysninger. Den konstaterede, at opbevaringen opfyldte et mål af almen interesse – nemlig bekæmpelse af grov kriminalitet, og som følge heraf havde den offentlig sikkerhed som endeligt mål. Ikke desto mindre erklærede EU-Domstolen, at EU-lovgiveren havde overtrådt proportionalitetsprincippet ved at vedtage direktivet. Selvom direktivet kan være passende til at nå det påkrævede mål, er direktivets indgreb af vidtrækkende og særligt alvorlig karakter i de grundlæggende rettigheder til respekt for privatliv og beskyttelse af personoplysninger ikke præcist afgrænset på tilstrækkelig vis til at sikre, at indgrebet faktisk er begrænset til det strengt nødvendige.

([799]) EDPS (2011), *Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse vedrørende evalueringsrapporten fra Kommissionen til Rådet og Europa-Parlamentet om datalagringsdirektivet (direktiv 2006/24/EF)*, 31. maj 2011.

([800]) Tysklands forfatningsdomstol (*Bundesverfassungsgericht*), 1 BvR 256/08, 2. marts 2010; Rumæniens forfatningsdomstol (*Curtea Constituțională a României*), nr. 1258, 8. oktober 2009; Den Tjekkiske Republiks forfatningsdomstol (*Ústavní soud České republiky*), 94/2011 sml., 22. marts 2011.

([801]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014, præmis 65.

Datalagring tillades som en forebyggende foranstaltning ved mangel på særlig lovgivning om datalagring og som en undtagelse til fortroligheden af telekommunikationsoplysninger under direktiv 2002/58/EF (direktiv om databeskyttelse inden for elektronisk kommunikation) ([802]), men skal udelukkende have bekæmpelse af grov kriminalitet som mål. En sådan lagring skal begrænses til det strengt nødvendige i forbindelse med kategorierne for de lagrede data, de påvirkede kommunikationsmidler, de berørte personer og lagringens valgte varighed. Nationale myndigheder kan have adgang til de lagrede data under strenge betingelser, herunder forudgående kontrol ved en uafhængig myndighed. Dataene skal lagres inden for EU's grænser.

Eksempel: Efter dommen i sagen *Digital Rights Ireland* og *Kärntner Landesregierung m.fl.* ([803]) blev to yderligere sager forelagt for EU-Domstolen vedrørende den generelle forpligtelse pålagt i Sverige og i Det Forenede Kongerige om, at udbydere af elektroniske kommunikationstjenester skulle lagre telekommunikationsoplysninger, jf. det ugyldiggjorte datalagringsdirektiv. I sagen *Tele2 Sverige* og *Home Department mod Tom Watson m.fl.* ([804]) afsagde EU-Domstolen dom om, at den nationale lovgivning, som foreskriver den generelle og udifferentierede lagring af data uden at kræve nogen sammenhæng mellem de data, som lagres, og en trussel mod den offentlige sikkerhed samt uden at angive nogen betingelser – f.eks. en tidsbegrænset lagringsperiode, geografisk område og persongrupper, som sandsynligvis er involveret i en grov forbrydelse – overskrider grænserne for det strengt nødvendige og kan ikke begrundes i et demokratisk samfund som krævet i direktiv 2002/58/EF og sammenholdt med EU's charter om grundlæggende rettigheder.

Fremtidsudsigter

I januar 2017 offentliggjorde Europa-Kommissionen et forslag til en forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse

([802]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), EFT L 201 af 31. juli 2002.

([803]) EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014.

([804]) EU-Domstolen, forenede sager C-203/15 og C-698/15, *Tele2 Sverige AB mod Post- och telestyrelsen* og *Secretary of State for the Home Department mod Tom Watson m.fl.* [GC], 21. december 2016.

med elektronisk kommunikation, som skulle ophæve og erstatte direktiv 2002/58/EF ([805]). Forslaget indeholder ingen specifikke bestemmelser om datalagring. Det fastlægger dog, at medlemsstater kan begrænse visse forpligtelser og rettigheder under forordningen i deres lovgivning, når en sådan begrænsning udgør en nødvendig og forholdsmæssig foranstaltning for at sikre bestemte offentlige interesser, herunder den nationale sikkerhed, forsvaret, den offentlige sikkerhed og forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner ([806]). Medlemsstaterne vil derfor være i stand til at beholde eller etablere nationale rammer for dataopbevaring, der indeholder bestemmelser om målrettet dataopbevaring, for så vidt som disse rammer – under hensyntagen til EU-Domstolens retspraksis vedrørende fortolkningen af e-databeskyttelsesdirektivet og EU's charter om grundlæggende rettigheder – er i overensstemmelse med EU-retten ([807]). Ved tidspunktet for håndbogens udarbejdelse var diskussionerne om forordningens vedtagelse endnu ikke afsluttet.

Paraplyaftalen mellem EU og USA om beskyttelse af personoplysninger, der udveksles til retshåndhævende formål

Den 1. februar 2017 trådte paraplyaftalen mellem EU og USA vedrørende behandlingen af personoplysninger til forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger i kraft ([808]). Paraplyaftalen mellem EU og USA har til formål at sikre et højt databeskyttelsesniveau for EU's borgere samt forstærke samarbejdet mellem EU's og USA's retshåndhævende myndigheder. Den supplerer eksisterende aftaler mellem EU og USA og medlemsstater og USA og deres retshåndhævende myndigheder, mens den også hjælper med at fastlægge klare og harmoniserede databeskyttelsesregler for fremtidige aftaler på dette område. I den sammenhæng er aftalen rettet mod at fastlægge holdbare lovrammer, der kan fremme udveksling af oplysninger.

Aftalen udgør alene ikke et passende retsgrundlag for udvekslingen af personoplysninger, men tilbyder i stedet passende databeskyttelsesgarantier for de

([805]) Europa-Kommissionen (2017), *forslag til Europa-Parlamentets og Rådets forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektroniske kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om databeskyttelse inden for elektronisk kommunikation)*, COM(2017) 10 final, Bruxelles, 10. januar 2017.

([806]) *Ibid.*, betragtning 26.

([807]) Se begrundelsen til forslaget til en forordning om databeskyttelse inden for elektronisk kommunikation, COM(2017) 10 final, punkt 1.3.

([808]) Se EU-Rådet (2016), »*Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign »Umbrella agreement*««, pressemeddelelse 305/16, 2. juni 2016.

berørte fysiske personer. Den omfatter al behandling af personoplysninger, som er nødvendig til forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, herunder terrorisme ([809]).

Aftalen fastsætter flere garantier til at sikre, at personoplysninger udelukkende anvendes til formålene anført i aftalen. Navnlig giver den følgende beskyttelse til EU-borgere:

- Begrænsninger for brugen af oplysninger: Personoplysninger må kun benyttes til at forebygge, efterforske, afsløre og retsforfølge strafbare handlinger.
- Beskyttelse mod vilkårlig og uberettiget forskelsbehandling.
- Videreoverførsler: Enhver videreoverførsel til et land uden for USA eller EU eller en international organisation skal være underlagt forudgående samtykke fra den kompetente myndighed i det land, som oprindeligt overførte dataene.
- Datakvalitet: Personoplysninger skal opbevares under hensyntagen til deres nøjagtighed, relevans, aktualitet og fuldstændighed.
- Behandlingens sikkerhed, herunder underretning omkring brud på persondatasikkerheden.
- Behandling af følsomme oplysninger tillades kun med passende garantier i medfør af lovgivningen.
- Lagringsperioder: Personoplysninger må ikke lagres i længere tid end nødvendigt, eller hvad der er passende.
- Adgangs- og berigtigelsesrettigheder: Alle enkeltpersoner er under visse betingelser berettiget til adgang til deres personoplysninger og vil kunne anmode om, at oplysningerne berigtiges, hvis de er ukorrekte.

([809]) Aftale mellem Amerikas Forenede Stater og Den Europæiske Union om beskyttelse af personoplysninger i forbindelse med forebyggelse, efterforskning, opdagelse og retsforfølgning af strafbare handlinger af 18. maj 2016, (OR.en) 8557/16, artikel 3, stk. 1. Se også meddelelsen fra Kommissionen om databeskyttelsesaftalen mellem EU og USA af 26. maj 2010, MEMO/10/216, og Europa-Kommissionens pressemeddelelse (2010) om høje standarder i aftalen mellem EU og USA om beskyttelse af personoplysninger af 26. maj 2010, IP/10/609.

- Automatiske afgørelser kræver passende garantier, inklusive muligheden for menneskelig indgriben.

- Effektivt tilsyn, herunder samarbejde mellem europæiske og amerikanske tilsynsmyndigheder.

- retslig prøvelse og håndhævelse: EU-borgere har ret ([810]) til at anmode om retslig prøvelse ved amerikanske domstole i sager, hvor de amerikanske myndigheder nægter adgang eller berigtigelse eller på ulovlig vis videregiver borgernes personoplysninger.

Der er også sat et system op jf. »paraplyaftalen« til at underrette den kompetente tilsynsmyndighed i medlemsstaten for berørte enkeltpersoner omkring eventuelle brud på databeskyttelsen, om nødvendigt. Retsgarantierne, som aftalen indeholder, sikrer en ensartet behandling af EU-borgere i USA, når der er en krænkelse af privatlivets fred ([811]).

8.3.1. Databeskyttelse i EU's retslige og retshåndhævende myndigheder

Europol

Europol, EU's retshåndhævende myndighed, har hovedkvarter i Haag og har etableret nationale enheder (ENU'er) i hver medlemsstat. Europol blev oprettet i 1998. Dets nuværende retlige status som en EU-institution er baseret på forordningen om Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol-forordningen) ([812]). Europol støtter bestræbelserne på at forebygge og efterforske organiseret kriminalitet, terrorisme og andre former for alvorlig kriminalitet (jf. bilaget

([810]) Den amerikanske Judicial Redress Act blev undertegnet af præsident Obama den 24. februar 2016.

([811]) Den Europæiske Tilsynsførende for Databeskyttelse: udstedt en udtalelse om aftalen mellem USA og EU, hvor denne bl.a. foreslår følgende ændringer: 1) tilføjelse af »til de særlige formål, som de blev overført til« til den artikel, som vedrører, at oplysninger ikke lagres i længere tid end nødvendigt og passende, og 2) udelukkelse af overførsler af følsomme oplysninger som bulkdata, hvilket måske er muligt. Se Den Europæiske Tilsynsførende for Databeskyttelse, Udtalelse 1/2016, *foreløbig udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om aftalen mellem Amerikas Forenede Stater og Den Europæiske Union om beskyttelse af personoplysninger i forbindelse med forebyggelse, opsporing, afsløring og retsforfølgelse i straffesager*, § 35.

([812]) Europa-Parlamentets og Rådets forordning (EU) 2016/794 af 11. maj 2016 om Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) og om erstatning og ophævelse af Rådets afgørelse 2009/371/RIA, 2009/934/RIA, 2009/935/RIA, 2009/936/RIA og 2009/968/RIA, EUT L 135 af 24. maj 2016, s. 53.

til Europol-forordningen), som berører to eller flere medlemsstater. Europol opnår dette ved at udveksle oplysninger og fungere som EU's informationscenter, som leverer efterretningsanalyser og trusselsvurderinger.

For at opfylde sine formål har Europol udviklet Europols informationssystem, som tilvejebringer en database, hvor medlemsstaterne via deres ENU'er kan udveksle strafferetlige efterretninger og oplysninger. Europols informationssystem kan bruges til at give adgang til oplysninger, som vedrører personer, der er mistænkt eller dømt for en strafbar handling, der er underlagt Europols kompetence, eller personer, hvor der er konkrete indicier for, at de vil begå en sådan strafbar handling. Europol og ENU'er kan indtaste data direkte i Europols informationssystem og hente data fra det. Kun den part, der har indtastet oplysningerne i systemet, kan redigere, berigtige eller slette dem. EU-organer, tredjelande og internationale organisationer kan også forsyne Europol med oplysninger.

Europol kan også indhente oplysninger, inklusive personoplysninger, fra offentligt tilgængelige kilder, såsom internettet. Overførsler af personoplysninger til EU-organer tillades kun, hvis det er nødvendigt til udførelse af Europols eller det modtagende EU-organs opgave. Overførsler af personoplysninger til tredjelande eller internationale organisationer tillades kun, hvis Europa-Kommissionen beslutter, at det pågældende land eller den internationale organisation sikrer et tilstrækkeligt databeskyttelsesniveau (»afgørelse om tilstrækkeligheden af beskyttelsesniveauet«), eller hvis der er en international aftale eller samarbejdsaftale. Europol kan modtage og behandle personoplysninger fra private parter og privatpersoner under de strenge betingelser, at disse oplysninger overføres af en ENU i medfør af dennes nationale lovgivning, af et kontaktpunkt i et tredjeland eller en international organisation, hvormed et samarbejde er indgået igennem en samarbejdsaftale, eller af en myndighed i et tredjeland eller en international organisation, som er underlagt en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, eller hvormed EU har indgået en international aftale. Alle informationsudvekslinger foretages igennem et netværksprogram til sikker informationsudveksling (SIENA).

Der er oprettet specialiserede centre inden for Europol som reaktion på nye udviklinger. Det Europæiske Center for Bekæmpelse af Cyberkriminalitet blev etableret inden for Europol i 2013 ([813]). Centret fungerer som europæisk knudepunkt for information om cyberkriminalitet. Det bidrager til at sikre hurtigere reaktioner i tilfælde

([813]) Se også EDPS (2012), *Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om meddelelse fra Kommissionen til Rådet og Europa-Parlamentet om oprettelse af et europæisk center til bekæmpelse af it-kriminalitet*, Bruxelles, 29. juni 2012.

af kriminalitet på internettet, udvikler og indfører digital retsmedicinsk teknologi og leverer bedste praksis inden for efterforskning af cyberkriminalitet. Centret fokuserer på cyberkriminalitet, der:

- begås af organiserede grupper med det formål at opnå store ulovlige fortjenester, såsom internetbedrageri
- forårsager alvorlige skader for ofrene, såsom seksuel udnyttelse af børn på internettet
- i alvorlig grad påvirker kritisk infrastruktur eller informationssystemer i EU.

Det Europæiske Center for Terrorbekæmpelse (ECTC) blev oprettet i januar 2016 for at yde operationel støtte til medlemsstater ved undersøgelser vedrørende terrorhandlinger. Det krydstjekker aktuelle driftsdata med oplysninger i Europols besiddelse, hvilket hurtigt fremhæver økonomiske ledetråde, og analyserer alle tilgængelige efterforskningsdetaljer for at bistå med at danne et struktureret billede af et terroristnetværk ([814]).

Det Europæiske Center vedrørende Migrantsmugling (EMSC) blev etableret i februar 2016 efter en samling i Rådet i november 2015 for at støtte medlemsstater med at udpege og nedbryde kriminelle netværk, som er involveret i migrantsmugling. Det fungerer som et knudepunkt for information, der støtter kontorerne for Den Europæiske Unions Taskforce for Regionale Strategier i Catania (Italien) og Piraeus (Grækenland), som hjælper nationale myndigheder på flere områder, herunder udveksling af efterretninger, strafferetlige efterforskninger og retsforfølgelse af kriminelle menneskesmuglingsnetværk ([815]).

Databeskyttelsesordningen, som styrer Europols aktiviteter, forstærkes og trækker på principperne i forordningen om databeskyttelse inden for EU-institutionerne ([816]) og stemmer også overens med databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder, den moderniserede konvention 108 og henstillingen om politiets brug af personoplysninger.

([814]) Se Europols websted om ECTC.

([815]) Se Europols websted om EMSC.

([816]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001).

Behandling af personoplysninger om ofre for strafbare handlinger, vidner eller andre personer, som kan give oplysninger vedrørende strafbare handlinger, samt om personer under 18 år er tilladt, hvis det er strengt nødvendigt for og står i rimeligt forhold til forebyggelse eller bekæmpelse af kriminalitet, som er omfattet af Europols målsætninger ([817]). Behandlingen af følsomme personoplysninger forbydes, medmindre det er strengt nødvendigt for og står i rimeligt forhold til forebyggelse eller bekæmpelse af kriminalitet, som er omfattet af Europols målsætninger, og hvis disse oplysninger supplerer andre personoplysninger, der behandles af Europol ([818]). I begge tilfælde er det kun Europol, som kan tilgå de pågældende oplysninger ([819]).

Opbevaring af oplysninger tillades kun i en fornøden og forholdsmæssig tidsperiode og deres fortsatte opbevaring er genstand for en kontrol hvert tredje år. Hvis det ikke besluttes fortsat at opbevare personoplysningerne, skal de automatisk slettes efter tre år ([820]).

Europol har under visse betingelser lov til at videregive personoplysninger direkte til et EU-organ, til en myndighed i et tredjeland eller til en international organisation ([821]). Databrud skal, hvis der er sandsynlighed for, at de i alvorlig grad og på krænkende vis påvirker de berørte registreredes rettigheder og frihedsrettigheder, meddeles til registrerede uden unødig forsinkelse ([822]). På medlemsstatsniveau udpeges en national tilsynsmyndighed til at overvåge Europols behandling af personoplysninger ([823]).

EDPS er ansvarlig for at overvåge og sikre beskyttelse af fysiske personers grundlæggende rettigheder i forbindelse med Europols behandling af personoplysninger og for at rådgive Europol og registrerede om alle spørgsmål vedrørende behandling af personoplysninger. Til dette formål fungerer EDPS som et undersøgelses- og klageorgan og arbejder i tæt samarbejde med de nationale tilsynsmyndigheder ([824]). EDPS og de nationale tilsynsmyndigheder vil mødes mindst to gange om året i samarbejdsudvalget, som har en rådgivende funktion ([825]). Medlemsstater er forpligtet

([817]) Europol-forordningen, artikel 30, stk. 1.

([818]) *Ibid.*, artikel 30, stk. 2.

([819]) *Ibid.*, artikel 30, stk. 3.

([820]) *Ibid.*, artikel 31.

([821]) *Ibid.*, henholdsvist artikel 24 og 25.

([822]) *Ibid.*, artikel 35.

([823]) Europol-forordningen, artikel stk. 42.

([824]) *Ibid.*, artikel 43 og 44.

([825]) *Ibid.*, artikel 45.

til at etablere en tilsynsmyndighed, som i medfør af dens nationale lovgivning har kompetence til at føre tilsyn med lovligheden af den pågældende medlemsstats videregivelse til, indhentning fra samt meddelelse til Europol af personoplysninger ([826]). Medlemsstater skal også sikre, at den nationale tilsynsmyndighed kan fungere fuldstændigt uafhængigt under udførelse af sine opgaver og pligter i medfør af Europol-forordningen ([827]). Europol fører logninger over og dokumenterer sine databehandlingsaktiviteter med henblik på at bekræfte lovligheden af og føre egenkontrol over disse samt sikre dataenes integritet og sikkerhed. Disse logninger indeholder oplysninger om automatiske databehandlingssystemers behandlingsaktiviteter vedrørende indsamling, ændring, adgang, videregivelse, samkøring og sletning ([828]).

En klage over en afgørelse truffet af EDPS kan indbringes for EU-Domstolen ([829]). Enhver, der har lidt skade som følge af ulovlig behandling af oplysninger, har ret til erstatning for den forvoldte skade enten fra Europol eller fra den ansvarlige medlemsstat ved at indbringe en sag for EU-Domstolen i det første tilfælde eller for den kompetente nationale domstol i det andet tilfælde ([830]). Derudover kan en specialiseret Gruppe for Fælles Parlamentarisk Kontrol for de nationale parlamenter og Europa-Parlamentet kontrollere Europols aktiviteter ([831]). Enhver har ret til at få adgang til personoplysninger, som Europol opbevarer om vedkommende, samt en ret til at anmode om, at disse personoplysninger kontrolleres, berigtiges eller slettes. Dette kan være underlagt undtagelser og begrænsninger.

Eurojust

Eurojust, som blev oprettet i 2002, er et EU-organ med hovedkvarter i Haag. Det fremmer det retlige samarbejde under efterforskninger og retsforfølgninger vedrørende grov kriminalitet, der berører mindst to medlemsstater ([832]). Eurojust har kompetence til at:

([826]) *Ibid.*, artikel 42, stk. 1.

([827]) *Ibid.*, artikel 42, stk. 1.

([828]) *Ibid.*, artikel 40.

([829]) *Ibid.*, artikel 48.

([830]) *Ibid.*, artikel 50.

([831]) *Ibid.*, artikel 51.

([832]) Rådet for Den Europæiske Union (2002), Rådets afgørelse 2002/187/RIA af 28. februar 2002 om oprettelse af Eurojust for at styrke bekæmpelsen af grov kriminalitet, EFT L 63 af 6. marts 2002; Rådet for Den Europæiske Union (2003), Rådets afgørelse 2003/659/RIA af 18. juni 2003 om ændring af afgørelse 2002/187/RIA om oprettelse af Eurojust for at styrke bekæmpelsen af grov kriminalitet (EUT L 44 af 29.10.2003) og Rådet for Den Europæiske Union (2009), Rådets afgørelse 2009/426/RIA af 16. december 2008 om styrkelse af Eurojust og om ændring af afgørelse 2002/187/RIA om oprettelse af Eurojust for at styrke bekæmpelsen af grov kriminalitet (EUT L 138 af 4.6.2009) (Eurojust-afgørelserne).

- fremme og forbedre koordineringen af efterforskninger og retsforfølgninger mellem de forskellige medlemsstaters kompetente myndigheder

- medvirke til at fuldbyrde anmodninger og afgørelser om retligt samarbejde.

Eurojusts funktioner varetages af nationale medlemmer. Hver medlemsstat udstationerer én dommer eller anklager ved Eurojust. Disse personer er, for så vidt angår deres status, underlagt deres medlemsstaters nationale lovgivning og bemyndiges med de nødvendige kompetencer til at udføre de opgaver, der kræves for at fremme og forbedre det retlige samarbejde. De nationale medlemmer udfører desuden særlige Eurojust-opgaver som et kollegium.

Eurojust kan behandle personoplysninger i det omfang, det er nødvendigt for at opfylde dets mål. Dette er dog begrænset til specifikke oplysninger vedrørende personer, der mistænkes for at have begået eller deltaget i en strafbar handling, som henhører under Eurojusts kompetence, eller som er dømt for en sådan strafbar handling. Eurojust kan også behandle visse oplysninger vedrørende vidner til eller ofre for strafbare handlinger, som henhører under Eurojusts kompetence ([833]). I undtagelsestilfælde kan Eurojust dog også i et begrænset tidsrum behandle mere omfattende personoplysninger vedrørende omstændighederne omkring en lovovertrædelse, såfremt de er relevante for en igangværende efterforskning. Inden for sit kompetenceområde kan Eurojust samarbejde med andre EU-institutioner, -organer og -agenturer og udveksle personoplysninger med dem. Eurojust kan også samarbejde og udveksle personoplysninger med tredjelande og organisationer.

Eurojust skal i forbindelse med databeskyttelse sikre et beskyttelsesniveau, som mindst svarer til principperne i den moderniserede konvention 108 og efterfølgende ændringer heraf. I forbindelse med dataudveksling skal særlige regler og begrænsninger overholdes, som er fastlagt enten ved en samarbejdsaftale eller arbejdsaftale i overensstemmelse med Rådets afgørelser om Eurojust og Eurojusts databeskyttelsesregler ([834]).

Der er oprettet en uafhængig fælles kontrolinstans under Eurojust, som har til opgave at overvåge Eurojusts behandling af personoplysninger. Personer kan klage til Den Fælles Kontrolinstans, hvis de ikke er tilfredse med Eurojusts besvarelse af en anmodning om indsigt, berigtigelse, blokering eller sletning af personoplysninger.

([833]) Konsolideret udgave af Rådets afgørelse 2002/187/RIA, som ændret ved Rådets afgørelse 2003/659/RIA og Rådets afgørelse 2009/426/RIA, artikel 15, stk. 2.

([834]) Eurojusts forretningsordens bestemmelser for behandling og beskyttelse af personoplysninger (EUT C 68/01, 19.3.2005, s. 1).

Hvis Eurojust behandler personoplysninger ulovligt, er Eurojust ansvarlig i henhold til den nationale lovgivning i den medlemsstat, hvor det har sit hovedkvarter, dvs. Nederlandene, for den skade, der påføres den registrerede.

Fremtidsudsigter

Europa-Kommissionen fremførte et udkast til en forordning om at reformere Eurojust i juli 2013. Dette udkast blev ledsaget af et forslag om at oprette en europæisk anklagemyndighed (se nedenstående). Denne forordning er rettet mod at strømline funktioner og struktur, så de er i overensstemmelse med Lissabontraktaten. Derudover er reformens mål at fastlægge en klar adskilning af Eurojusts operationelle opgaver, som udføres af Eurojusts kollegie, og dennes administrative opgaver. Dette vil også give medlemsstater mulighed for at fokusere mere på de operationelle opgaver. En ny direktion oprettes for at bistå kollegiet med udførelsen af administrative opgaver ([835]).

Den Europæiske Anklagemyndighed

Medlemsstater har enekompetence til at retsforfølge de strafbare handlinger bedrageri og forkert anvendelse af EU-budgettet, hvilket også har potentielle grænseoverskridende konsekvenser. Det er grundet den igangværende finanskrise blevet vigtigere at efterforske, retsforfølge og dømme gerningsmændene til sådanne lovovertrædelser ([836]). Europa-Kommissionen har udfærdiget et forslag til en forordning om oprettelse af en uafhængig europæisk anklagemyndighed (EPPO ([837]) med det formål at bekæmpe lovovertrædelser, som påvirker EU's økonomiske interesser. EPPO oprettes via den forbedrede samarbejdsprocedure, som tillader, at mindst ni medlemsstater indleder et forstærket samarbejde inden for EU-sammenhæng, uden at de andre EU-lande involveres ([838]). Belgien, Bulgarien, Cypern, Estland, Finland, Frankrig, Grækenland, Kroatien, Letland, Litauen, Luxembourg, Portugal, Rumænien, Slovakiet, Slovenien, Spanien, Den Tjekkiske

([835]) Se Europa-Kommissionens webside om Eurojust.

([836]) Se Europa-Kommissionen (2013), forslag til Rådets forordning om oprettelse af en europæisk anklagemyndighed, COM(2013) 534 final, Bruxelles, 17. juli 2013, s. 1, og Kommissionens webside om EPPO.

([837]) Europa-Kommissionen (2013), forslag til Rådets forordning om oprettelse af en europæisk anklagemyndighed, COM(2013) 534 final, Bruxelles, 17. juli 2013.

([838]) Traktaten om Den Europæiske Unions funktionsmåde, artikel 86, stk. 1, og artikel 329, stk. 1.

Republik og Tyskland har alle sluttet sig til det forstærkede samarbejde. Italien og Østrig har meddelt, at de agter at tilslutte sig samarbejdet ([839]).

EPPO vil have kompetencer til at efterforske og retsforfølge EU-svindel og andre forbrydelser, som påvirker EU's finansielle interesser, med henblik på effektivt at koordinere efterforskninger og retsforfølgelser på tværs af de forskellige nationale retsordener og på at forbedre brugen af ressourcer og udvekslingen af oplysninger på europæisk niveau ([840]).

EPPO skal ledes af en europæisk anklager, og der vil være mindst én delegeret europæisk anklager i hver medlemsstat med ansvar for at udføre efterforskning og retsforfølgning i den medlemsstat.

Forslaget fastlægger stærke garantier til at sikre rettighederne for personer, som er omfattet af EPPO's efterforskninger som fastlagt i national lovgivning, EU-retten og EU's charter om grundlæggende rettigheder. Efterforskningsmæssige foranstaltninger, som for det meste vedrører grundlæggende rettigheder, kræver forudgående godkendelse ved en national domstol ([841]). EPPO's efterforskninger vil være genstand for domstolsprøvelse ved de nationale domstole ([842]).

Forordningen om databeskyttelse inden for EU-institutionerne ([843]) finder anvendelse for EPPO's behandling af administrative personoplysninger. Ved behandling af personoplysninger i forbindelse med operationelle spørgsmål, ligesom Europol, vil EPPO have en selvstændig databeskyttelsesordning lig den, som styrer Europols og Eurojusts aktiviteter, da udøvelsen af EPPO's funktioner vil omfatte behandling af personoplysninger med retshåndhævende myndigheder og anklagemyndigheder på medlemsstatsniveau. EPPO's databeskyttelsesregler er derfor næsten identiske med reglerne i databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder. I henhold til forslaget om oprettelse af EPPO skal behandling

([839]) Se EU-Rådet (2017), »20 medlemslande når til enighed om de nærmere bestemmelser i forbindelse med oprettelsen af Den Europæiske Anklagemyndighed (EPPO)«, pressemeddelelse, 8. juni 2017.

([840]) Europa-Kommissionen (2013), forslag til Rådets forordning om oprettelse af en europæisk anklagemyndighed, COM(2013) 534 final, Bruxelles, 17. juli 2013, s. 1 og 51. Se også Kommissionens webside om EPPO.

([841]) Europa-Kommissionen (2013), forslag til Rådets forordning om oprettelse af en europæisk anklagemyndighed, COM(2013) 534 final, Bruxelles, 17. juli 2013, artikel 26, stk. 4.

([842]) *Ibid*., artikel 36.

([843]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, EFT L 8 af 12. januar 2001.

af personoplysninger overholde principperne for lovlighed, rimelighed og gennemsigtighed, formålsbegrænsning, dataminimering, nøjagtighed, integritet og fortrolighed. EPPO skal så vidt muligt tydeligt skelne mellem personoplysninger tilhørende forskellige typer af registrerede, såsom personer, der er dømt for en strafbar handling, personer, der bare er mistænkte, ofre og vidner. Den skal også forsøge at bekræfte kvaliteten af behandlede personoplysninger og så vidt muligt skelne mellem personoplysninger baseret på fakta og personoplysninger baseret på personlige vurderinger.

Forslaget indeholder bestemmelser om registreredes rettigheder, navnlig rettighederne til information, til adgang til deres personoplysninger og til berigtigelse, sletning og begrænsning af behandling, og fastlægger, at sådanne rettigheder også kan udøves indirekte igennem EDPS. Det omfatter også principperne om behandlingssikkerhed og ansvarlighed, som kræver, at EPPO gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der er passende til de risici, som behandlingen medfører, for at registrere alle behandlingsaktiviteter og for at udføre en konsekvensanalyse af databeskyttelsen inden behandlingen, når en form for behandling (for eksempel behandling, der indebærer brugen af nye teknologier) med sandsynlighed medfører en høj risiko for enkeltpersoners rettigheder. Endelig fastsætter forslaget, at kollegiet udpeger en databeskyttelsesansvarlig, som skal inddrages på korrekt vis i alle spørgsmål vedrørende beskyttelse af personoplysninger og skal sikre, at EPPO overholder den gældende databeskyttelseslovgivning.

8.3.2. Databeskyttelse i de fælles informationssystemer på EU-plan

Ud over dataudveksling mellem medlemsstaterne og oprettelsen af særlige EU-myndigheder med henblik på at bekæmpe grænseoverskridende kriminalitet, såsom Europol, Eurojust og EPPO, er der på EU-plan indført en række fælles informationssystemer til at muliggøre og fremme samarbejde og dataudveksling mellem kompetente nationale myndigheder og EU-myndigheder til særlige formål på områderne for grænsekontrol, immigration og asyl og told. Da Schengenområdet først blev oprettet igennem en international aftale, som fungerede uafhængigt fra EU-retten, udviklede man Schengeninformationssystemet (SIS) ud fra multilaterale aftaler, og dette system blev derefter lagt ind under EU-retten. Visuminformationssystemet (VIS), Eurodac, Eurosur og toldinformationssystemet (CIS) blev oprettet som instrumenter, der er underlagt EU-retten.

Tilsynet med disse systemer foretages af både de nationale tilsynsmyndigheder og EDPS. For at sikre et højt beskyttelsesniveau samarbejder disse myndigheder i særlige konsultationsgrupper (SKG), hvilket henviser til følgende store IT-systemer: 1) Eurodac, 2) visuminformationssystemet, 3) Schengeninformationssystemet, 4) toldinformationssystemet og 5) informationssystemet for det indre marked ([844]). GKT'erne mødes typisk to gange om året under ledelse af en valgt formand og vedtager retningslinjer, diskuterer grænseoverskridende sager eller vedtager fælles tilsynsrammer.

Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) ([845]), som blev oprettet i 2012, er ansvarlig for den operationelle forvaltning af anden generation af Schengeninformationssystemet (SIS II), visuminformationssystemet (VIS) og Eurodac. Hovedopgaven for eu-LISA er at sikre den effektive, sikre og løbende drift af IT-systemer. Det er også ansvarligt for vedtagelsen af fornødne foranstaltninger til at sikre systemernes og dataenes sikkerhed.

Schengeninformationssystemet

I 1985 tiltrådte flere medlemsstater af de tidligere Europæiske Fællesskaber aftalen mellem staterne i Den Økonomiske Union Benelux, Tyskland og Frankrig om gradvis ophævelse af kontrollen ved de fælles grænser (Schengenaftalen) med henblik på at skabe et område med fri bevægelighed for personer uhindret af grænsekontrol inden for Schengenområdet ([846]). For at opveje den trussel mod den offentlige sikkerhed, der kunne opstå som følge af åbne grænser, blev der indført yderligere grænsekontrol ved Schengenområdets ydre grænser, og der blev etableret et tæt samarbejde mellem landenes politi og retsmyndigheder.

Som følge af yderligere landes tiltræden til Schengenaftalen blev Schengensystemet endeligt integreret i EU's retlige ramme med Amsterdamtraktaten ([847]). Denne

([844]) Se Den Europæiske Tilsynsførende for Databeskyttelses websted om koordinering af tilsyn.

([845]) Europa-Parlamentets og Rådets forordning (EU) nr. 1077/2011 af 25. oktober 2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store IT-systemer inden for området med frihed, sikkerhed og retfærdighed, EUT L 286 af 1. november 2011.

([846]) Aftale mellem regeringerne for staterne i Den Økonomiske Union Benelux, Forbundsrepublikken Tyskland og Den Franske Republik om gradvis ophævelse af kontrollen ved de fælles grænser (EFT L 239 af 22.9.2000).

([847]) De Europæiske Fællesskaber (1997), Amsterdamtraktaten om ændring af traktaten om Den Europæiske Union, traktaterne om oprettelse af De Europæiske Fællesskaber og visse tilknyttede akter (EFT C 340 af 10.11.1997).

beslutning blev gennemført i 1999. Den nyeste version af Schengeninformationssystemet, det såkaldte »SIS II«, blev sat i drift den 9. april 2013. Det betjener nu de fleste af EU's medlemsstater ([848]) samt Island, Liechtenstein, Norge og Schweiz ([849]). Europol og Eurojust har også adgang til SIS II.

SIS II består af et centralt system (C-SIS), et nationalt system (N-SIS) i hver medlemsstat og en kommunikationsinfrastruktur mellem det centrale system og de nationale systemer. C-SIS indeholder visse data, som medlemsstaterne har indført om personer og genstande. SIS bruges af de nationale grænsekontroller, politi, toldvæsenet samt visum- og retsmyndigheder i hele Schengenområdet. Hver medlemsstat driver en national udgave af C-SIS, den nationale del af Schengeninformationssystemet: »N-SIS«, som løbende ajourføres, således at også C-SIS ajourføres. SIS har forskellige typer af indberetninger:

- Personen har ikke ret til at rejse til eller opholde sig i Schengenområdet.
- Personen eller genstanden er eftersøgt af retslige eller retshåndhævende myndigheder (f.eks. europæiske arrestordrer og anmodninger om diskret kontrol).
- Personen er meldt savnet.
- Genstande, som f.eks. pengesedler, motorkøretøjer, skydevåben og identitetspapirer, er meldt stjålet eller forsvundet.

I tilfælde af en indberetning iværksættes opfølgende aktiviteter via SIRENE-kontoret. SIS II har nye funktioner, herunder f.eks. mulighed for at indlæse biometriske data, såsom fingeraftryk og fotografier; eller nye kategorier af indberetninger, såsom stjålne både, luftfartøjer, containere eller betalingsmidler; forbedrede indberetninger om personer og genstande og kopier af europæiske arrestordrer vedrørende personer, der begæres anholdt med henblik på overgivelse/udlevering.

([848]) Kroatien, Cypern og Irland er igang med at gennemføre forberedende aktiviteter til at blive integreret i SIS II, men er endnu ikke en del heraf. Se oplysninger om Schengeninformationssystemet på webstedet for Europa-Kommissionens Generaldirektorat for Migration og Indre Anliggender.

([849]) Europa-Parlamentets og Rådets forordning (EF) nr. 1987/2006 af 20. december 2006 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (EUT L 381 af 28.12.2006), og Rådets afgørelse 2007/533/RIA af 12. juni 2007 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (EUT L 205 af 7.8.2007).

SIS II er baseret på to retsakter, som supplerer hinanden: SIS II-afgørelsen ([850]) og SIS II-forordningen ([851]). EU-lovgiveren anvendte forskellige lovgrundlag for afgørelsens og forordningens vedtagelse. Afgørelsen vedrører brugen af SIS II til formål omfattet af politisamarbejde og retligt samarbejde i kriminalsager (EU's tidligere tredje søjle). Forordningen finder anvendelse for indberetningsprocedurer, som hører under visa, asyl, immigration og andre politikker vedrørende den frie bevægelighed for personer (den tidligere første søjle). Indberetningsprocedurerne for hver søjle skulle registreres ved særskilte retsakter, da de to retsakter blev vedtaget inden Lissabontraktaten og ophævelsen af søjlestrukturen.

Begge retsakter indeholder regler om databeskyttelse. SIS II-afgørelsen forbyder behandlingen af følsomme oplysninger ([852]). Behandlingen af personoplysninger skal være underlagt den moderniserede konvention 108 ([853]). Derudover har personer ret til at få adgang til personoplysninger vedrørende dem, som er indlæst i SIS II ([854]).

SIS II-forordningen regulerer betingelser og procedurer for indlæsning og behandling af indberetninger vedrørende nægtelse af indrejse eller ophold for ikke-EU-borgere. Den fastlægger også regler for udveksling af supplerende og yderligere oplysninger i forbindelse med indrejse til eller ophold i en medlemsstat ([855]). Denne forordning indeholder også regler om databeskyttelse. Følsomme datakategorier, som er angivet i artikel 9, stk. 1, i den generelle forordning om databeskyttelse, må ikke behandles ([856]). SIS II-forordningen indeholder også visse rettigheder for den registrerede, som er:

- retten til indsigt i personoplysninger vedrørende sig selv ([857])
- retten til at få rettet oplysninger om sig selv, der er ukorrekte ([858])

([850]) Rådets afgørelse 2007/533/RIA af 12. juni 2007 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (EUT L 205 af 7.8.2007).

([851]) Europa-Parlamentets og Rådets forordning (EF) nr. 1987/2006 af 20. december 2006 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (EUT L 381 af 28.12.2006).

([852]) SIS II-afgørelsen, artikel 56; SIS II-forordningen, artikel 40.

([853]) SIS II-afgørelsen, artikel 57.

([854]) SIS II-afgørelsen, artikel 58; SIS II-forordningen, artikel 41.

([855]) SIS II-forordningen, artikel 2.

([856]) *Ibid*., artikel 40.

([857]) *Ibid*., artikel 41, stk. 1.

([858]) *Ibid*., artikel 41, stk. 5.

- retten til få slettet oplysninger, der lagres ulovligt ([859])

- retten til at blive informeret, når der er en indberetning om den registrerede. Disse oplysninger gives skriftligt sammen med en kopi eller en henvisning til den nationale afgørelse, der ligger til grund for indberetningen ([860]).

Retten til at blive informeret er ikke gældende, hvis 1) personoplysningerne ikke er indsamlet hos den registrerede, og information viser sig umulig eller er uforholdsmæssig vanskelig, 2) den registrerede allerede har informationerne, eller 3) hvis national lovgivning tillader en begrænsning, bl.a. for at beskytte den nationale sikkerhed eller forebygge strafbare handlinger ([861]).

For både SIS II-afgørelsen og SIS II-forordningen kan enkeltpersoners adgangsrettigheder i forbindelse med SIS II udøves i alle medlemsstater og vil blive håndteret i medfør af den pågældende medlemsstats nationale lovgivning ([862]).

Eksempel: I sagen *Dalea mod Frankrig* ([863]) blev sagsøgeren nægtet visum til indrejse i Frankrig, da de franske myndigheder i Schengeninformationssystemet havde indberettet, at han burde nægtes indrejsetilladelse. Sagsøgeren anmodede forgæves de franske databeskyttelsesmyndigheder og i sidste ende Conseil d'État om indsigt i samt berigtigelse eller sletning af oplysningerne. EMD fastslog, at indberetningen af sagsøgeren i Schengeninformationssystemet havde været i overensstemmelse med loven og havde forfulgt et legitimt mål om at beskytte den nationale sikkerhed. Da sagsøgeren ikke kunne bevise, at han faktisk led skade, fordi han blev nægtet indrejse i Schengenområdet, og da der var indført tilstrækkelige foranstaltninger til at beskytte ham mod vilkårlige afgørelser, havde indgrebet i hans ret til respekt for privatlivet været rimeligt. Sagsøgerens klage i henhold til artikel 8 blev derfor afvist.

Den kompetente nationale tilsynsmyndighed i hver medlemsstat fører tilsyn med det nationale N-SIS. Den nationale tilsynsmyndighed skal sikre, at der gennemføres

([859]) *Ibid.*, artikel 41, stk. 5.

([860]) *Ibid.*, artikel 42, stk. 1.

([861]) *Ibid.*, artikel 42, stk. 2.

([862]) SIS II-forordningen, artikel 41, stk. 1, og SIS II-forordningen, artikel 58.

([863]) EMD, *Dalea mod Frankrig*, nr. 964/07, 2. februar 2010.

en revision af databehandlingerne i det nationale N-SIS mindst hvert fjerde år ([864]). De nationale tilsynsmyndigheder og EDPS samarbejder og koordinerer tilsynet med N-SIS, og EDPS er ansvarlig for tilsynet med C-SIS. Af hensyn til gennemsigtigheden forelægges en fælles aktivitetsrapport for Europa-Parlamentet, Rådet og eu-LISA hvert andet år. SIS II's særlige konsultationsgruppe (SKG) blev oprettet til at sikre koordinering af SIS' tilsyn, og den mødes to gange om året. Gruppen består af EDPS og repræsentanter for tilsynsmyndighederne i de medlemsstater, som har implementeret SIS II, samt Island, Liechtenstein, Norge og Schweiz, da SIS også er gældende for dem grundet deres Schengen-medlemskab ([865]). Cypern, Irland og Kroatien er endnu ikke en del af SIS II og kan derfor kun deltage som observatører til SKG. I forbindelse med SKG samarbejder SKG, EDPS og de nationale tilsynsmyndigheder aktivt ved at udveksle oplysninger, hjælpe hinanden med udførelsen af audits og inspektioner, udforme harmoniserede forslag til fælles løsninger til potentielle problemer og ved at sprede opmærksomhed om databeskyttelsesrettigheder ([866]). SIS II's SKG vedtager også retningslinjer til at hjælpe registrerede. Ét eksempel er vejledningen til at hjælpe registrerede med at udøve deres ret til aktindsigt ([867]).

Fremtidsudsigter

I 2016 gennemførte Europa-Kommissionen en evaluering af SIS ([868]), som viste, at nationale mekanismer var oprettet, hvormed registrerede kunne få adgang til, berigtige og slette deres personoplysninger i SIS II eller kræve erstatning i tilfælde af ukorrekte data. Europa-Kommissionen har for at forbedre effektiviteten af SIS II forelagt tre forslag til forordninger:

- en forordning om oprettelse, drift og brug af SIS på området ind- og udrejsekontrol, som ophæver SIS II-forordningen

- en forordning om oprettelse, drift og brug af SIS på området politisamarbejde og strafferetligt samarbejde, som, bl.a., ophæver SIS II-afgørelsen

([864]) SIS II-forordningen, artikel 60, stk. 2.

([865]) Se Den Europæiske Tilsynsførende for Databeskyttelses websted om Schengeninformationssystemet.

([866]) SIS II-forordningen, artikel 46, og SIS II-afgørelsen, artikel 62.

([867]) Se SIS II's SKG, *The Schengen Information System. Vejledning i udøvelse af retten til aktindsigt*, tilgængelig på EDPS' websted.

([868]) Europa-Kommissionen (2016), rapport fra Kommissionen til Europa-Parlamentet og Rådet om evalueringen af anden generation af Schengeninformationssystemet (SIS II) i overensstemmelse med artikel 24, stk. 5, artikel 43, stk. 3, og artikel 50, stk. 5, i forordning (EF) nr. 1987/2006 og artikel 59, stk. 3, og artikel 66, stk. 5, i afgørelse 2007/533/RIA, COM(2016) 880 final, Bruxelles, 21. december 2016.

- en forordning om brug af SIS i forbindelse med tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold.

Det er vigtigt at bemærke, at forslagene tillader behandling af andre kategorier af biometriske data – udover fotografier og fingeraftryk, som allerede indgår i den gældende SIS II-ordning. Ansigtsbilleder, håndfladeaftryk og DNA-profiler vil også blive lagret i SIS-databasen. Selvom SIS II-forordningen og SIS II-afgørelsen fastsatte en mulighed for at foretage søgninger med fingeraftryk til identifikation af en person, gør forslagene denne søgning obligatorisk, hvis personens identitet ikke kan fastslås på nogen anden måde. Ansigtsbilleder, fotografier og håndfladeaftryk vil blive brugt til at søge i systemet og identificere personer, når dette bliver teknisk muligt. De nye regler om biometriske identifikatorer udgør særlige risici for enkeltpersoners rettigheder. I sin udtalelse om Kommissionens forslag ([869]) bemærkede EDPS, at biometriske data er meget følsomme, og deres indførelse i så stor en database bør baseres på en evidensbaseret vurdering af behovet for at inkludere dem i SIS. Med andre ord skal nødvendigheden af at behandle de nye identifikatorer dokumenteres. EDPS overvejede også, at der er et behov for i større grad at præcisere, hvilke oplysningsformer som kan inkluderes i DNA-profilen. Da DNA-profilen kan indeholde følsomme oplysninger (det mest nævneværdige eksempel ville være oplysninger, som afslører sundhedsproblemer), bør DNA-profilerne, som er lagret i SIS, kun indeholde: de minimale oplysninger, som er strengt nødvendige til identifikation af de forsvundne personer, og ikke udtrykkelige sundhedsoplysninger, racemæssig oprindelse og alle andre følsomme oplysninger ([870]). Forslagene fastlægger dog yderligere garantier til at begrænse indsamlingen og viderebehandlingen af oplysninger til det, der er strengt nødvendigt og kræves rent operationelt, og adgang begrænses til personer, som har et operationelt behov for at behandle personoplysningerne ([871]). Forslagene giver også eu-LISA beføjelse til regelmæssigt at udarbejde datakvalitetsrapporter til medlemsstaterne med henblik på regelmæssigt at gennemgå indberetninger for at sikre datakvalitet ([872]).

([869]) EDPS (2017), Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om det nye retsgrundlag for Schengeninformationssystemet, udtalelse 7/2017, 2. maj 2017.

([870]) *Ibid.*, stk. 22.

([871]) Europa-Kommissionen (2016), forslag til Europa-Parlamentets og Rådets forordning om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området politisamarbejde og strafferetligt samarbejde, om ændring af forordning (EU) nr. 515/2014 og om ophævelse af forordning (EF) nr. 1986/2006, Rådets afgørelse 2007/533/RIA og Kommissionens afgørelse 2010/261/EU, COM(2016) 883 final, Bruxelles, 21. december 2016.

([872]) *Ibid.*, s. 15.

Visuminformationssystemet

Visuminformationssystemet (VIS), som også drives af eu-LISA, blev udviklet med henblik på at støtte gennemførelsen af en fælles visumpolitik i EU ([873]). VIS sætter Schengenlandene i stand til at udveksle oplysninger om visumansøgere gennem et fuldt centraliseret system, der forbinder Schengenlandenes konsulater og ambassader i tredjelande med alle Schengenlandenes ydre grænseovergangssteder. VIS behandler oplysninger vedrørende ansøgninger om visa til kortvarigt ophold i eller transit gennem Schengenområdet. VIS sætter grænsemyndighederne i stand til ved hjælp af biometriske data, navnlig fingeraftryk, at kontrollere, om den person, der fremlægger et visum, er dets retmæssige indehaver, og identificere personer uden identitetspapirer eller med falske identitetspapirer.

Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008 om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (VIS-forordningen) regulerer betingelser og procedurer for overførsel af personoplysninger vedrørende ansøgninger om visa til kortvarigt ophold. Den regulerer også afgørelser, som træffes om ansøgninger, herunder beslutninger om at annullere, ophæve eller forlænge visummet ([874]). VIS-forordningen omfatter primært oplysninger om ansøgeren, vedkommendes visa, fotografier, fingeraftryk, forbindelser til tidligere ansøgninger og ansøgningsdokumenter for personer, som ledsager vedkommende, eller oplysninger om inviterede personer ([875]). Adgangen til VIS med henblik på at indtaste, ændre eller slette oplysninger er udelukkende begrænset til visummyndigheder, hvor adgang til søgning i oplysninger gives til visummyndigheder og myndigheder, som er kompetente til kontroller ved de ydre grænseovergangssteder, immigrationskontroller og asyl.

Under visse betingelser kan kompetente nationale myndigheder og Europol anmode om adgang til oplysninger, som er indtastet i VIS, med henblik på at forebygge,

([873]) Rådet for Den Europæiske Union (2004), Rådets beslutning 2004/512/EF af 8. juni 2004 om indførelse af visuminformationssystemet (VIS), EUT L 213 af 15. juni 2004; Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008 af 9. juli 2008 om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (VIS-forordningen) (EUT L 218 af 13.8.2008); Rådet for Den Europæiske Union (2008), Rådets afgørelse 2008/633/RIA af 23. juni 2008 om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger (EUT L 218 af 13.8.2008).

([874]) VIS-forordningen, artikel 1.

([875]) Artikel 5 i Europa-Parlamentets og Rådets forordning (EF) nr. 767/2008 af 9. juli 2008 om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (VIS-forordningen) (EUT L 218 af 13.8.2008).

afsløre eller efterforske terrorhandlinger og strafbare handlinger ([876]). Da VIS er udformet til at være et instrument, som understøtter implementeringen af den fælles visumpolitik, ville princippet om formålsbegrænsning, hvilket, som forklaret i kapitel 3.2., kræver, at personoplysninger udelukkende behandles til udtrykkeligt angivne og legitime formål, og at de skal være tilstrækkelige, relevante og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil oplysninger behandles, blive krænket, hvis VIS blev omdannet til et retshåndhævelsesværktøj. Af denne årsag tildeles nationale retshåndhævende myndigheder og Europol ikke rutinemæssig adgang til VIS-databasen. Adgang må kun tildeles ud fra et individuelt grundlag og skal ledsages af strenge sikkerhedskrav. Betingelser og garantier for, at disse myndigheder har adgang til og må søge i VIS, er reguleret i Rådets afgørelse 2008/633/RIA ([877]).

Derudover fastlægger VIS-forordningen registreredes rettigheder. Det drejer sig om:

- Retten til at blive informeret af den ansvarlige medlemsstat om identiteten af og kontaktoplysninger for den dataansvarlige, som står for behandlingen af personoplysninger i denne medlemsstat, formålene med behandlingen af deres personoplysninger i VIS, personkategorierne, som oplysningerne kan overføres til, (modtagere) og datalagringsperioden. Derudover skal visumansøgere informeres om det faktum, at indsamlingen af deres personoplysninger er obligatorisk i forbindelse med behandlingen af deres ansøgning, og medlemsstater skal også informere dem om eksistensen af deres ret til at få indsigt i deres oplysninger, anmode om deres berigtigelse eller sletning og omkring de procedurer, som gør dem i stand til at udøve disse rettigheder ([878]).

- Retten til at få adgang til personoplysninger vedrørende dem, som er registreret i SIS II ([879]).

- Retten til berigtigelse af ukorrekte oplysninger ([880]).

- Retten til få slettet oplysninger, der lagres ulovligt ([881]).

([876]) Rådet for Den Europæiske Union (2008), Rådets afgørelse 2008/633/RIA af 23. juni 2008 om adgang til søgning i visuminformationssystemet (VIS) for de udpegede myndigheder i medlemsstaterne og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger (EUT L 218 af 13.8.2008).

([877]) *Ibid.*

([878]) VIS-forordningen, artikel 37.

([879]) *Ibid.*, artikel 38, stk. 1.

([880]) *Ibid.*, artikel 38, stk. 2.

([881]) *Ibid.*, artikel 38, stk. 2.

En SKG for VIS blev oprettet for at sikre tilsyn hermed. Den består af repræsentanter for EDPS og de nationale tilsynsmyndigheder, som mødes to gange årligt. Denne gruppe består af repræsentanter fra de 28 EU-medlemsstater og fra Island, Liechtenstein, Norge og Schweiz.

Eurodac

Eurodac er en forkortelse for europæisk daktyloskopi ([882]). Det er et centralt system, som indeholder fingeraftryksoplysninger om tredjelandsstatsborgere og statsløse personer, der søger om asyl i en af EU's medlemsstater ([883]). Systemet har været i drift siden januar 2003 med vedtagelsen af Rådets forordning nr. 2725/2000. En omarbejdning heraf trådte i kraft i 2015. Det har til formål at hjælpe med at fastslå, hvilken medlemsstat der er ansvarlig for at undersøge en bestemt asylansøgning i medfør af forordning (EF) nr. 604/2013. Denne forordning fastsætter kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet af en tredjelands-statsborger eller en statsløs i en af medlemsstaterne (Dublin III-forordningen) ([884]). Personoplysninger i Eurodac må kun anvendes til at lette anvendelsen af Dublin III-forordningen ([885]).

Nationale retshåndhævende myndigheder og Europol må sammenligne fingeraftryk knyttet til strafferetlige efterforskninger med de fingeraftryk, der er lagret i Eurodac, men kun med henblik på at forebygge, afsløre eller efterforske terrorhandlinger og andre alvorlige strafbare handlinger. Da Eurodac er udformet som et instrument til at

([882]) Se Den Europæiske Tilsynsførende for Databeskyttelses websted om Eurodac.

([883]) Rådets forordning (EF) nr. 2725/2000 af 11. december 2000 om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af Dublin-konventionen (EFT L 316 af 15.12.2000); Rådets forordning (EF) nr. 407/2002 af 28. februar 2002 om visse gennemførelsesbestemmelser til forordning (EF) nr. 2725/2000 om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af Dublin-konventionen (EFT L 62 af 5.3.2002) (Eurodacforordningerne) og Europa-Parlamentets og Rådets forordning (EU) nr. 603/2013 af 26. juni 2013 om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet i en af medlemsstaterne af en tredjelandsstatsborger eller en statsløs og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse og om ændring af forordning (EU) nr. 1077/2011 om oprettelse af et europæisk agentur for den operationelle forvaltning af store IT-systemer inden for området med frihed, sikkerhed og retfærdighed (EUT L 180 af 29.6.2013, s. 1) (den omarbejdede Eurodacforordning).

([884]) Europa-Parlamentets og Rådets forordning (EU) nr. 604/2013 af 26. juni 2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet af en tredjelandsstatsborger eller en statsløs i en af medlemsstaterne (EUT L 180 af 29.6.2013) (Dublin III-forordningen).

([885]) Den omarbejdede Eurodacforordning (EUT L 180 af 29.6.2013, s. 1), artikel 1, stk. 1.

støtte implementeringen af EU's asylpolitik og ikke som et retshåndhævende værktøj, har retshåndhævende myndigheder kun adgang til databasen i særlige tilfælde, under særlige omstændigheder og under strenge betingelser ([886]). Databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder finder anvendelse for den videre brug af oplysninger til retshåndhævende formål, hvorimod oplysninger primært anvendt til at gennemføre Dublin III-forordningen er beskyttet under den generelle forordning om databeskyttelse. Yderligere overførsel af personoplysninger indhentet af en medlemsstat eller Europol i henhold til den omarbejdede Eurodacforordning til et tredjeland, en international organisation eller privat enhed, som er etableret i eller uden for EU, er forbudt ([887]).

Eurodac består af en central enhed, som drives af eu-LISA, til lagring og sammenligning af fingeraftryk og et system til elektronisk dataoverførsel mellem medlemsstater og den centrale database. Medlemsstater tager og overfører fingeraftryk for alle personer, der mindst er 14 år gamle, som søger om asyl i deres område, og for alle tredjelandsstatsborgere eller statsløse, der mindst er 14 år gamle og pågribes for uautoriseret krydsning af deres ydre grænser. Medlemsstater kan også tage og overføre fingeraftryk for tredjelandsstatsborgere eller statsløse, som opholder sig inden for deres område uden tilladelse.

Selvom alle medlemsstater kan rådgive Eurodac og anmode om sammenligninger med fingeraftryksoplysninger, er det kun medlemsstaten, der indsamlede fingeraftrykkene og overførte dem til den centrale enhed, som har ret til at ændre oplysningerne ved at berigtige, supplere eller slette dem ([888]). eu-LISA fører registre over alle behandlinger af oplysninger for at overvåge databeskyttelse og sikre datasikkerhed ([889]). De nationale tilsynsmyndigheder hjælper og rådgiver de registrerede om udøvelsen af deres rettigheder ([890]). Indsamling og overførelse af fingeraftryksoplysninger er underlagt domstolsprøvelse ved de nationale domstole ([891]). Forordningen om databeskyttelse inden for EU-institutionerne ([892]) og tilsyn foretaget af EDPS finder anvendelse for det centrale systems

([886]) *Ibid.*, artikel 1, stk. 2.

([887]) *Ibid.*, artikel 35.

([888]) *Ibid.*, artikel 27.

([889]) *Ibid.*, artikel 28.

([890]) *Ibid.*, artikel 29.

([891]) *Ibid.*, artikel 29.

([892]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001).

behandlingsaktiviteter, som forvaltes af eu-LISA i tilknytning til Eurodac ([893]). Hvis en person lider skade som følge af en ulovlig behandling eller fra en handling, som er i strid med Eurodacforordningen, har denne person ret til erstatning fra den medlemsstat, der er ansvarlig for skaden ([894]). Det bør dog understreges, at asylansøgere er en særligt sårbar persongruppe, som ofte har været igennem en lang og farefuld rejse. Det kan i praksis være vanskeligt for dem at udøve deres rettigheder, herunder retten til erstatning, grundet den sårbare og usikre situation, som de ofte befinder sig i, imens deres asylansøgning vurderes.

For at bruge Eurodac til retshåndhævelse skal medlemsstater udpege de myndigheder, som vil have ret til at anmode om adgang, samt de myndigheder, der vil bekræfte, at sammenligningsanmodningerne er lovlige ([895]). Nationale myndigheders og Europols adgang til Eurodacs fingeraftryksoplysninger foregår under meget strenge betingelser. Den anmodende myndighed skal kun indsende en begrundet elektronisk anmodning, efter at oplysningerne er sammenlignet med dem i andre tilgængelige informationssystemer, såsom nationale fingeraftryksdatabaser og VIS. For at sammenligningen er forholdsmæssig, skal der være et tungtvejende hensyn til den offentlige sikkerhed. Sammenligningen skal være absolut nødvendig, vedrøre en specifik sag, og der skal være rimelige grunde til at mene, at sammenligningen i væsentlig grad bidrager til forebyggelse, afsløring eller efterforskning af en af de pågældende strafbare handlinger, navnlig når der er en begrundet mistanke om, at den mistænkte, lovovertræderen eller ofret for en terrorhandling eller anden alvorlig strafbar handling tilhører en kategori, der medfører, at deres fingeraftryk skal indsamles i Eurodac-systemet. Sammenligningen skal udelukkende foretages med fingeraftryksoplysninger. Europol skal også indhente godkendelse fra den medlemsstat, som indsamlede fingeraftryksoplysningerne.

Personoplysninger, som lagres i Eurodac og vedrører asylansøgere, opbevares i 10 år fra datoen, hvor fingeraftrykkene blev taget, medmindre den registrerede bliver statsborger i en EU-medlemsstat. I dette tilfælde skal oplysningerne omgående slettes. Oplysninger vedrørende udenlandske statsborgere, som pågribes for uautoriseret krydsning af de ydre grænser, opbevares i 18 måneder. Disse oplysninger skal omgående slettes, hvis den registrerede modtager en opholdstilladelse, forlader EU's område eller bliver statsborger i en medlemsstat. Oplysninger om de personer,

([893]) Den omarbejdede Eurodacforordning, artikel 31 (EUT L 180 af 29.6.2013, s. 1).

([894]) *Ibid.*, artikel 37.

([895]) Roots, L. (2015), »The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination«, *Baltic Journal of European Studies Tallinn University of Technology*, bind 5, nr. 2, s. 108-129.

som fik tildelt asyl, forbliver tilgængelige til sammenligninger i tre år i forbindelse med at forebygge, afsløre og efterforske terrorhandlinger og andre alvorlige strafbare handlinger.

Udover alle EU-medlemsstater benytter Island, Norge, Liechtenstein og Schweiz også Eurodac på baggrund af internationale aftaler.

Der er oprettet en SKG for Eurodac for at sikre tilsyn med Eurodac. Den består af repræsentanter for EDPS og de nationale tilsynsmyndigheder, som mødes to gange årligt. Denne gruppe består af repræsentanter fra de 28 EU-medlemsstater og fra Island, Liechtenstein, Norge og Schweiz ([896]).

Fremtidsudsigter

I maj 2016 udstedte Kommissionen et forslag om en ny omarbejdet Eurodacforordning som del af en reform, der havde til mål at forbedre funktionen af det fælles europæiske asylsystem ([897]). Den foreslåede omarbejdning er vigtig, da den i væsentlig grad vil udvide omfanget af den oprindelige Eurodacdatabase. Eurodac blev oprindeligt oprettet til at støtte implementeringen af det fælles europæiske asylsystem ved at levere fingeraftryksbeviser, som gjorde det muligt at bestemme, hvilken medlemsstat som er ansvarlig for at undersøge en asylansøgning indgivet i EU. Den foreslåede omarbejdning vil udvide databasens omfang for at lette tilbagesendelse af ulovlige migranter ([898]). Nationale myndigheder vil være i stand til at bruge databasen til at identificere tredjelandsstatsborgere, der ulovligt opholder sig i EU, eller som ulovligt er kommet ind i EU, med henblik på at indhente dokumentation, der kan hjælpe medlemsstater med at sende disse personer tilbage. Selvom den gældende retlige ordning kun kræver indsamling og lagring af

([896]) Se Den Europæiske Tilsynsførende for Databeskyttelses websted om Eurodac.

([897]) Europa-Kommissionen, Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af [forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet af en tredjelandsstatsborger eller en statsløs i en af medlemsstaterne], identificering af en tredjelandsstatsborger eller en statsløs person med ulovligt ophold og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse (omarbejdning), COM(2016) 272 final, 4. maj 2016.

([898]) Jf. forslagets begrundelse, s. 3.

fingeraftryk, indfører forslaget indsamling af enkeltpersoners ansigtsbilleder ([899]), hvilket er en anden form for biometriske oplysninger. Forslaget ville også sænke mindstealderen for børn, der må indsamles biometriske oplysninger om, til seks år ([900]) i stedet for 14 år, hvilket er mindstealderen i forordningen af 2013. Forslagets udvidede omfang betyder, at det vil udgøre et indgreb i retten til privatliv og databeskyttelsen af flere enkeltpersoner, som kan blive optaget i databasen. For at opveje dette indgreb sigter forslaget og ændringerne foreslået af Europa-Parlamentets LIBE-udvalg ([901]) mod at forstærke databeskyttelseskrav. Ved tidspunktet for håndbogens udarbejdelse var diskussionerne om forslaget i Parlamentet og Rådet endnu ikke afsluttet.

Eurosur

Det europæiske grænseovervågningssystem (Eurosur) ([902]) er udformet til at styrke kontrollen med Schengenområdets ydre grænser ved at afsløre, forebygge og bekæmpe ulovlig immigration og grænseoverskridende kriminalitet. Det har til formål at styrke informationsudvekslingen og det operative samarbejde mellem nationale koordinationscentre og Frontex, som er EU-agenturet med ansvar for at udvikle og anvende det nye begreb »integreret grænseforvaltning« ([903]). Dets generelle mål er:

([899]) Europa-Kommissionen, Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af [forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet af en tredjelandsstatsborger eller en statsløs i en af medlemsstaterne], identificering af en tredjelandsstatsborger eller en statsløs person med ulovligt ophold og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse (omarbejdning), COM(2016) 272 final, 4. maj 2016, artikel 2, stk. 1.

([900]) *Ibid*., artikel 2, stk. 2.

([901]) Europa-Parlamentet, *Rapport om forslaget til Europa-Parlamentets og Rådets forordning om oprettelse af »Eurodac« til sammenligning af fingeraftryk med henblik på en effektiv anvendelse af [forordning (EU) nr. 604/2013 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en ansøgning om international beskyttelse, der er indgivet af en tredjelandsstatsborger eller en statsløs i en af medlemsstaterne], identificering af en tredjelandsstatsborger eller en statsløs person med ulovligt ophold og om medlemsstaternes retshåndhævende myndigheders og Europols adgang til at indgive anmodning om sammenligning med Eurodacoplysninger med henblik på retshåndhævelse (omarbejdning)*, PE 597.620v03-00, 9 juni 2017.

([902]) Europa-Parlamentets og Rådets forordning (EU) nr. 1052/2013 af 22. oktober 2013 om oprettelse af det europæiske grænseovervågningssystem (Eurosur) (EUT L 295 af 6.11.2013).

([903]) Europa-Parlamentets og Rådets forordning (EU) 2016/1624 af 14. september 2016 om den europæiske grænse- og kystvagt og om ændring af Europa-Parlamentets og Rådets forordning (EU) 2016/399 og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 863/2007, Rådets forordning (EF) nr. 2007/2004, og Rådets beslutning 2005/267/EF (EUT L 251 af 16.9.2016).

- at reducere antallet af ulovlige migranter, der kommer til EU uden at blive opdaget

- at reducere antallet af dødsfald blandt ulovlige migranter ved at redde flere liv til søs

- at øge den interne sikkerhed i EU som helhed ved at bidrage til forebyggelsen af grænseoverskridende kriminalitet ([904]).

Eurosur indledte sit arbejde den 2. december 2013 i alle medlemsstater med ydre grænser, og den 1. december 2014 blev det iværksat i de øvrige. Forordningen gælder for overvågning af medlemsstaternes ydre land- og søgrænser samt luftgrænser. Eurosur udveksler og behandler personoplysninger i meget begrænset omfang, da medlemsstater og Frontex kun er berettiget til at udveksle skibsidentifikationsnumre. Eurosur udveksler driftsoplysninger, såsom patruljers placering og hændelser, og som en generel regel må de udvekslede oplysninger ikke omfatte personoplysninger ([905]). I usædvanlige tilfælde, hvor personoplysninger udveksles inden for rammerne af Eurosur, fastlægger forordningen, at EU's generelle lovrammer om databeskyttelse fuldt ud er gældende ([906]).

Eurosur sikrer dermed retten til databeskyttelse, navnlig ved at fastslå, at udvekslinger af personoplysninger skal overholde kriterierne og garantierne fastlagt i databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder og den generelle forordning om databeskyttelse ([907]).

([904]) Se også: Europa-Kommissionen (2008), *Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget: undersøgelse af oprettelsen af et europæisk grænseovervågningssystem (EUROSUR)*, KOM(2008) 68 endelig, Bruxelles, 13. februar 2008; Europa-Kommissionen (2011), *Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur)*, arbejdsdokument, SEC(2011) 1536 final, Bruxelles,12. december 2011, s. 18.

([905]) Europa-Kommissionen, *EUROSUR:EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell,* 29. november 2013.

([906]) Forordning 1052/2013, betragtning 13 og artikel 13.

([907]) *Ibid.*, betragtning 13 og artikel 13.

Toldinformationssystemet

Et andet vigtigt fælles informationssystem, som er oprettet på EU-plan, er CIS (toldinformationssystemet) ([908]). Ved oprettelsen af det indre marked blev alle kontroller og formaliteter i forbindelse med varers bevægelser inden for EU's territorium afskaffet, hvilket øgede risikoen for svindel. Denne risiko blev opvejet af et intensiveret samarbejde mellem medlemsstaternes toldmyndigheder. CIS har til formål at hjælpe medlemsstaterne med at forebygge, undersøge og retsforfølge alvorlige overtrædelser af nationale og europæiske told- og landbrugslove. CIS er etableret ved to retsakter, som er vedtaget på forskellige lovgrundlag: Rådets forordning (EF) nr. 515/97 omhandler samarbejde imellem de forskellige nationale administrative myndigheder med henblik på bekæmpelse af bedrageri i forbindelse med toldunionen og den fælles landbrugspolitik, hvor Rådets afgørelse 2009/917/RIA er rettet mod at hjælpe med at forebygge, efterforske og retsforfølge alvorlige overtrædelser af toldlovgivningen. Dette betyder, at CIS ikke kun vedrører retshåndhævelse.

Informationerne i CIS omfatter personoplysninger med henvisning til råvarer, transportmidler, virksomheder, personer, varer og kontanter, der er tilbageholdt, beslaglagt eller konfiskeret. De datakategorier, som kan behandles, er tydeligt defineret og omfatter navne, nationalitet, køn, fødselssted og -dato for de pågældende enkeltpersoner, årsagen til optagelsen af deres oplysninger i systemet og transportmidlets registreringsnummer ([909]). Disse informationer må udelukkende bruges med henblik på observation, rapportering eller gennemførelse af særlige inspektioner eller strategiske eller operationelle analyser vedrørende personer, der mistænkes for at have overtrådt toldbestemmelserne.

De nationale myndigheder for told, skat, landbrug, offentlig sundhed og politi samt Europol og Eurojust tildeles adgang til CIS.

Behandlingen af personoplysninger skal være i overensstemmelse med de specifikke regler i Rådets forordning nr. 515/97 og Rådets afgørelse 2009/917/RIA samt bestemmelserne i den generelle forordning om databeskyttelse, forordningen om

([908]) Rådet for Den Europæiske Union (1995), Rådets retsakt af 26. juli 1995 om udarbejdelse af konventionen om brug af informationsteknologi på toldområdet (EFT C 316 af 27.11.1995), som ændret ved Rådet for Den Europæiske Union (2009), forordning (EF) nr. 515/97 af 13. marts 1997 om gensidig bistand mellem medlemsstaternes administrative myndigheder og om samarbejde mellem disse og Kommissionen med henblik på at sikre den rette anvendelse af told- og landbrugsbestemmelserne og Rådets afgørelse 2009/917/RIA af 30. november 2009 om brug af informationsteknologi på toldområdet (EUT L 323 af 10.12.2009) (CIS-afgørelsen).

([909]) Se CIS-afgørelsen, artikel 24, 25 og 28.

databeskyttelse inden for EU-institutionerne, den moderniserede konvention 108 og henstillingen om politiets brug af personoplysninger. EDPS er ansvarlig for tilsynet med overensstemmelsen af CIS med forordning (EF) nr 45/2001. Denne indkalder til et møde mindst en gang om året med alle nationale tilsynsmyndigheder for databeskyttelse, som er kompetente i CIS-relaterede tilsynsspørgsmål.

Interoperabilitet mellem EU-informationssystemer

Migrationshåndtering, integreret grænseforvaltning af EU's ydre grænser og bekæmpelse af terrorisme og grænseoverskridende kriminalitet er væsentlige udfordringer og er i en globaliseret verden blevet mere og mere kompliceret. I de seneste år har EU arbejdet på en ny omfattende tilgang til at sikre og opretholde sikkerhed uden at gå på kompromis med EU's værdier og grundlæggende frihedsrettigheder. I forbindelse med disse bestræbelser er effektiv informationsudveksling mellem nationale retshåndhævende myndigheder og mellem medlemsstater og relevante EU-agenturer af afgørende betydning ([910]). De eksisterende EU-informationssystemer for grænseforvaltning og intern sikkerhed har deres respektive mål, institutionelle opbygning, registrerede og brugere. EU har arbejdet på at overvinde mangler i funktionaliteten af fragmenteret EU-dataforvaltning imellem de forskellige informationssystemer, såsom SIS II, VIS og Eurodac, ved at udforske potentialet for interoperabilitet ([911]). Hovedmålet er at sikre, at kompetente politi-, told- og retslige myndigheder systematisk besidder de fornødne oplysninger til at udføre deres pligter, mens de opretholder en balance i forbindelse med rettighederne til privatliv, databeskyttelse og andre grundlæggende rettigheder.

([910]) Europa-Kommissionen (2016), Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: stærkere og mere intelligente informationssystemer for grænser og sikkerhed, COM(2016) 205 final, Bruxelles, 6. april 2016, Europa-Kommissionen (2016), Meddelelse fra Kommissionen til Europa-Parlamentet, Det Europæiske Råd og Rådet: øge sikkerheden i en verden med mobilitet - forbedret informationsudveksling i forbindelse med terrorbekæmpelse og stærkere ydre grænser, COM(2016) 602 final, Bruxelles, 14. september 2016 og Europa-Kommissionen (2016), Forslag til Europa-Parlamentets og Rådets forordning om brug af Schengeninformationssystemet i forbindelse med tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold. Jf. ligeledes Meddelelse fra Kommissionen til Europa-Parlamentet, Det Europæiske Råd og Rådet: syvende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion, COM(2017) 261 final, Bruxelles, 16. maj 2017.

([911]) Rådet for Den Europæiske Union (2005), Haag-programmet: styrkelse af frihed, sikkerhed og retfærdighed i Den Europæiske Union (EUT C 53 af 3.3.2005), Europa-Kommissionen (2010), Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: oversigt over informationsstyring på området frihed, sikkerhed og retfærdighed, KOM(2010) 385 endelig, Europa-Kommissionen (2016), Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: stærkere og mere intelligente informationssystemer for grænser og sikkerhed, COM(2016) 205 final, Bruxelles, 6. april 2016 og Europa-Kommissionen (2016), Kommissionens afgørelse af 17. juni 2016 om nedsættelse af en ekspertgruppe på højt niveau vedrørende informationssystemer og interoperabilitet (EUT C 257 af 15.7.2016).

Interoperabilitet betyder, »at der kan udveksles og deles information mellem informationssystemer« ([912]). Denne udveksling må ikke tilsidesætte de nødvendigvis strenge regler om adgang og brug, som er garanteret ved den generelle forordning om databeskyttelse, databeskyttelsesdirektivet vedrørende politi og strafferetlige myndigheder, EU's charter om grundlæggende rettigheder og alle andre relevante regler. Enhver integreret løsning til dataforvaltning må ikke påvirke principperne om formålsbegrænsning, databeskyttelse gennem design eller databeskyttelse gennem standardindstillinger ([913]).

Udover at forbedre funktionaliteterne for de tre primære informationssystemer — SIS II, VIS og Eurodac — har Kommissionen foreslået oprettelsen af et fjerde centraliseret grænseforvaltningssystem, der behandler tredjelandsstatsborgere: ind- og udrejsesystemet ([914]), som forventes at være implementeret inden 2020 ([915]). Kommissionen har også udstedt et forslag om oprettelsen af et EU-system vedrørende rejseinformation og rejsetilladelse (ETIAS) ([916]), hvilket er et system, som vil indsamle oplysninger om personer, der rejser visumfrit til EU, for at muliggøre forudgående kontrol af irregulær migration og sikkerhedskontrol.

([912]) Europa-Kommissionen (2016), Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: stærkere og mere intelligente informationssystemer for grænser og sikkerhed, COM(2016) 205 final, Bruxelles, 6. april 2016, s. 14.

([913]) *Ibid*., s. 4-5.

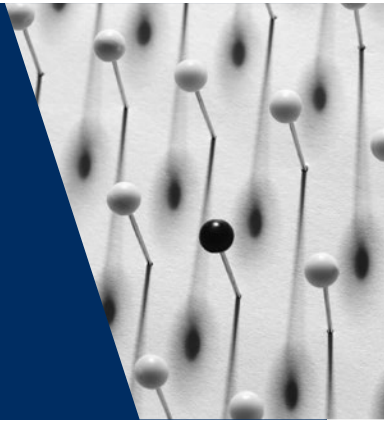
([914]) Europa-Kommissionen (2016), Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af et ind- og udrejsesystem til registrering af ind- og udrejseoplysninger og oplysninger om nægtelse af indrejse vedrørende tredjelandsstatsborgere, der passerer Den Europæiske Unions medlemsstaters ydre grænser, og om fastlæggelse af betingelserne for adgang til ind- og udrejsesystemet til retshåndhævelsesformål og om ændring af forordning (EF) nr. 767/2008 og forordning (EU) nr. 1077/2011, COM(2016) 194 final, Bruxelles, 6. april 2016.

([915]) Europa-Kommissionen (2016), Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: stærkere og mere intelligente informationssystemer for grænser og sikkerhed, COM(2016) 205 final, Bruxelles, 6. april 2016, s. 5.

([916]) Europa-Kommissionen (2016), Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af et EU-system vedrørende rejseinformation og rejsetilladelse (ETIAS) og om ændring af forordning (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/794 og (EU) 2016/1624, COM(2016) 731 final, 16. november 2016.

9

Specifikke datatyper og deres relevante databeskyttelsesregler



EU	Omhandlede emner	Europarådet
Generel forordning om databeskyttelse Direktiv om databeskyttelse inden for elektronisk kommunikation	**Elektronisk kommunikation**	Den moderniserede konvention 108 Henstilling om telekommunikations-tjenester
Generel forordning om databeskyttelse, artikel 88	**Arbejdsmarkeds-relationer**	Den moderniserede konvention 108 Beskæftigelseshenstilling EMD, *Copland mod Det Forenede Kongerige*, nr. 62617/00, 2007
Generel forordning om databeskyttelse, artikel 9, stk. 2, litra h) og i)	**Medicinske data**	Den moderniserede konvention 108 Henstilling om medicinske oplysninger EMD, *Z mod Finland*, nr. 22009/93, 1997
Forordningen om kliniske forsøg	**Kliniske forsøg**	
Generel forordning om databeskyttelse, artikel 6, stk. 4, og artikel 89	**Statistikker**	Den moderniserede konvention 108 Henstilling om statistiske data
Forordning (EF) nr. 223/2009 om europæiske statistikker EU-Domstolen, C-524/06, *Heinz Huber mod Bundesrepublik Deutschland* [GC], 2008	**Officielle statistikker**	Den moderniserede konvention 108 Henstilling om statistiske data

EU	Omhandlede emner	Europarådet
Direktiv 2014/65/EU om markeder for finansielle instrumenter Forordning (EU) nr. 648/2012 om OTC-derivater, centrale modparter og transaktionsregistre Forordning (EF) nr. 1060/2009 om kreditvurderingsbureauer Direktiv 2007/64/EF om betalingstjenester i det indre marked	**Finansielle oplysninger**	Den moderniserede konvention 108 Henstilling 90 (19) benyttet til betalinger og andre tilknyttede operationer EMD, *Michaud mod Frankrig*, nr. 12323/11, 2012

I flere tilfælde er der vedtaget særlige retslige instrumenter på europæisk niveau, så de generelle regler i den moderniserede konvention 108 eller i den generelle forordning om databeskyttelse kan anvendes mere indgående i særlige situationer.

9.1. Elektronisk kommunikation

Hovedpunkter

- Specifikke regler for databeskyttelse på telekommunikationsområdet, herunder især telefontjenester, findes i Europarådets henstilling fra 1995.
- Behandling af personoplysninger vedrørende levering af kommunikationstjenester på EU-plan er omhandlet i direktivet om databeskyttelse inden for elektronisk kommunikation.
- Fortroligheden af elektronisk kommunikation vedrører ikke kun indholdet af kommunikation, men også metadata, såsom oplysninger om, hvem der har kommunikeret med hvem, hvornår og hvor længe, og lokaliseringsdata, såsom hvorfra data blev kommunikeret.

Kommunikationsnet rummer et forøget potentiale for ubeføjede indgreb i brugernes privatsfære, fordi de giver omfattende tekniske muligheder for at lytte til og overvåge kommunikation, der gennemføres på sådanne net. Som følge deraf fandt man det nødvendigt at indføre særlige databeskyttelsesbestemmelser for at imødegå risiciene for brugere af kommunikationstjenester.

I 1995 udsendte **Europarådet** en henstilling vedrørende databeskyttelse på telekommunikationsområdet, herunder især telefontjenester ([917]). I henhold til henstillingen bør formålene med indsamling og behandling af personoplysninger i forbindelse med telekommunikation begrænses til: tilslutning af en bruger til netværket, levering af den pågældende telekommunikationstjeneste, fakturering, bekræftelse, sikring af optimal teknisk drift og udvikling af netværket og tjenesten.

Fokus blev også rettet mod brugen af kommunikationsnet til udsendelse af direkte markedsføringsmeddelelser. Generelt må direkte markedsføringsmeddelelser ikke sendes til en abonnent, der direkte har fravalgt modtagelsen af reklamemeddelelser. Automatiserede opkaldsanordninger, der overfører optagne reklamemeddelelser, må kun bruges, hvis en abonnent har givet sit udtrykkelige samtykke. Detaljerede regler for dette område fastlægges ved national lov.

Med hensyn til **EU-retten** blev direktivet om databeskyttelse inden for elektronisk kommunikation efter et første forsøg i 1997 vedtaget i 2002 og ændret i 2009. Formålet hermed var at supplere og tilpasse bestemmelserne i det tidligere databeskyttelsesdirektiv specifikt til telekommunikationssektoren ([918]).

Direktivet om databeskyttelse inden for elektronisk kommunikation finder kun anvendelse på kommunikationstjenester på offentlige elektroniske net.

I direktivet om databeskyttelse inden for elektronisk kommunikation skelnes der mellem tre kategorier af data, der genereres i forbindelse med kommunikation:

- de data, der udgør indholdet af de meddelelser, som sendes under kommunikationen; disse data er strengt fortrolige

([917]) Europarådet, Ministerudvalget (1995), Henstilling Rec(95)4 til medlemsstaterne om beskyttelse af personoplysninger på telekommunikationsområdet, herunder især telefontjenester, 7. februar 1995.

([918]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse (EUT L 337 af 18.12.2009).

- de data, der er nødvendige for at etablere og opretholde kommunikationen, dvs. metadata, som i direktivet kaldes »trafikdata«, såsom information om kommunikationspartnerne samt tidspunkt for og varighed af kommunikationen

- metadata omfattende data, der specifikt vedrører placeringen af kommunikationsudstyret, såkaldte lokaliseringsdata; disse data er samtidig data om placeringen af brugerne af kommunikationsudstyret og er især relevante for brugere af mobilt kommunikationsudstyr.

Tjenesteudbyderen må udelukkende bruge trafikdata til fakturering og til teknisk at levere tjenesten. Med den registreredes samtykke kan disse data dog videregives til andre dataansvarlige, som tilbyder tillægstjenester, såsom oplysninger om den nærmeste metrostation eller det nærmeste apotek i forhold til brugerens aktuelle placering eller vejrudsigten for den pågældende placering.

Anden adgang til data om kommunikation på elektroniske netværk skal i henhold til artikel 15 i e-databeskyttelsesdirektivet opfylde betingelserne for begrundede indgreb som fastlagt i artikel 8, stk. 2, i EMRK og bekræftet ved artikel 8 og 52 i EU's charter om grundlæggende rettigheder. En sådan adgang kan omfatte adgang med henblik på kriminalefterforskning.

Ved ændringerne af direktivet om databeskyttelse inden for elektronisk kommunikation ([919]) i 2009 indførtes følgende:

- Begrænsningerne for udsendelse af e-mail i direkte markedsføringsøjemed blev udvidet til at gælde for tjenester for korte meddelelser, tjenester for multimediemeddelelser og andre lignende anvendelser. Markedsførings-e-mail er forbudt, medmindre der er indhentet forudgående samtykke. Uden et sådant samtykke må tidligere kunder kun kontaktes med markedsførings-e-mails, hvis de har oplyst deres e-mail-adresse og ikke gør indsigelse.

- Medlemsstaterne blev pålagt en forpligtelse til at sikre klageadgang i tilfælde af overtrædelse af forbuddet mod uanmodet kommunikation ([920]).

([919]) Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse (EUT L 337 af 18.12.2009).

([920]) Se det ændrede direktiv, artikel 13.

- Indsættelse af cookies, dvs. software, som overvåger og registrerer en computerbrugers handlinger, er ikke længere tilladt uden computerbrugerens samtykke. Hvordan dette samtykke skal udtrykkes og indhentes for at sikre tilstrækkelig beskyttelse, fastsættes ved national lov ([921]).

I tilfælde af brud på datasikkerheden som følge af uautoriseret adgang, tab eller tilintetgørelse af data skal den kompetente tilsynsmyndighed straks underrettes. Abonnenterne skal så vidt muligt oplyses om den skade, de er blevet påført som følge af et sådant brud på datasikkerheden ([922]).

I henhold til datalagringsdirektivet ([923]) havde telekommunikationsudbydere pligt til at bevare metadata. Dette direktiv blev dog annulleret af EU-Domstolen (se flere detaljer i afsnit 8.3.).

Fremtidsudsigter

I januar 2017 vedtog Europa-Kommissionen et nyt forslag til en e-databeskyttelsesforordning, som skal erstatte det gamle e-databeskyttelsesdirektiv. Formålet forbliver beskyttelse »af fysiske og juridiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med levering og anvendelse af elektroniske kommunikationstjenester og navnlig for retten til respekt for privatlivet og kommunikation, samt at der sørges for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger«. På samme tid skal det nye forslag sikre fri bevægelighed af elektroniske kommunikationsdata og elektroniske kommunikationstjenester i Unionen ([924]). Selvom den generelle forordning om databeskyttelse primært omhandler artikel 8 i EU's charter om grundlæggende rettigheder, er den foreslåede forordning rettet mod at indarbejde chartrets artikel 7 i afledt EU-ret.

([921]) Se *Ibid.*, artikel 5. Se også Artikel 29-Gruppen (2012), *Udtalelse 04/2012 om undtagelser fra kravet om, at der skal gives samtykke til cookies*, WP 194, Bruxelles, 7. juni 2012.

([922]) Se også Artikel 29-Gruppen (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, WP 184, Bruxelles, 5. april 2011.

([923]) Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT L 105 af 13.4.2006).

([924]) Forslag til Europa-Parlamentets og Rådets forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektroniske kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om databeskyttelse inden for elektronisk kommunikation), COM(2017) 10 final), artikel 1.

Forordningen vil tilpasse det tidligere direktivs bestemmelser til nye teknologier og virkeligheden på markedet og vil opstille nogle omfattende rammer, som stemmer overens med den generelle forordning om databeskyttelse. I denne sammenhæng vil e-databeskyttelsesforordning udgøre særlovgivning i forhold til den generelle forordning om databeskyttelse, hvor denne er fokuseret på elektronisk kommunikation, der betragtes som personoplysninger. Den nye forordning omfatter behandling af »elektroniske kommunikationsdata«, herunder elektronisk kommunikationsindhold og metadata, der ikke nødvendigvis er personoplysninger. Det territoriale anvendelsesområde er begrænset til EU, inklusive når oplysninger indhentes i EU og behandles uden for EU, og omfatter udbydere af »over the top«-kommunikationstjenester. Disse tjenesteudbydere leverer indhold, tjenester eller applikationer over internettet uden direkte indblanding fra en netværksoperatør eller internetudbyder. Skype (stemme- og videoopkald), WhatsApp (beskeder), Google (søgning), Spotify (musik) eller Netflix (videoindhold) er eksempler på sådanne udbydere. Håndhævelsesmekanismerne i den generelle forordning om databeskyttelse vil også gælde for den nye forordning.

Planen er at vedtage e-databeskyttelsesforordningen inden den 25. maj 2018, hvorinden den generelle forordning om databeskyttelse vil være gældende i alle 28 medlemsstater. Dette afhænger dog af godkendelse fra både Europa-Parlamentet og Rådet ([925]).

9.2. Personoplysninger i ansættelsesforhold

Hovedpunkter

- Europarådet har fastsat specifikke regler for databeskyttelse i ansættelsesforhold i sin henstilling om personoplysninger i ansættelsesforhold.
- Ansættelsesmæssige forhold er kun specifikt omhandlet i den generelle forordning om databeskyttelse, for så vidt angår behandling af følsomme oplysninger.
- Det er tvivlsomt, om samtykke, der skal være givet frit, er gyldigt som retsgrundlag for behandling af medarbejderes personoplysninger i betragtning af den økonomiske skævhed mellem arbejdsgiver og medarbejdere. Omstændighederne omkring afgivelsen af samtykke skal vurderes nøje.

([925]) Yderligere oplysninger: Europa-Kommissionen (2017), »Kommissionen foreslår et højt niveau for beskyttelse af privatlivets fred og databeskyttelsesregler inden for elektronisk kommunikation og opdaterer EU-institutionernes databeskyttelsesregler«, pressemeddelelse, 10. januar 2017.

Databehandling i forbindelse med ansættelsesforhold er underlagt den generelle EU-ret om beskyttelse af personoplysninger. Én forordning ([926]) omhandler dog specifikt beskyttelse af europæiske institutioners behandling af personoplysninger i forbindelse med ansættelsesforhold (blandt andre ting). I den generelle forordning om databeskyttelse henvises der udtrykkeligt til ansættelsesforhold i artikel 9, stk. 2, som fastlægger, at personoplysninger må behandles ved opfyldelse af forpligtelser eller udøvelse af den dataansvarliges eller den registreredes specifikke rettigheder, for så vidt angår ansættelsesforhold.

I henhold til den generelle forordning om databeskyttelse skal arbejdsgiveren have mulighed for tydeligt at adskille de oplysninger, hvis behandling/lagring vedkommende afgiver frivilligt samtykke til, og formålene, som vedkommendes oplysninger lagres til. Medarbejdere bør også oplyses om deres rettigheder og tidsrummet, oplysningerne lagres i, inden samtykke kan afgives. Hvis et brud på persondatasikkerheden finder sted, som med sandsynlighed medfører en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal arbejdsgiveren meddele dette brud til medarbejderen. Forordningens artikel 88 tillader, at medlemsstater fastlægger mere specifikke regler til at sikre beskyttelse af medarbejderes rettigheder og frihedsrettigheder i forbindelse med deres personoplysninger, for så vidt angår ansættelsesforhold.

Eksempel: I *Worten*-sagen ([927]) omfattede oplysningerne et register over arbejdstid, som indeholdt daglige arbejdstider og pauser, hvilket udgør personoplysninger. National lovgivning kan kræve, at en arbejdsgiver gør arbejdstidsregistrene tilgængelige for de nationale myndigheder, der er ansvarlige for at overvåge arbejdsvilkår. Dette ville tillade omgående adgang til de relevante personoplysninger. Adgang til personoplysningerne er dog nødvendigt for, at den nationale myndighed kan overvåge lovgivningen om arbejdsvilkår ([928]).

([926]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001).

([927]) EU-Domstolen, C-342/12, *Worten — Equipamentos para o Lar SA mod Autoridade para as Condições de Trabalho (ACT)*, 30. maj 2013, præmis 19.

([928]) *Ibid*., præmis 43.

Europarådet udsendte i 1989 sin henstilling om personoplysninger i ansættelsesforhold, som blev ajourført i 2015 ([929]). Henstillingen omfatter behandling af personoplysninger af arbejdsmæssige grunde i både private og offentlige sektorer. Behandlingen skal overholde visse principper og begrænsninger, såsom princippet om gennemsigtighed og høring af medarbejderrepræsentanter, inden overvågningssystemer installeres på arbejdspladsen. Henstillingen fastsætter også, at arbejdsgivere bør anvende forebyggende foranstaltninger, såsom filtre, i stedet for at overvåge medarbejderes internetbrug.

En undersøgelse af de mest udbredte databeskyttelsesproblemer netop i forbindelse med ansættelsesforhold findes i et arbejdsdokument fra Artikel 29-Gruppen ([930]). Arbejdsgruppen analyserede betydningen af samtykke som retsgrundlag for behandling af personoplysninger ([931]). Arbejdsgruppen fandt, at den økonomiske skævhed mellem arbejdsgiveren, der anmodede om samtykke, og medarbejderen, som gav sit samtykke, ofte vil give anledning til tvivl om, hvorvidt et samtykke er givet frit. De omstændigheder, hvorunder samtykke benyttes som retsgrundlag for databehandling, bør derfor overvejes nøje ved vurderingen af gyldigheden af samtykke i ansættelsesforhold.

Et udbredt databeskyttelsesproblem på mange arbejdspladser er i dag omfanget af den legitime overvågning af medarbejdernes elektroniske kommunikation på arbejdspladsen. Det hævdes ofte, at dette problem let kan løses ved at forbyde privat brug af kommunikationsudstyr på arbejde. Et sådant generelt forbud kan dog være uforholdsmæssigt og urealistisk. EMD's domme i *Copland mod Det Forenede Kongerige* og *Bărbulescu mod Rumænien* er især relevante i denne forbindelse.

Eksempel: I sagen *Copland mod Det Forenede Kongerige* ([932]) blev en medarbejders brug af telefon, e-mail og internettet i hemmelighed overvåget for at kontrollere, om hun i overdreven grad anvendte arbejdsgiverens udstyr til private formål. EMD fastslog, at telefonopkald fra virksomhedslokaler var omfattet af begreberne privatliv og korrespondance. Sådanne opkald og e-mails, der var sendt fra arbejdspladsen, og oplysninger, der blev udledt

([929]) Europarådet, Ministerkomité (2015), Henstilling CM/Rec(2015)5 til medlemsstaterne om behandling af personoplysninger i ansættelsesforhold, april 2015.

([930]) Artikel 29-Gruppen (2017), *Udtalelse 2/2017 om databehandling på arbejdspladsen*, WP 249, Bruxelles, 8. juni 2017.

([931]) Artikel 29-Gruppen (2005), *Arbejdsdokument om en ensartet fortolkning af artikel 26, stk. 1, i direktiv 95/46/EF af 24. oktober 1995*, WP 114, Bruxelles, 25. november 2005.

([932]) EMD, *Copland mod Det Forenede Kongerige*, nr. 62617/00, 3. april 2007.

af overvågningen af den personlige anvendelse af internettet, var således beskyttet af artikel 8 i EMRK. I sagsøgerens tilfælde var der ingen bestemmelser, som omhandlede de omstændigheder, hvorunder arbejdsgivere kunne overvåge medarbejderes brug af telefon, e-mail og internettet. Indgrebet var derfor ikke i overensstemmelse med loven. Domstolen konkluderede, at EMRK's artikel 8 var blevet overtrådt.

Eksempel: I sagen *Bărbulescu mod Rumænien* ([933]) var sagsøgeren blevet afskediget for at bruge hans ansættelsessteds internet i arbejdstiden i strid med interne regler. Hans arbejdsgiver overvågede hans kommuniikationer. Registrene, som indeholdt meddelelser udelukkende af privat karakter, blev udarbejdet under den nationale retssag. Da EMD mente, at artikel 8 var gældende, efterlod det spørgsmålet om, hvorvidt arbejdsgiverens restriktive regler gav sagsøgeren en rimelig beskyttelse af privatlivets fred, ubesvaret, men domstolen konkluderede dog, at en arbejdsgivers anvisninger ikke kunne reducere en persons private socialliv til ingenting på arbejdspladsen.

Hvad angår sagens grundlag, var det nødvendigt at tildele kontraherende stater brede muligheder for skøn ved vurdering af behovet for at fastlægge lovrammer for de betingelser, som en arbejdsgiver kan regulere sine arbejdstageres ikke-erhvervsmæssige kommunikationer – elektroniske eller andre former – under på arbejdspladsen. De nationale myndigheder skulle dog stadig sikre, at en arbejdsgivers foranstaltninger for overvågning af korrespondance og andre kommunikationer, uanset omfanget og varigheden af sådanne foranstaltninger, blev indført sammen med passende og tilstrækkelige garantier mod misbrug. Proportionalitet og proceduremæssige garantier mod vilkårlig behandling var nødvendige, og EMD udpegede en række faktorer, som var relevante i de pågældende omstændigheder. Eksempler på sådanne faktorer var: omfanget af arbejdsgiverens overvågning, graden af indblanding i arbejdstagerens privatliv, konsekvenserne for arbejdstageren og hvorvidt tilstrækkelige garantier var fastlagt. Derudover skulle nationale myndigheder sikre, at en arbejdstager, hvis kommunikationer var blevet overvåget, havde adgang til retsmidler hos en retsinstans med kompetence til at bestemme, i realiteten som minimum, hvordan de pågældende kriterier skulle overholdes, og om de anfægtede foranstaltninger var lovlige.

([933]) EMD, *Bărbulescu mod Rumænien* [GC], nr. 61496/08, 5. september 2017, præmis 121.

I denne sag konstaterede EMD, at artikel 8 var blevet overtrådt, da de nationale myndigheder ikke havde beskyttet sagsøgerens ret til respekt for hans privatliv og korrespondance i tilstrækkelig grad og dermed ikke havde sikret en rimelig balance mellem de foreliggende interesser.

I henhold til Europarådets henstilling om personoplysninger i ansættelsesforhold bør personoplysninger, der indsamles i forbindelse med ansættelsesforhold, indhentes direkte fra den enkelte medarbejder.

Personoplysninger, der indhentes med henblik på rekruttering, skal begrænses til de informationer, der er nødvendige for at vurdere kandidaternes egnethed og karrierepotentiale.

I henstillingen nævnes også specifikt vurderinger vedrørende enkelte medarbejderes resultater eller potentiale. Vurderinger skal baseres på retfærdige og ærlige evalueringer og må ikke være stødende i deres formulering. Dette kræves i medfør af principperne om rimelig databehandling og oplysningers rigtighed.

Et specifikt aspekt af databeskyttelseslovgivningen i forholdet mellem arbejdsgiver og arbejdstager er medarbejderrepræsentanternes rolle. Sådanne repræsentanter må kun modtage medarbejderes personoplysninger, hvis de er nødvendige for, at de kan repræsentere de pågældende medarbejderes interesser, eller hvis disse oplysninger er nødvendige til at opfylde eller overvåge forpligtelserne fastlagt i kollektive overenskomster.

Følsomme personoplysninger, der indsamles i ansættelsesforhold, må kun behandles i særlige tilfælde og i overensstemmelse med de særlige garantier, der er fastlagt i den nationale ret. Arbejdsgivere må kun anmode medarbejdere eller jobansøgere om oplysninger om deres helbred eller underkaste dem en lægeundersøgelse, hvis det er nødvendigt. Nødvendige grunde kan være: for at afgøre, om en medarbejder er egnet til ansættelse, om kravene til forebyggende medicin er opfyldt, for at beskytte den registreredes eller andre medarbejderes og fysiske personers vitale interesser, så en medarbejder kan få tildelt sociale ydelser, eller for at svare på retslige anmodninger. Helbredsdata må ikke indsamles fra andre kilder end den berørte medarbejder, medmindre der er indhentet udtrykkeligt og informeret samtykke, eller når det er tilladt i henhold til national lov.

Ifølge henstillingen om personoplysninger i ansættelsesforhold bør medarbejdere informeres om formålet med behandlingen af deres personoplysninger, typen af lagrede personoplysninger, de enheder, oplysningerne regelmæssigt videregives til, samt formålet med og retsgrundlaget for sådanne videregivelser. Adgang til elektroniske kommunikationer på arbejdspladsen må kun foregå på baggrund af sikkerhed eller andre legitime årsager, og denne adgang tillades kun, efter medarbejderne er blevet informeret om, at arbejdsgiveren kan have adgang til denne form for kommunikation.

Medarbejdere skal have ret til indsigt i deres ansættelsesmæssige data, og de skal have ret til berigtigelse eller sletning. Hvis vurderingsoplysninger behandles, skal medarbejderne endvidere have ret til at anfægte vurderingen. Disse rettigheder kan dog begrænses midlertidigt i forbindelse med interne undersøgelser Hvis en medarbejder nægtes indsigt, berigtigelse eller sletning af personoplysninger i ansættelsesforhold, skal den nationale lovgivning omfatte passende procedurer for at anfægte en sådan afvisning.

9.3. Helbredsoplysninger

Hovedpunkt

- Medicinske oplysninger er følsomme oplysninger og er derfor garanteret særlig beskyttelse.

Personoplysninger vedrørende den registreredes helbred udgør følsomme oplysninger i henhold til artikel 9, stk. 1, i den generelle forordning om databeskyttelse og artikel 6 i den moderniserede konvention 108. Helbredsoplysninger er til gengæld underlagt strengere databehandlingsregler end ikke-følsomme oplysninger. Den generelle forordning om databeskyttelse forbyder behandlingen af »helbredsoplysninger« (hvilket defineres som »alle personoplysninger om den registreredes helbredstilstand, som giver oplysninger om den registreredes tidligere, nuværende eller fremtidige fysiske eller mentale helbredstilstand«) ([934]) samt genetiske og biometriske oplysninger, medmindre det er godkendt under artikel 9, stk. 2. Begge typer af oplysninger er føjet til listen over »særlige kategorier af oplysninger« ([935]).

([934]) Generel forordning om databeskyttelse, betragtning 35.

([935]) *Ibid.*, artikel 2.

Eksempel: I sagen *Z mod Finland* ([936]) havde sagsøgerens tidligere mand, som var hiv-smittet, begået en række seksuelle forbrydelser. Han blev efterfølgende dømt for manddrab med den begrundelse, at han bevidst udsatte sine ofre for risikoen for hiv-infektion. Den nationale domstol fastslog, at dommen i sin helhed samt sagsakterne skulle forblive fortrolige i 10 år trods sagsøgerens anmodning om en længere fortrolighedsperiode. Disse anmodninger blev afvist af appeldomstolen, og dens dom indeholdt både sagsøgerens og hendes tidligere mands fulde navne. EMD afgjorde, at indgrebet ikke var nødvendigt i et demokratisk samfund, fordi beskyttelsen af medicinske oplysninger er af grundlæggende betydning for, at en person kan nyde sin ret til respekt for privat- og familieliv, især med hensyn til oplysninger om hiv-infektioner på grund af stigmatiseringen heraf i mange samfund. Domstolen konkluderede derfor, at indsigt i sagsøgerens identitet og medicinske tilstand som beskrevet i appeldomstolens dom kun 10 år efter domsafsigelsen ville være i strid med artikel 8 i EMRK.

Under **EU-retten** tillader artikel 9, stk. 2, litra h), i den generelle forordning om databeskyttelse behandling af medicinske oplysninger, når dette kræves med henblik på forebyggende medicin, medicinsk diagnose, ydelse af omsorg eller behandling eller forvaltning af sundhedsplejetjenester. Behandling tillades dog kun, når den udføres af en sundhedsperson, som er underlagt en tavshedspligt, eller af en anden person, som er underlagt en tilsvarende forpligtelse.

Under **Europarådets retsorden** overfører Europarådets henstilling om medicinske oplysninger fra 1997 principperne i konvention 108 til databehandling på det lægelige område i nærmere detaljer ([937]). De foreslåede regler er i overensstemmelse med dem i den generelle forordning om databeskyttelse vedrørende de legitime formål for behandling af medicinske oplysninger, de nødvendige faglige tavshedspligter for personer, som bruger helbredsoplysninger, og registreredes ret til gennemsigtighed, indsigt, berigtigelse og sletning. Medicinske oplysninger, som behandles lovligt af sundhedspersoner, må desuden ikke videregives til retshåndhævende myndigheder, medmindre der gennemføres tilstrækkelige foranstaltninger til at forhindre videregivelse, der er uforenelig med respekten for retten til privatliv garanteret ved

([936]) EMD, *Z mod Finland*, nr. 22009/93, 25. februar 1997, præmis 94 og 112. Se også EMD, *M.S. mod Sverige*, nr. 20837/92, 27. august 1997, EMD, *L.L. mod Frankrig*, nr. 7508/02, 10. oktober 2006, EMD, *I. mod Finland*, nr. 20511/03, 17. juli 2008, EMD, *K.H. m.fl. mod Slovakiet*, nr. 32881/04, 28. april 2009, og EMD, *Szuluk mod Det Forenede Kongerige*, nr. 36936/05, 2. juni 2009.

([937]) Europarådet, Ministerkomité (1997), Henstilling Rec(97)5 til medlemsstaterne om beskyttelse af medicinske oplysninger, 13. februar 1997. Bemærk, at denne henstilling i øjeblikket revideres.

artikel 8 i EMRK ([938]). Den nationale lovgivning skal også formuleres med en tilstrækkelig præcision og gives passende retlig beskyttelse mod vilkårlig behandling ([939]).

Henstillingen om beskyttelse af medicinske oplysninger indeholder endvidere særlige bestemmelser om medicinske oplysninger vedrørende ufødte børn og personer, der ikke er i stand til at give deres samtykke, og om behandlingen af genetiske oplysninger. Videnskabelig forskning anerkendes udtrykkeligt som en grund til at opbevare oplysninger i længere tid end nødvendigt, selv om dette normalt kræver anonymisering. I artikel 12 i henstillingen om beskyttelse af medicinske oplysninger foreslås der detaljerede bestemmelser vedrørende situationer, hvor forskere har brug for personoplysninger, og anonymiserede data ikke er tilstrækkelige.

Pseudonymisering kan være en hensigtsmæssig metode til at opfylde de videnskabelige behov og samtidig beskytte de berørte patienters interesser. Begrebet pseudonymisering i forbindelse med databeskyttelse er forklaret i detaljer i afsnit 2.1.1.

Europarådets henstilling af 2016 om oplysninger fra genetiske prøver er også gældende for behandling på det medicinske område ([940]). Denne henstilling har stor betydning for e-sundhed, hvor IKT (Informations- og kommunikationsteknologi) benyttes til at yde sundhedspleje. Et eksempel er at sende en patients oprindelige testresultater fra en sundhedstjenesteyder til en anden. Denne henstilling er rettet mod at beskytte rettighederne for personer, hvis personoplysninger behandles i forsikringsøjemed med henblik på at sikre sig mod risici knyttet til en persons helbred, fysiske integritet, alder eller dødsfald. Forsikringsgivere skal begrunde behandlingen af sundhedsrelaterede oplysninger, og denne behandling skal være forholdsmæssig i forhold til arten og vigtigheden af risikoen, som er under betragtning. Behandlingen af denne form for oplysninger afhænger af den registreredes samtykke. Forsikringsgivere skal også have garantier på plads for lagringen af sundhedsrelaterede oplysninger.

Kliniske forsøg, som omfatter vurdering af virkningerne af nye stoffer på patienter inden for dokumenterede forskningsmiljøer, har stor betydning for databeskyttelse. Kliniske forsøg med lægemidler til mennesker er reguleret ved Europa-Parlamentets og Rådets forordning (EU) nr. 536/2014 af 16. april 2014 om kliniske forsøg med

([938]) EMD, *Avilkina m.fl. mod Rusland*, nr. 1585/09, 6. juni 2013, præmis 53. Se også EMD, *Biriuk mod Litauen*, nr. 23373/03, 25. november 2008.

([939]) EMD, *L.H. mod Letland*, nr. 52019/07, 29. april 2014, præmis 59.

([940]) Europarådet, Ministerudvalget (2016), Recommendation Rec(2016)8 to member states on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, 26. oktober 2016.

humanmedicinske lægemidler og om ophævelse af direktiv 2001/20/EF (forordningen om kliniske forsøg) ([941]). De væsentligste elementer i forordningen om kliniske forsøg er:

- en strømlinet ansøgningsprocedure via EU-portalen ([942])
- tidsfrister for vurderingen af en ansøgning om kliniske forsøg ([943])
- en etisk komités deltagelse i vurderingen i medfør af medlemsstaternes lovgivning (og europæisk lovgivning om definition af de pågældende tidsperioder) ([944])
- forbedret gennemsigtighed for kliniske forsøg og deres resultater ([945]).

Den generelle forordning om databeskyttelse angiver, at forordning (EU) nr. 536/2014 finder anvendelse, for så vidt angår samtykke til deltagelse i videnskabelige forskningsaktiviteter i forbindelse med kliniske forsøg ([946]).

En række andre lovgivningsmæssige og andre initiativer vedrørende personoplysninger i sundhedssektoren behandles aktuelt på EU-plan ([947]).

Elektroniske patientjournaler

Elektroniske patientjournaler defineres som »en hel patientjournal eller lignende dokumentation i elektronisk form vedrørende en persons tidligere og nuværende fysiske og psykiske tilstand, som giver let adgang til disse data med henblik på lægelig behandling og andre dermed tæt relaterede formål« ([948]). Elektroniske patientjournaler er elektroniske udgaver af patienters sygehistorie og kan omfatte

([941]) Europa-Parlamentets og Rådets forordning (EU) nr. 536/2014 af 16. april 2014 om kliniske forsøg med humanmedicinske lægemidler og om ophævelse af direktiv 2001/20/EF (forordningen om kliniske forsøg) (EUT L 158 af 27.5.2014).

([942]) Forordningen om kliniske forsøg, artikel 5, stk. 1.

([943]) *Ibid.*, artikel 5, stk. 2-5.

([944]) *Ibid.*, artikel 2, stk. 2, nr. 11.

([945]) *Ibid.*, artikel 9, stk. 1, og betragtning 67.

([946]) Generel forordning om databeskyttelse, betragtning 156 og 161.

([947]) EDPS (2013), *Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om Kommissionens meddelelse »Handlingsplan for e-sundhed 2012-2020 – et innovativt sundhedsvæsen i det 21. århundrede«*, Bruxelles, 27. marts 2013.

([948]) Kommissionens henstilling af 2. juli 2008 om grænseoverskridende interoperabilitet mellem elektroniske patientjournalsystemer, stk. 3, litra c).

kliniske data om disse personer, såsom tidligere sygehistorie, problemer og lidelser, lægemidler og medicinsk behandling samt resultater og rapporter fra undersøgelser og laboratorieundersøgelser. Disse elektroniske filer, som kan variere fra hele registre til enkelte uddrag eller sammenfatninger, kan tilgås af den praktiserende læge, farmaceuter og andet sundhedspersonale. Disse patientjournaler er også omfattet af begrebet e-sundhed.

Eksempel: A har tegnet en forsikringspolice med virksomhed B, forsikringsgiveren. Sidstnævnte vil indsamle nogle sundhedsrelaterede oplysninger fra A, såsom vedvarende sundhedsproblemer eller sygdomme. Forsikringsgiveren bør lagre A's sundhedsrelaterede personoplysninger særskilt fra andre oplysninger. Forsikringsgiveren skal også lagre de sundhedsrelaterede personoplysninger særskilt fra andre personoplysninger. Dette betyder, at det kun er A's sagsbehandler, som har adgang til A's sundhedsrelaterede oplysninger.

Ikke desto mindre medfører elektroniske patientjournaler visse databeskyttelsesproblemer, såsom deres tilgængelighed, korrekte lagring og adgang for den registrerede.

Udover elektroniske patientjournaler offentliggjorde Europa-Kommissionen den 10. april 2014 en grønbog om mobilsundhedsydelser (m-sundhed), hvor denne fremlagde, at m-sundhed er et nyt og hurtigt voksende område, som har potentialet til at omdanne sundhedspleje og øge dets effektivitet og kvalitet. Begrebet omfatter læge- og folkesundhedspraksis, der understøttes af mobilt udstyr såsom mobiltelefoner, patientovervågningsudstyr, PDA'er (portable digital assistants) og andet trådløst udstyr samt applikationer (for eksempel trivselsapplikationer), som kan forbinde til medicinsk udstyr eller sensorer ([949]). Grønbogen skitserer risiciene for retten til beskyttelse af personoplysninger, som udviklingen af m-sundhed kan medføre, og angiver, at udviklingen, grundet helbredsoplysningers følsomme natur, bør indeholde specifikke og passende sikkerhedsforanstaltninger for patientdata, såsom kryptering og passende patientautentificeringsmekanismer til at mindske sikkerhedsrisici. Overholdelse af regler om beskyttelse af personoplysninger, herunder forpligtelsen om at oplyse den registrerede, datasikkerhed og princippet om lovlig behandling af personoplysninger, er nødvendig for at opbygge

([949]) Europa-Kommissionen (2014), *Grønbog om mobilsundhedsydelser (»m-sundhed«)*, COM(2014) 219 final, Bruxelles, 10. april 2014.

tiltro til m-sundhedsløsninger ([950]). Til dette formål har industrien udarbejdet et adfærdskodeks, som er baseret på bidrag fra en række interessenter, som består af repræsentanter med ekspertise i databeskyttelse, selv- og samregulering, IKT og sundhedspleje ([951]). Ved tidspunktet for håndbogens udarbejdelse er udkastet til adfærdskodeks fremlagt for bemærkninger ved Artikel 29-Gruppen, hvor det afventer en formel godkendelse.

9.4. Databehandling i forskningsmæssigt og statistisk øjemed

Hovedpunkter

- Oplysninger, der indsamles med henblik på videnskabelige eller historiske forskningsformål eller til statistiske formål, må ikke anvendes til noget andet formål.
- Oplysninger, der er indsamlet legitimt til et formål, må derudover anvendes til videnskabelige eller historiske forskningsformål eller til statistiske formål, såfremt der er fastlagt tilstrækkelige garantier. Disse garantier kan sikres ved anonymisering og pseudonymisering inden videregivelse til tredjemand.

EU-retten tillader databehandling til videnskabelige eller historiske forskningsformål eller til statistiske formål, hvis passende garantier for registreredes rettigheder og frihedsrettigheder er fastlagt. Disse kan omfatte pseudonymisering ([952]). EU-retten eller national lovgivning kan fastlægge visse undtagelser fra registreredes rettigheder, hvis det er sandsynligt, at disse rettigheder gør det umuligt eller alvorligt hæmmer at opnå forskningens legitime formål ([953]). Der kan indføres undtagelser fra den registreredes indsigtsret, ret til berigtigelse, ret til begrænsning af behandling og ret til indsigelse.

Selv om oplysninger, som lovligt er indsamlet af en dataansvarlig til et formål, må genanvendes af denne dataansvarlige til dennes egne videnskabelige eller historiske forskningsformål eller til statistiske formål, skal oplysningerne anonymiseres eller gennemgå foranstaltninger såsom pseudonymisering, afhængigt af sammenhængen, inden de videregives til tredjemand til videnskabelige eller historiske

([950]) *Ibid.*, s. 8.

([951]) Draft Code of Conduct on privacy for mobile health applications, 7. juni 2016.

([952]) Generel forordning om databeskyttelse, artikel 89, stk. 1.

([953]) *Ibid.*, artikel 89, stk. 2.

forskningsformål eller til statistiske formål, medmindre den registrerede har givet sit samtykke dertil, eller det specifikt er fastsat ved national lov. Oplysninger, som gennemgår pseudonymisering, er stadig underlagt den generelle forordning om databeskyttelse, hvilket anonyme oplysninger ikke er ([954]).

Forordningen undtager dermed forskningen fra de generelle databeskyttelsesregler for at undgå begrænsning af forskning og udvikling og opfylde målet om at opnå et europæisk forskningsrum som fastsat i artikel 179 i TEUF. Den tillader en bred fortolkning af behandlingen af personoplysninger til videnskabelige formål, herunder teknologisk udvikling og demonstration, grundforskning, anvendt forskning og privat finansieret forskning. Den anerkender også vigtigheden af at indsamle oplysninger i registre til forskningsformål og de potentielle udfordringer ved, at man ved tidspunktet for oplysningernes indsamling ikke fuldstændigt kender til formålet med behandlingen af personoplysninger til videnskabelige forskningsformål ([955]). Af denne årsag tillader forordningen behandling af oplysninger til disse formål uden den registreredes samtykke, såfremt relevante garantier er på plads.

Et vigtigt eksempel på brugen af oplysninger i statistisk øjemed er officielle statistikker, der indsamles af statistiske kontorer på nationalt plan og EU-plan med udgangspunkt i nationale og europæiske love om officiel statistik. I henhold til disse love har borgere og virksomheder normalt pligt til at fremsende oplysninger til de relevante statistiske kontorer. Tjenestemænd ved de statistiske kontorer har særlig tavshedspligt, som nøje skal overholdes, da det er afgørende for borgernes tillid, som er nødvendig, hvis de statistiske kontorer skal have adgang til oplysninger ([956]).

Forordning (EF) nr. 223/2009 om europæiske statistikker (forordning om europæiske statistikker) indeholder vigtige regler om beskyttelse af personoplysninger i officielle statistikker og er derfor også relevant for bestemmelser om officielle statistikker på nationalt plan ([957]). Forordningen fastholder princippet om, at der skal

([954]) *Ibid.*, betragtning 26.

([955]) *Ibid.*, betragtning 33, 157 og 159.

([956]) *Ibid.*, artikel 90.

([957]) Europa-Parlamentets og Rådets forordning (EF) nr. 223/2009 af 11. marts 2009 om europæiske statistikker og om ophævelse af forordning (EF, Euratom) nr. 1101/2008 om fremsendelse af fortrolige statistiske oplysninger til De Europæiske Fællesskabers Statistiske Kontor, Rådets forordning (EF) nr. 322/97 om EF-statistikker og Rådets afgørelse 89/382/EØF, Euratom om nedsættelse af et udvalg for De Europæiske Fællesskabers statistiske program (EUT L 87 af 31.3.2009), som ændret ved Europa-Parlamentets og Rådets forordning (EU) 2015/759 af 29. april 2015 om ændring af forordning (EF) nr. 223/2009 om europæiske statistikker (EUT L 123 af 19.5.2015).

være et tilstrækkeligt præcist retsgrundlag for behandling af oplysninger i officielle statistikker ([958]).

Eksempel: I sagen *Huber mod Bundesrepublik Deutschland* ([959]) klagede en østrigsk forretningsmand, som var flyttet til Tyskland, over, at de tyske myndigheders indsamling og lagring af personoplysninger over udenlandske statsborgere i et centralt register (AZR) i statistiske øjemed overtrådte hans rettigheder under databeskyttelsesdirektivet. Siden direktiv 95/46/EF er beregnet til at sikre et ensartet beskyttelsesniveau i alle medlemsstaterne, fastholdt EU-Domstolen, at nødvendighedsbegrebet fastlagt i artikel 7, litra e), ikke kan tillægges forskelligt indhold i medlemsstaterne for at sikre et højt beskyttelsesniveau i EU. Det er derfor et selvstændigt fællesskabsretligt begreb i EU-retten og skal fortolkes på en måde, som til fulde afspejler målet med direktiv 95/46/EF. EU-Domstolen bemærkede, at anonyme oplysninger burde være tilstrækkeligt til statistiske øjemed, og afsagde dom om, at det tyske register ikke var foreneligt med nødvendighedsbegrebet i artikel 7, litra e).

På baggrund af **Europarådets retsorden** kan viderebehandling af oplysninger finde sted til videnskabelige eller historiske forskningsformål eller til statistiske formål, når dette er i offentlighedens interesse, og det skal være underlagt passende garantier ([960]). Registreredes rettigheder kan også begrænses under behandling af oplysninger i statistiske øjemed, hvis der ikke er nogen identificerbar risiko for overtrædelse af deres rettigheder og frihedsrettigheder ([961]).

Henstillingen vedrørende statistiske oplysninger udstedt i 1997 omhandler udarbejdelsen af statistik i offentlige og private sektorer ([962]).

([958]) Dette princip forklares yderligere i Eurostats adfærdskodeks, som i medfør af artikel 11 i forordning om europæiske statistikker giver etisk vejledning i, hvordan officielle statistikker skal udføres, herunder hensynsfuld anvendelse af personoplysninger.

([959]) EU-Domstolen, C-524/06, *Heinz Huber mod Bundesrepublik Deutschland* [GC], 16. december 2008, se især præmis 68.

([960]) Den moderniserede konvention 108, artikel 5, stk. 4, litra b).

([961]) *Ibid.*, artikel 11, stk. 2.

([962]) Europarådet, Ministerudvalget (1997), henstilling Rec(97)18 til medlemsstaterne om beskyttelse af personoplysninger, der indsamles og behandles i statistisk øjemed, 30. september 1997.

Oplysninger, der indsamles af en dataansvarlig i statistisk øjemed, må ikke anvendes til noget andet formål. Oplysninger, som er indsamlet til andre formål, skal være tilgængelige til videre statistiske formål. Henstillingen vedrørende statistiske oplysninger tillader også videregivelse af oplysninger til tredjeparter, hvis dette udelukkende er i statistiske øjemed. I sådanne tilfælde bør parterne aftale og nedskrive omfanget af den legitime statistiske videreanvendelse. Siden dette ikke kan erstatte den registreredes samtykke — hvis nødvendigt — skal passende garantier være fastlagt i national lovgivning til at minimere risikoen for misbrug af personoplysninger, såsom en forpligtelse om at anonymisere eller pseudonymisere oplysningerne inden videregivelse.

Personer, der arbejder erhvervsmæssigt med statistisk forskning, skal være bundet af tavshedspligt — som det er sædvanligt for officiel statistik –— i henhold til national lov. Dette skal også gælde interviewere og andre indsamlere af personoplysninger, hvis de er beskæftiget med at indsamle oplysninger fra registrerede eller andre personer.

Hvis en statistisk undersøgelse, der anvender personoplysninger, ikke er godkendt ved lov, skal de registrerede muligvis afgive deres samtykke til anvendelsen af deres oplysninger for at gøre anvendelsen lovlig, eller de skal måske have mulighed for at gøre indsigelse. Hvis personoplysninger indsamles i statistisk øjemed af interviewere, skal de interviewede klart oplyses om, hvorvidt videregivelse af oplysninger er påkrævet i henhold til national lov.

Hvis en statistisk undersøgelse ikke kan gennemføres uden anonymiseret data, og der faktisk er behov for personoplysninger, bør oplysninger, der indsamles til dette formål, så vidt muligt anonymiseres. Resultaterne af den statistiske undersøgelse må ikke gøre det muligt at identificere nogen af de registrerede, medmindre dette i realiteten ikke udgør en risiko.

Når den statistiske analyse er afsluttet, bør de anvendte personoplysninger slettes eller anonymiseres. I dette tilfælde foreslår henstillingen vedrørende statistiske oplysninger, at identifikationsoplysninger lagres adskilt fra andre personoplysninger. Dette betyder for eksempel, at krypteringsnøglen eller listen med identificerende synonymer bør lagres adskilt fra de andre oplysninger.

9.5. Finansielle oplysninger

Hovedpunkter

- Selv om finansielle oplysninger ikke er følsomme oplysninger som defineret i den moderniserede konvention 108 eller den generelle forordning om databeskyttelse, kræver behandlingen heraf særlige garantier for at sikre oplysningernes rigtighed og sikkerhed.
- Elektroniske betalingssystemer skal navnlig have indbygget beskyttelse, dvs. indbygget privatlivsbeskyttelse eller databeskyttelse gennem design og standardindstillinger.
- Der opstår særlige databeskyttelsesproblemer på dette område, fordi der er behov for effektive autentifikationsmekanismer.

Eksempel: I sagen *Michaud mod Frankrig* ([963]) anfægtede sagsøgeren, en fransk advokat, sin pligt til i henhold til fransk lovgivning om at indberette mistanker vedrørende hans klienters mulige hvidvaskning af penge. EMD bemærkede, at krav om, at advokater meddeler de administrative myndigheder oplysninger vedrørende en anden person, som vedkommende er kommet i besiddelse af gennem udvekslinger med den pågældende, udgjorde et indgreb i advokaternes ret til respekt for deres korrespondance og privatliv i medfør af artikel 8 i EMRK, da dette begreb også dækker professionelle eller erhvervsmæssige aktiviteter. Indgrebet var dog i overensstemmelse med loven og forfulgte et legitimt formål, nemlig at forebygge uro og kriminalitet. Eftersom advokater kun under meget begrænsede omstændigheder har pligt til at indberette mistænkelig adfærd, fandt EMD, at denne forpligtelse var forholdsmæssig. Domstolen konkluderede, at EMRK's artikel 8 ikke var blevet overtrådt.

Eksempel: I sagen *M.N. m.fl. mod San Marino* ([964]) indgik sagsøgeren, en italiensk statsborger, en forvaltningsaftale med en virksomhed, som var omfattet af en undersøgelse. Dette betød, at virksomheden blev udsat for ransagning og beslaglæggelse af kopier af (elektronisk) dokumentation. Sagsøgeren indsendte en klage til San Marinos domstol, hvor han påstod,

([963]) EMD, *Michaud mod Frankrig*, nr. 12323/11, 6. december 2012. Se også EMD, *Niemietz mod Tyskland*, nr. 13710/88, 16. december 1992, præmis 29, og EMD, *Halford mod Det Forenede Kongerige*, nr. 20605/92, 25. juni 1997, præmis 42.

([964]) EMD, *M.N. m.fl. mod San Marino*, nr. 28005/12, 7. juli 2015.

at der ikke var nogen forbindelse imellem ham og de påståede forbrydelser. Domstolen erklærede dog hans klage for ugyldig, da han ikke var en »interesseret part«. EMD fastholdt, at sagsøgeren havde været dårligt stillet i forhold til domstolsbeskyttelse sammenlignet med en »interesseret part«, men hans oplysninger var stadig genstand for ransagning og beslaglæggelse. Domstolen fastholdt derfor, at artikel 8 var blevet overtrådt.

Eksempel: I sagen *G.S.B. mod Schweiz* ([965]) blev sagsøgerens bankoplysninger sendt til de amerikanske skattemyndigheder på baggrund af den administrative samarbejdsaftale mellem Schweiz og USA. EMD fastholdt, at overførslen ikke overtrådte artikel 8 i EMRK, da indgrebet i sagsøgerens ret til privatlivets fred var fastlagt i lovgivningen, forfulgte et legitimt formål og var forholdsmæssig i forhold til den pågældende samfundsinteresse.

Anvendelsen af den generelle lovramme for databeskyttelse, der er fastsat i konvention 108, i forhold til betalinger blev udviklet af **Europarådet** i henstilling Rec(90)19 fra 1990 ([966]). Denne henstilling præciserer omfanget af lovlig indsamling og anvendelse af oplysninger i forbindelse med betalinger, især ved hjælp af betalingskort. Den forsyner endvidere de nationale lovgivere med detaljerede bestemmelser vedrørende reglerne for meddelelse af betalingsoplysninger til tredjemand, tidsfrister for lagring af oplysninger, gennemsigtighed, datasikkerhed og grænseoverskridende videregivelse af oplysninger samt tilsyn og retsmidler. Europarådet har også udviklet en udtalelse om overførsler af skatteoplysninger ([967]), som tages under overvejelse ved overførsel af skatteoplysninger.

EMD tillader overførsel af finansielle oplysninger – navnlig oplysninger om en enkeltpersons bankkonto – under artikel 8 i EMD, hvis det er fastsat i lovgivningen, forfølger et legitimt formål og er forholdsmæssig i forhold til den pågældende samfundsinteresse ([968]).

Under **EU-retten** skal elektroniske betalingssystemer, der omfatter behandling af personoplysninger, overholde den generelle forordning om databeskyttelse. Disse

([965]) EMD, *G.S.B. mod Schweiz*, nr. 28601/11 22. december 2015.

([966]) Europarådet, Ministerudvalget (1990), henstilling nr. R(90)19 om beskyttelse af personoplysninger, der anvendes ved betaling og andre tilknyttede handlinger, 13. september 1990.

([967]) Europarådet, det rådgivende udvalg for konvention 108 (2014), Opinion on the implication for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes, 4 juni 2014.

([968]) EMD, *G.S.B. mod Schweiz*, nr. 28601/11 , 22. december 2015.

systemer skal derfor sikre databeskyttelse gennem design og gennem standardindstillinger. Databeskyttelse gennem design forpligter den dataansvarlige til at fastlægge passende tekniske og organisatoriske foranstaltninger til at gennemføre databeskyttelsesprincipperne. Data gennem standardindstillinger betyder, at den dataansvarlige skal sikre standardindstillinger, hvormed kun de personoplysninger, der er nødvendige til et bestemt formål, kan behandles (se afsnit 4.4.). EU-Domstolen fastholdt vedrørende finansielle oplysninger, at overførte skatteoplysninger kan udgøre personoplysninger ([969]). Artikel 29-Gruppen udstedte tilknyttede retningslinjer for medlemsstater, herunder kriterier til at sikre overholdelse af databeskyttelsesregler, når personoplysninger af skattemæssige grunde automatisk udveksles via automatiske midler ([970]). Derudover er der vedtaget en række retslige instrumenter til at regulere finansmarkederne samt kreditinstitutters og investeringsselskabers aktiviteter ([971]). Andre retslige instrumenter hjælper med at bekæmpe insiderhandel og markedsmanipulation ([972]). De primære områder, som påvirker databeskyttelse, er:

- opbevaring af registreringer om finansielle transaktioner
- videregivelse af personoplysninger til tredjelande
- optagelse af telefonsamtaler eller elektronisk kommunikation, herunder kompetente myndigheders beføjelser til at anmode om telefon- og datatrafikregistreringer
- videregivelse af personoplysninger, herunder offentliggørelse af sanktioner

([969]) EU-Domstolen, C-201/14, *Smaranda Bara m.fl. mod Casa Națională de Asigurări de Sănătate m.fl.*, 1. oktober 2015, præmis 29.

([970]) Artikel 29-Gruppen (2015), Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes, 14/EN WP 230.

([971]) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014); Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af forordning (EU) nr. 648/2012 (EUT L 173 af 12.6.2014) og Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013).

([972]) Europa-Parlamentets og Rådets forordning (EU) nr. 596/2014 af 16. april 2014 om markedsmisbrug (forordningen om markedsmisbrug) og om ophævelse af Europa-Parlamentets og Rådets direktiv 2003/6/EF og Kommissionens direktiv 2003/124/EF, 2003/125/EF og 2004/72/EF (EUT L 173 af 12.6.2014).

- de kompetente myndigheders tilsyns- og undersøgelsesbeføjelser, herunder kontrolbesøg på stedet og adgang til private lokaler med henblik på beslaglæggelse af dokumenter

- mekanismerne for indberetning af overtrædelser, dvs. whistle blowing-ordninger

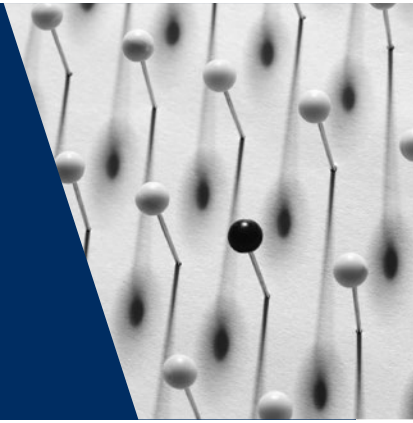
- samarbejdet mellem medlemsstaternes kompetente myndigheder og ESMA (Den Europæiske Værdipapir- og Markedstilsynsmyndighed).

Der er også andre problemstillinger på disse områder, som er specifikt omhandlet, herunder indsamling af oplysninger om registreredes økonomiske status ([973]) eller grænseoverskridende betaling via bankoverførsler, som uundgåeligt medfører videregivelse af personoplysninger ([974]).

([973]) Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 af 16. september 2009 om kreditvurderingsbureauer (EUT L 302 af 17.11.2009), og som senest ændret ved Europa-Parlamentets og Rådets direktiv 2014/51/EU af 16. april 2014 om ændring af direktiv 2003/71/EF og 2009/138/EF samt forordning (EF) nr. 1060/2009, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 for så vidt angår de beføjelser, der er tillagt den europæiske tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger) og den europæiske tilsynsmyndighed (Den Europæiske Værdipapirtilsynsmyndighed) (EUT L 153 af 22.5.2014) og Europa-Parlamentets og Rådets forordning (EU) nr. 462/2013 af 21. maj 2013 om ændring af forordning (EF) nr. 1060/2009 om kreditvurderingsbureauer (EUT L 146 af 31.5.2013).

([974]) Europa-Parlamentets og Rådets direktiv 2007/64/EF af 13. november 2007 om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF (EUT L 319 af 5.12.2007), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/111/EF af 16. september 2009 om ændring af direktiv 2006/48/EF, 2006/49/EF og 2007/64/EF for så vidt angår banker tilsluttet centralorganer, visse komponenter i egenkapitalen, store engagementer, tilsynsordninger og krisestyring (EUT L 302 af 17.11.2009).

10 Nutidens udfordringer med beskyttelse af personoplysninger



Den digitale tidsalder, eller informationsteknologiens tidsalder, er karakteriseret ved den omfattende anvendelse af computere, internettet og digitale teknologier. Det medfører indsamling og behandling af kolossale datamængder, herunder personoplysninger. Indsamlingen og behandlingen af personoplysninger i en globaliseret økonomi betyder, at antallet af grænseoverskridende datastrømme vokser. Denne behandling kan give væsentlige og synlige fordele i dagligdagen: Søgemaskiner giver adgang til enorme mængder af oplysninger og viden, sociale netværkstjenester giver personer over hele verden mulighed for at kommunikere med hinanden, udtrykke holdninger og mobilisere støtte til sociale, miljømæssige og politiske mærkesager, og virksomheder samt forbrugere drager fordel af effektive markedsføringsteknikker, som sætter skub i økonomien. Teknologi og behandling af personoplysninger er også uundværlige værktøjer for statslige myndigheder, når de skal bekæmpe kriminalitet og terrorisme. På samme måde kan big data — indsamling, lagring og analyse af store datamængder for at identificere mønstre og forudsige adfærd — være en væsentlig værdikilde for samfundet, som forbedrer produktivitet, den offentlige sektors resultater og social deltagelse ([975]).

På trods af de mange fordele udgør den digitale tidsalder også udfordringer for privatlivets fred og databeskyttelse, da store mængder af personoplysninger indsamles og behandles på måder, som bliver mere og mere komplekse og uigennemskuelige. Teknologiske fremskridt har ført til udviklingen af enorme datasæt, som nemt kan krydskontrolleres og analyseres yderligere for at lede efter mønstre eller

([975]) Europarådet, det rådgivende udvalg for konvention 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg, 23. januar 2017.

vedtage beslutninger på baggrund af algoritmer, hvilket kan føre til hidtil uset indsigt i menneskets adfærd og privatliv ([976]).

Nye teknologier er kraftfulde og kan være farlige, hvis de bruges af de forkerte. Statslige myndigheder, som udfører masseovervågningsaktiviteter, der gør brug af disse teknologier, er et eksempel på de betydelige følger, som disse teknologier kan have på enkeltpersoners rettigheder. I 2013 gav Edward Snowdens afsløringer om, at visse staters efterretningstjenester gennemførte omfattende overvågningsprogrammer af telefoni og internet, anledning til væsentlige bekymringer om de farer, som overvågningsaktiviteter indebærer for privatliv, demokratisk regeringsførelse og ytringsfrihed. Masseovervågning og teknologier, som muliggør globaliseret lagring og behandling af personoplysninger, og masseadgang til oplysninger kan krænke selve kernen af retten til privatlivets fred ([977]). Derudover kan de have en negativ virkning på politisk kultur og en neddæmpende virkning på demokrati, kreativitet og nytænkning ([978]). Hvis borgere frygter, at staten konstant sporer og analyserer deres adfærd og handlinger, kan det afskrække dem fra at udtrykke deres holdninger om visse emner og føre til varsomhed og forsigtighed ([979]). Disse udfordringer har fået en række offentlige myndigheder, forskningscentre og civilsamfundsorganisationer til at analysere nye teknologiers potentielle konsekvenser for samfundet. I 2015 iværksatte Den Europæiske Tilsynsførende for Databeskyttelse flere initiativer, som var rettet mod at vurdere de etiske følger af big data og Tingenes internet. Navnlig har den oprettet en rådgivende etikgruppe, der sigter mod at sætte gang i »en åben og informeret debat om digital etik, som gør det muligt for EU at opnå fordelene ved teknologien for samfundet og økonomien og samtidig styrker fysiske personers rettigheder og frihedsrettigheder, navnlig deres ret til privatlivets fred og databeskyttelse ([980])«.

([976]) Europa-Parlamentet (2017), Beslutning om big datas indvirkning på de grundlæggende rettigheder: privatlivets fred, databeskyttelse, ikke-forskelsbehandling, sikkerhed og retshåndhævelse, P8_TA-PROV(2017)0076, Strasbourg, 14. marts 2017.

([977]) Se FN's Generalforsamling, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Ben Emmerson, A/69/397, 23. september 2014, stk. 59. Se også EMD, *Factsheet on Mass surveillance*, juli 2017.

([978]) EDPS (2015), *Udfordringerne ved massedata*, udtalelse 7/2015, Bruxelles, 19. november 2015.

([979]) Se navnlig EU-Domstolen, forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014, præmis 37.

([980]) EDPS, Decision of 3 December 2015 establishing an external advisory group on the ethical dimensions of data protection (»the Ethics Advisory Group«), 3. december 2015, betragtning 5.

Behandling af personoplysninger er også et kraftfuldt værktøj i hænderne på virksomheder. I skrivende stund kan det afsløre detaljerede oplysninger om en persons helbredsmæssige eller finansielle situation, hvor disse oplysninger så benyttes af virksomheder til at træffe vigtige beslutninger for enkeltpersoner, såsom den sundhedsforsikringspræmie, som skal gælde for dem, eller deres kreditværdighed. Databehandlingsteknikker kan også påvirke demokratiske processer, når politikere eller virksomheder benytter dem til at påvirke valg – for eksempel igennem mikromålretning af vælgeres kommunikationer. Med andre ord: Selvom privatliv oprindeligt blev betragtet som en ret til at beskytte enkeltpersoner mod ubegrundede indgreb fra offentlige myndigheder, kan denne ret i moderne tid også være truet af private aktørers beføjelser. Dette giver anledning til spørgsmål om brugen af teknologi og prædiktive analyser i forbindelse med beslutninger, der påvirker enkeltpersoners dagligdag, og forstærker behovet for at sikre, at al behandling af personoplysninger respekterer kravene i de grundlæggende rettigheder.

Databeskyttelse er uløseligt forbundet til teknologiske, sociale og politiske forandringer. Det er derfor umuligt at udarbejde en omfattende liste over fremtidige udfordringer. Dette kapitel undersøger udvalgte områder inden for big data, sociale netværk på internettet og EU's digitale indre marked. I stedet for at være en udtømmende vurdering af disse emner ud fra et databeskyttelsesperspektiv fremhæves de mange mulige interaktioner mellem nye eller reviderede menneskelige aktiviteter og databeskyttelse.

10.1. Big data, algoritmer og kunstig intelligens

Hovedpunkter

- Banebrydende innovationer inden for IKT skaber nye levemåder, hvor sociale relationer, forretning, private og offentlige tjenester er digitalt forbundet, hvilket skaber en i stigende grad stor mængde data, mange af dem personoplysninger.
- Regeringer, virksomheder og borgere befinder sig i stigende grad i en datadrevet økonomi, hvor dataene i sig selv er blevet værdifulde aktiver.
- Begrebet big data henviser både til dataene og analyserne heraf.
- Personoplysninger, der behandles i big data-analyser, er omfattet af EU-retten og Europarådets retsorden.

- Afvigelser fra databeskyttelsesregler og -rettigheder er begrænset til bestemte rettigheder og bestemte situationer, hvor håndhævelsen af en rettighed ville være umulig eller pålægge dataansvarlige en uforholdsmæssig arbejdsbyrde.
- Fuldautomatiske afgørelser er generelt forbudt, undtagen i særtilfælde.
- Det er vigtigt, at enkeltpersoner oplyses og gives kontrol, for at sikre håndhævelse af rettigheder.

I vores i stigende grad digitaliserede samfund efterlader alle aktiviteter digitale spor, som kan indsamles, behandles og evalueres eller analyseres. Med nye informations- og kommunikationsteknologier indsamles og registreres der flere og flere oplysninger ([981]). Indtil fornylig var der ikke nogen teknologier, som kunne analysere eller evaluere de store datamængder, eller som var i stand til at drage brugbare konklusioner. Datamængderne var simpelthen for store til, at de kunne evalueres, og for komplekse, dårligt struktureret og tempoet for højt til, at tendenser og vaner kunne identificeres.

10.1.1. Definition af big data, algoritmer og kunstig intelligens

Big data

Begrebet »big data« er et modeord, som kan henvise til flere begreber alt efter omstændighederne. Normalt omfatter det den voksende tekniske evne til at indsamle, behandle og uddrage ny og forudseende viden fra store datamængder, -hastigheder og –variationer ([982]). Begrebet big data omfatter derfor både selve dataene og analyserne heraf.

Datakilderne omfatter forskellige typer, såsom personer og deres personoplysninger, maskiner eller sensorer, klimaoplysninger, satellitbilleder, digitale billeder og videoer eller GPS-signaler. En stor del af dataene og oplysningerne er dog

([981]) Europa-Kommissionen, Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Hen imod en blomstrende datadreven økonomi, COM(2014) 442 final, Bruxelles, 2. juli 2014.

([982]) Europarådet, det rådgivende udvalg for konvention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23. januar 2017, s. 2; Europa-Kommissionen, Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Hen imod en blomstrende datadreven økonomi, COM(2014) 442 final, Bruxelles, 2. juli 2014, s. 4 og Den Internationale Telekommunikationsunion (2015), henstilling Y.3600. Big Data — Cloud computing based requirements and capabilities.

personoplysninger, hvilket kan være et navn, foto, e-mail-adresse, bankoplysninger, GPS-sporingsdata, opslag på sociale medier, medicinske oplysninger eller en computers IP-adresse ([983]).

Big data henviser også til **behandling**, analyse og evaluering af datamængderne og de tilgængelige oplysninger, dvs. for at indhente brugbare oplysninger med henblik på analyse af big data. Dette betyder, at de indsamlede data og oplysninger kan benyttes til andre formål end dem, som oprindeligt var tiltænkt, såsom statistiske tendenser eller mere skræddersyede tjenester, så som reklame. Alle oplysningsformer kan faktisk kombineres og genevalueres, hvor teknologierne er tilstede til at indsamle, behandle og evaluere big data: finansielle transaktioner, kreditværdighed, lægelig behandling, privat forbrug, erhvervsmæssig virksomhed, sporing og anvendte ruter, internetbrug, elektroniske kort og smartphones, video- eller kommunikationsovervågning. Analyse af big data indebærer en ny kvantitativ dimension for data, som kan evalueres og anvendes i realtid, for eksempel til at levere skræddersyede tjenester til forbrugere.

Algoritmer og kunstig intelligens

Kunstig intelligens (AI) henviser til maskiners intelligens, der fungerer som »intelligente agenter«. Visse enheder kan som en intelligent agent og med støtte fra software opfatte deres miljø og træffe handlinger på baggrund af algoritmer. Begrebet AI benyttes, når en maskine efterligner »kognitive« funktioner – såsom læring og problemløsning – som normalt forbindes med fysiske personer ([984]). Moderne teknologier og software benytter algoritmer, som enheder anvender til at træffe »automatiske afgørelser«, til at efterligne beslutningstagning. En algoritme er kort fortalt en trinvis procedure til beregning, databehandling, evaluering og automatisk argumentation og automatiske afgørelser.

Ligesom big data-analyser kræver AI og de automatiske afgørelser, som den tilvejebringer, indsamling og behandling af store datamængder. Disse data kan stamme fra selve enheden (bremsers varmeniveau, brændstof osv.) eller fra det omgivende miljø. Profilering er for eksempel en proces, der kan gøre brug af automatiske afgørelser i medfør af prædefinerede mønstre eller faktorer.

([983]) Europa-Kommissionens faktaark om reformen af EU's databeskyttelsesregler og big data og Europarådet, det rådgivende udvalg for konvention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23. januar 2017, s. 2.

([984]) Stuart Russel og Peter Norvig, *Artificial Intelligence: A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, s. 27, 32–58, 968–972; Stuart Russel og Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, s. 2.

Eksempel: Profilering og målrettede reklamer

Profilering baseret på big data omfatter søgning efter mønstre, der afspejler en personlighedstypes karakteristika – for eksempel foreslår virksomheder under onlineshopping produkter, som du måske også kan lide, på baggrund af oplysninger, der indsamles fra de produkter, som en kunde tidligere har placeret i sin indkøbskurv. Jo flere data, jo tydeligere bliver billedet. En smartphone er for eksempel et omfattende spørgeskema, som enkeltpersoner udfylder ved hver anvendelse, om det er bevidst eller ej.

Moderne psykologi – en videnskab, der studerer personligheder – benytter OCEAN-metoden, hvorudfra den bestemmer de karaktertyper, der er tale om. The Big Five, fem overordnede dimensioner i personligheden, består af åbenhed (hvor åben personen er over for nyt), samvittighedsfuldhed (i hvor stor grad personen er en perfektionist), ekstraversion (hvor udadvendt en person er), venlighed (hvor godmodig en person er) og neuroticisme (hvor sårbar en person er). Disse oplysninger danner en profil over den pågældende, deres behov og bekymringer, deres adfærd osv. Den suppleres derefter med andre oplysninger om personen, der indhentes fra tilgængelige kilder, såsom dataformidlere, sociale netværk (herunder »synes godt om« på opslag og billeder), musik lyttet til på nettet eller GPS- og lokaliseringsdata.

Mængderne af profiler, som udarbejdes via big data-analyseteknikker, sammenlignes derefter for at identificere mønstre og opbygge personlighedsgrupperinger. Oplysninger om bestemte personligheders adfærd og holdninger indgår dermed i en anden sammenhæng. Med adgangen til og brugen af big data er personlighedstesten vendt på hovedet, da oplysninger om adfærd og holdninger nu bruges til at beskrive enkeltpersonens personlighed. Igennem den kombination af oplysninger fra »synes godt om« fra sociale netværk, sporingsdata, musik, som er lyttet til, eller film, som er set, kan der dannes et klart billede over en persons personlighed, hvormed virksomheder kan udsende målrettede reklamer og/eller oplysninger på baggrund af denne persons »personlighed«. Frem for alt kan disse oplysninger behandles i realtid ([985]).

([985]) Behandlingsteknikker og ny software evaluerer oplysningerne om, hvad en person kan lide, kigger på under onlineshopping eller føjer til en online indkøbskurv i realtid, og kan foreslå »produkter«, der kan være af interesse ud fra de indsamlede oplysninger.

10.1.2. Afvejning af fordele og risici ved big data

Moderne behandlingsteknikker kan håndtere store datamængder, hurtigt importere nye, tilvejebringe realtidsbehandling af oplysningerne med kort responstid (selv ved komplekse anmodninger), tilvejebringe muligheden for flere og simultane anmodninger og kan analysere forskellige oplysningstyper (billeder, tekst eller tal). Disse teknologiske innovationer gør det muligt at strukturere, behandle og evaluere datamængder og oplysninger i realtid ([986]). Via en eksponentiel stigning af de datamængder, som er tilgængelige og analyseres, kan man nu opnå resultater, der ikke ville være mulige via analyser med mindre omfang. Big data har bidraget til at udvikle et nyt forretningsområde, som kan skabe nye tjenester for både virksomheder og forbrugere. Værdien af EU-borgeres personoplysninger har potentialet til at vokse til næsten 1 billion EUR om året inden 2020 ([987]). Big data kan derfor på baggrund af evalueringen af massedata tilbyde nye **muligheder** for ny social, økonomisk eller videnskabelig viden, der kan hjælpe enkeltpersoner samt virksomheder og regeringer ([988]).

Big data-analyser kan afsløre mønstre blandt forskellige kilder og datasæt, og dette kan føre til nyttige opdagelser inden for områder som videnskab og medicin. Dette er for eksempel tilfældet inden for områder som sundhed, fødevaresikkerhed, intelligente transportsystemer, energieffektivitet eller byplanlægning. Denne analyse af oplysninger i realtid kan benyttes til at forbedre de implementerede systemer. I forbindelse med forskning kan nye indsigter opnås ved at kombinere store mængder af data og statistiske evalueringer, navnlig inden for fag, hvor store datamængder tidligere kun er blevet evalueret manuelt. Nye behandlinger kan

([986]) Udviklingen af software til behandling af big data er stadig i en tidlig fase. Ikke desto mindre er der fornylig udviklet analytiske programmer, navnlig til analyse af massedata og oplysninger i realtid, som vedrører enkeltpersoners aktiviteter. Muligheden for at analysere og behandle big data på en struktureret måde har medført nye metoder til profilering og målrettede reklamer. Europa-Kommissionen, Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Hen imod en blomstrende datadreven økonomi, COM(2014) 442 final, Bruxelles, 2. juli 2014; Europa-Kommissionens faktaark om reformen af EU's databeskyttelsesregler og big data og Europarådet, det rådgivende udvalg for konvention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23. januar 2017, s. 2.

([987]) Europa-Kommissionens faktaark om reformen af EU's databeskyttelsesregler og big data.

([988]) Den internationale konference for databeskyttelsesmyndigheder og -ansvarlige (2014), resolution om big data og Europa-Kommissionen, Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Hen imod en blomstrende datadreven økonomi, COM(2014) 442 final, Bruxelles, 2. juli 2014, s. 2; Europa-Kommissionens faktaark om »Reformen af EU's databeskyttelsesregler og big data« og Europarådet, det rådgivende udvalg for konvention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23. januar 2017, s. 1.

udvikles og skræddersyes til enkelte patienter på baggrund af sammenligninger med de tilgængelige informationsmængder. Virksomheder håber, at analysen af big data vil gøre dem i stand til at opnå konkurrencefordele, generere potentielle besparelser og skabe nye forretningsområder igennem direkte og individuel kundeservice. Regeringsagenturer håber at opnå forbedringer inden for strafferet. Kommissionens strategi for det digitale indre marked anerkender potentialet for datadrevne teknologier, tjenester og big data til at fungere som en katalysator for økonomisk vækst, nytænkning og digitalisering inden for EU ([989]).

Big data indebærer dog også **risici**, som normalt forbindes med behandlede datas mængder, hastigheder og variationer. Mængde henviser til de behandlede datamængder, variation til datatypernes antal og forskellighed, og hastighed henviser til databehandlingens hastighed. Der opstår særlige overvejelser vedrørende databeskyttelse, navnlig når big data-analyser anvendes på store datasæt til at uddrage ny og forudseende viden med henblik på beslutningstagning vedrørende enkeltpersoner og/eller grupper ([990]). Risiciene for databeskyttelse og privatliv knyttet til big data er fremhævet i udtalelser fra EDPS og Artikel 29-Gruppen, resolutioner fra Europa-Parlamentet og Europarådets politiske retningslinjer ([991]).

Risici kan omfatte fejlhåndtering af big data ved dem med adgang til informationsmængderne via manipulation, forskelsbehandling eller undertrykkelse af enkeltpersoner eller bestemte samfundsgrupper ([992]). Når mængder af personoplysninger eller informationer om enkeltes adfærd indsamles, behandles og evalueres, kan deres udnyttelse føre til væsentlige overtrædelser af grundlæggende rettigheder og frihedsrettigheder, som går videre end retten til respekt for privatliv. Det er ikke muligt at måle nøjagtigt, i hvilket omfang privatlivetsfred og personoplysninger kan

([989]) Europa-Parlamentet (2017), Beslutning af 14. marts 2017 om big datas indvirkning på de grundlæggende rettigheder: privatlivets fred, databeskyttelse, ikke-forskelsbehandling, sikkerhed og retshåndhævelse (2016/2225(INI)).

([990]) Europarådet, det rådgivende udvalg for konvention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23. januar 2017, s. 2.

([991]) Se for eksempel EDPS (2015), *Meeting the Challenges of big data* (udfordringerne ved massedata), udtalelse 7/2015, 19. november 2015; EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data* (effektiv håndhævelse i den digitale økonomi), udtalelse 8/2016, 23. september 2016, Europa-Parlamentet (2016), Beslutning om big datas indvirkning på de grundlæggende rettigheder: privatlivets fred, databeskyttelse, ikke-forskelsbehandling, sikkerhed og retshåndhævelse, P8_TA(2017)0076, Strasbourg, 14. marts 2017 og Europarådet, det rådgivende udvalg for konvention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01, Strasbourg, 23. januar 2017.

([992]) Den internationale konference for databeskyttelsesmyndigheder og -ansvarlige (2014), Resolution on Big Data.

påvirkes. Europa-Parlamentet udpegede, at der mangler metoder til at kunne gennemføre en evidensbaseret vurdering af den samlede virkning af big data, men der er tegn på, at big data-analyser kan have en væsentlig horisontal virkning på tværs af både den offentlige og den private sektor ([993]).

Den generelle forordning om databeskyttelse indeholder bestemmelser om retten til ikke at blive udsat for automatiske afgørelser, herunder profilering ([994]). Problemstillingen med privatliv opstår, når udøvelsen af retten til at gøre indsigelse kræver menneskelig indgriben, som gør det muligt for registrerede at udtrykke deres holdninger og anfægte afgørelsen ([995]). Dette kan medføre udfordringer med at sikre et passende beskyttelsesniveau for personoplysninger, hvis menneskelig indgriben for eksempel ikke er en mulighed, eller når algoritmerne er for komplekse, og den pågældende datamængde for stor, til at give enkeltpersoner begrundelser for bestemte afgørelser og/eller forudgående oplysninger med henblik på at indhente deres samtykke. Et eksempel på brugen af AI og automatiske afgørelser er de nylige udviklinger inden for ansøgninger om realkreditlån eller ansættelsesprocedurer. Ansøgninger afvises ud fra det faktum, at ansøgerne ikke opfylder prædefinerede parametre eller faktorer.

10.1.3. Problemstillinger vedrørende databeskyttelse

I forbindelse med databeskyttelse vedrører de primære problemstillinger både mængden og variationen af de behandlede personoplysninger samt behandlingen og dennes resultater. Indførelsen af komplekse algoritmer og software, som kan omdanne massedata til en ressource til beslutningstagning, påvirker enkeltpersoner og grupper, navnlig i forbindelse med profilering eller klassificering, og giver i sidste ende anledning til mange problemstillinger med databeskyttelse ([996]).

Identifikation af dataansvarlige og databehandlere og deres ansvar

Big data og AI giver anledning til flere spørgsmål vedrørende identifikation af dataansvarlige og databehandlere og deres ansvar: Hvem ejer dataene, når

([993]) Europa-Parlamentet (2017), Beslutning af 14. marts 2017 om big datas indvirkning på de grundlæggende rettigheder: privatlivets fred, databeskyttelse, ikke-forskelsbehandling, sikkerhed og retshåndhævelse (2016/2225(INI)).

([994]) Generel forordning om databeskyttelse, artikel 22.

([995]) *Ibid.*, artikel 22, stk. 3.

([996]) Europarådet, det rådgivende udvalg for konvention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23. januar 2017, s. 2.

datamængden, som indsamles og behandles, er så omfattende? Hvem er den dataansvarlige, når data behandles af intelligente maskiner og software? Hvad er de præcise ansvarsområder for hver aktør i forbindelse med behandlingen? Og til hvilke formål må big data anvendes?

Spørgsmålet om ansvar i forbindelse med AI bliver endnu mere udfordrende, når en AI træffer en afgørelse på baggrund af databehandling, som den selv har udviklet. Den generelle forordning om databeskyttelse fastlægger en lovramme for den dataansvarliges og databehandlerens ansvar. Ulovlig behandling af personoplysninger medfører forpligtelser for den dataansvarlige og databehandleren ([997]). Kunstig intelligens og automatiske afgørelser giver anledning til spørgsmål om, hvem der er ansvarlig for overtrædelser, som påvirker registreredes privatliv, hvor kompleksiteten og mængden af behandlede oplysninger ikke kan fastlægges med sikkerhed. Når AI og algoritmer betragtes som produkter, opstår der et problematisk forhold mellem personligt ansvar, som reguleres under den generelle forordning om databeskyttelse, og produktansvar, som ikke reguleres ([998]). Dette kræver regler om ansvarsområder til at forene personligt ansvar og produktansvar i forbindelse med robotteknologi og AI, herunder, f.eks, automatiske afgørelser ([999]).

Indvirkning på databeskyttelsesprincipper

Arten, analyser og brugen af big data beskrevet ovenfor sætter spørgsmålstegn ved anvendelsen af nogle af de traditionelle, grundlæggende principper i europæisk databeskyttelseslovgivning ([1000]). Disse spørgsmålstegn vedrører primært principperne om lovlighed, dataminimering, formålsbegrænsning og gennemsigtighed.

Princippet om dataminimering kræver, at personoplysninger er tilstrækkelige, relevante og begrænset til det, som er nødvendigt til de formål, de behandles til. Big datas forretningsmodel kan dog være i strid med dataminimering, da modellen kræver mere og mere data til uspecificerede formål.

([997]) Generel forordning om databeskyttelse, artikel 77-79 og artikel 82.

([998]) Europa-Parlamentet, europæiske civilretlige bestemmelser om robotteknologi, Generaldirektoratet for Unionens Interne Politikker (oktober 2016), s. 14.

([999]) Tale fra Roberto Viola under medieseminarer om europæisk lovgivning om robotteknologi ved Europa-Parlamentet. (SPEECH 16/02/2017), meddelelse fra Europa-Parlamentet om en anmodning sendt til Kommissionen vedrørende et forslag til civilretlige bestemmelser om robotteknologi og AI.

([1000]) Europarådet, det rådgivende udvalg for konvention 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg, 23. januar 2017.

Det samme gør sig gældende for princippet om formålsbegrænsning, som kræver, at oplysninger skal behandles til udtrykkeligt angivne formål og ikke må benyttes til formål, som er uforenelige med det oprindelige indsamlingsformål, medmindre denne behandling er baseret på et juridisk grundlag – såsom, men ikke begrænset til, samtykke fra den registrerede (se afsnit 4.1.1.).

Endelig sætter big data også spørgsmålstegn ved princippet om oplysningers rigtighed, da big data-applikationer ofte indsamler oplysninger fra flere kilder uden mulighed for at kontrollere og/eller vedligeholde rigtigheden af de indsamlede oplysninger ([1001]).

Specifikke regler og rettigheder

Den generelle regel om, at personoplysninger, der behandles i forbindelse med big data-analyser, er omfattet af databeskyttelseslovgivningen, er stadig gældende. Specifikke regler eller undtagelser for specifikke sager vedrørende databehandling med komplekse algoritmer er dog stadig gennemført i EU-retten og Europarådets retsorden.

Under Europarådets retsorden tildeler den moderniserede konvention 108 nye rettigheder til den registrerede med henblik på at give denne en mere effektiv kontrol over vedkommendes personoplysninger i massedataenes tidsalder. Dette er for eksempel tilfældet med artikel 9, stk. 1, litra a), c) og d), i den moderniserede konvention i forbindelse med retten til ikke at være underlagt en afgørelse, som i væsentlig grad påvirker den registrerede, udelukkende baseret på automatisk behandling af oplysninger, uden at der tages hensyn til vedkommendes holdninger; retten til efter anmodning at få baggrunden for databehandling at vide, når resultaterne herved påvirker en registreret, samt retten til indsigelse. Andre bestemmelser i den moderniserede konvention 108, navnlig om gennemsigtighed, og yderligere forpligtelser supplerer beskyttelsesmekanismerne fastlagt i den moderniserede konvention 108 til at håndtere digitale udfordringer.

Under EU-retten skal **gennemsigtighed** sikres for al behandling af personoplysninger, bortset fra i de tilfælde angivet i GDPR's artikel 23. Dette er særligt vigtigt i forbindelse med internettjenester og anden kompleks automatisk databehandling, såsom brugen af algoritmer til beslutningstagning. Funktionerne i databehandlingssystemer skal i denne sammenhæng give de registrerede reel mulighed for at

([1001]) EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data* (effektiv håndhævelse i den digitale økonomi), udtalelse 8/2016, 23. september 2016, s. 8.

forstå, hvad der sker med deres oplysninger. For at sikre rimelig og gennemsigtig behandling kræver den generelle forordning om databeskyttelse, at den dataansvarlige forsyner den registrerede med meningsfulde oplysninger omkring den logik, som styrer automatiske afgørelser, herunder profilering ([1002]). I sin henstilling om beskyttelse og fremme af retten til ytringsfrihed og retten til privatlivets fred i forbindelse med netneutralitet anbefalede Ministerudvalget ved Europarådet, at internetudbydere forsyner brugere med tydelige, fuldstændige og offentligt tilgængelige oplysninger omkring alle trafikstyringspraksisser, som kan påvirke brugeres adgang til og distribution af indhold, applikationer eller tjenester ([1003]). Rapporter om trafikstyringspraksisser på internettet, som er udarbejdet af kompetente myndigheder i alle medlemsstater, bør udarbejdes på en åben og gennemsigtig måde og gøres tilgængelig for offentligheden uden vederlag ([1004]).

Dataansvarlige skal både **give** registrerede – enten på det tidspunkt, hvor dataene blev indsamlet fra dem, eller på et andet tidspunkt – specifikke oplysninger vedrørende de indsamlede data og den planlagte behandling (se afsnit 6.1.1.) samt, hvor det er relevant, oplyse dem om forekomsten af processer med automatiske afgørelser og give dem »meningsfulde oplysninger om logikken heri« ([1005]), formålene med og de potentielle konsekvenser ved sådanne processer. Den generelle forordning om databeskyttelse præciserer også (kun i tilfælde, hvor personoplysninger ikke er indhentet fra den registrerede), at den dataansvarlige ikke er forpligtet til at videregive disse oplysninger til den registrerede, når det »viser sig at være umuligt eller vil kræve en uforholdsmæssigt stor indsats at underrette den registrerede« ([1006]), Som Artikel 29-Gruppen understreger i sine *Retningslinjer for automatiseret individuel beslutningstagning og profilering i medfør af forordning 2016/679*, bør behandlingens kompleksitet ikke i sig selv udelukke den dataansvarlige fra at videregive tydelige forklaringer til den registrerede om databehandlingens formål og analyser anvendt under behandlingen ([1007]).

Registreredes ret til at få **adgang til**, **berigtige** og **slette** deres personoplysninger samt deres ret til at **begrænse** behandlingen omfatter ikke en tilsvarende

([1002]) Generel forordning om databeskyttelse, artikel 13, stk. 2, litra f).

([1003]) Europarådet, Ministerudvalget (2016), Recommendation CM/Rec(2016)1 of the Committee of Ministers to the member states on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, 13. januar 2016, stk. 5.1.

([1004]) *Ibid.*, stk. 5.2.

([1005]) Generel forordning om databeskyttelse, artikel 13, stk. 2, litra f), og artikel 14, stk. 2, litra g).

([1006]) *Ibid.*, artikel 14, stk. 5, litra b).

([1007]) Artikel 29-Gruppen, *Retningslinjer for automatiseret individuel beslutningstagning og profilering i medfør af forordning 2016/679*, WP 251, 3. oktober 2017, s. 14.

undtagelse. Dataansvarliges forpligtelse om at underrette den registrerede om enhver berigtigelse eller sletning af deres personoplysninger (se afsnit 6.1.4.) kan også ophæves, når en sådan underretning viser sig at være umulig »eller vil kræve en uforholdsmæssigt stor indsats« ([1008]).

I medfør af GDPR's artikel 21 har registrerede også en ret til at gøre **indsigelse** (se afsnit 6.1.6.) mod enhver behandling af deres personoplysninger, herunder i forbindelse med big data-analyser. Selvom dataansvarlige kan fritages fra denne forpligtelse, hvis de kan påvise vægtige legitime grunde, gælder denne fritagelse ikke ved behandling med henblik på direkte markedsføring.

Dataansvarlige kan også påberåbe sig specifikke undtagelser fra disse rettigheder ved behandling af personoplysninger til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål ([1009]).

GDPR har indført særlige regler i forbindelse med **profilering og automatiske afgørelser**: Artikel 22, stk. 1, fastsætter, at den registrerede »har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende«. Som Artikel 29-Gruppens retningslinjer fremhæver, fastsætter denne artikel et generelt forbud mod fuldstændigt automatiske afgørelser ([1010]). Dataansvarlige kan være fritaget fra et sådant forbud i tre specifikke situationer: Når afgørelsen er: 1) nødvendig for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og en dataansvarlig, 2) hjemlet i EU-ret eller medlemsstaternes nationale ret eller 3) baseret på den registreredes udtrykkelige samtykke ([1011]).

Individuel styring

Kompleksiteten af og manglen på gennemsigtighed i forbindelse med big data-analyser kan kræve en revurdering af opfattelser omkring individuel styring af personoplysninger. Dette bør skræddersyes til den pågældende sociale og teknologiske sammenhæng, hvor der tages hensyn til den enkelte persons mangel på viden. Databeskyttelse i forbindelse med big data bør derfor benytte en bredere fortolkning af styring med brugen af oplysninger, i medfør af hvilken individuel

([1008]) Generel forordning om databeskyttelse, artikel 19.

([1009]) *Ibid*., artikel 89, stk. 2 og 3.

([1010]) Artikel 29-Gruppen, *Retningslinjer for automatiseret individuel beslutningstagning og profilering i medfør af forordning 2016/679*, WP 251, 3. oktober 2017, s. 9.

([1011]) Generel forordning om databeskyttelse, artikel 22, stk. 2.

styring udvikler sig til en mere kompleks proces med flere konsekvensanalyser over risici relateret til brugen af oplysninger ([1012]).

Kvaliteten af anvendelsen af big data afhænger af, i hvor stor grad den kan forudsige fysiske personers (eller forbrugeres) ønsker eller adfærd. De nuværende forudsigelsesmodeller, som er baseret på big data-analyser, finjusteres hele tiden. De seneste udviklinger omfatter ikke bare at bruge oplysninger til at kategorisere personligheder (dvs. adfærd og holdninger), men analyse af adfærd igennem analyser af stemmemønstre og intensiteten, hvormed beskeder skrives, eller kropstemperatur. Alle disse oplysninger kan for eksempel benyttes i realtid sammen med den viden, som opnås ved big data-evalueringer, til at bestemme kreditværdighed under et møde med en repræsentant for banken. Denne bestemmelse er ikke foretaget på baggrund af den enkelte persons kvalifikationer, men ud fra adfærdsmæssige karakteristika opnået igennem analyse og evaluering af big data-oplysninger, såsom at ansøgeren taler med en stærk eller smigrende stemme eller vedkommendes kropssprog eller kropstemperatur.

Profilering og målrettede reklamer er ikke nødvendigvis et problem, hvis den enkelte person er **opmærksom på**, at de udsættes for målrettede reklamer. Profileringbliver et problem, når det benyttes til at manipulere enkeltpersoner, dvs. søgning efter bestemte personligheder eller persongrupper i forbindelse med politiske kampagner. For eksempel kan politiske beskeder, som er tilpasset til modtagernes »personlighed« og holdninger, rettes mod grupper af vælgere, som ikke har besluttet sig. Et andet problem kan være brugen af en sådan profilering til at nægte bestemte personer adgang til varer og tjenester. Én garanti, som kan beskytte mod misbrug af big data og personoplysninger, er pseudonymisering (se afsnit 2.1.1.) ([1013]). Når personoplysninger er fuldstændigt anonyme, dvs. de indeholder ingen oplysninger, der forbinder dem med den registrerede, hører det uden for omfanget af den generelle forordning om databeskyttelse. Samtykke fra registrerede og enkeltpersoner i forbindelse med big data-behandling udgør også en udfordring for databeskyttelseslovgivning. Dette omfatter samtykke til at blive udsat for målrettede reklamer og profilering, som kan begrundes af hensyn til »kundeoplevelsen«, og samtykke til brugen af store mængder personoplysninger til at justere og udvikle informationsbaserede analyseværktøjer. Opmærksomheden, eller mangel på samme, omkring big data-behandling giver anledning til flere spørgsmål vedrørende de metoder, hvormed

([1012]) Europarådet, det rådgivende udvalg for konvention 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg, 23. januar 2017.

([1013]) *Ibid.*, s. 2.

registrerede kan udøve deres rettigheder, da big data-behandling kan gøre brug af både pseudonymiserede og anonymiserede oplysninger, som er underlagt algoritmer. Selvom pseudonymiserede oplysninger er omfattet af den generelle forordning om databeskyttelse, finder forordningen ikke anvendelse for anonymiserede oplysninger. Individuel styring med, og opmærksomhed omkring, behandlingen af registreredes personoplysninger er vigtigt i forbindelse med big data-analyser: Uden disse ting vil den registrerede ikke vide, hvem den dataansvarlige eller databehandleren er, og uden denne viden kan de ikke udøve deres rettigheder effektivt.

10.2. Web 2.0 og 3.0: sociale netværk og Tingenes internet

Hovedpunkter

- Sociale netværkstjenester er online kommunikationsplatforme, som giver enkeltpersoner mulighed for at tilslutte sig eller oprette netværk med ligesindede brugere.
- Tingenes internet er tilslutning af genstande til internettet og den indbyrdes forbindelse imellem genstandene.
- Registreredes samtykke er det mest almindelige retsgrundlag for dataansvarliges lovlige databehandling på sociale netværk.
- Generelt er brugere af sociale netværk beskyttet af undtagelsen for familiemæssige aktiviteter, men denne undtagelse finder dog ikke anvendelse i særlige sammenhænge.
- Udbydere af sociale netværk er ikke beskyttet af undtagelsen for familiemæssige aktiviteter.
- Privatliv gennem design og gennem standardindstillinger er afgørende for at sikre datasikkerhed på området.

10.2.1. Definition af web 2.0 og 3.0

Sociale netværkstjenester

I starten var internettet tiltænkt som et netværk til at forbinde computere med hinanden og sende beskeder med begrænsede muligheder for at udveksle data, hvor websteder udelukkende gav den enkelte person mulighed for passivt at se

indholdet ([1014]). I web 2.0-epoken blev internettet omdannet til et forum, hvor brugere interagerer, samarbejder og genererer input. Denne epoke er karakteriseret ved den bemærkelsesværdige succes og udbredte anvendelse af sociale netværkstjenester, som nu er en essentiel del af mange millioner menneskers dagligdag.

Sociale netværkstjenester eller sociale medier kan bredt defineres som »internetbaserede kommunikationsplatforme, der gør det muligt for enkeltpersoner at tilmelde sig eller oprette netværk af ligesindede brugere« ([1015]). Enkeltpersoner anmodes om at videregive personoplysninger og oprette en profil for at tilmelde sig eller oprette et netværk. Sociale netværkstjenester giver brugere mulighed for at generere digitalt »indhold«, der strækker sig fra billeder og videoer til links til aviser på internettet og personlige opslag, hvor de kan udtrykke deres holdninger. Via disse online kommunikationsplatforme kan brugere interagere og kommunikere med adskillige andre brugere. Endnu vigtigere opkræver de fleste populære sociale netværkstjenester ingen registreringsgebyrer. Sociale netværkstjenester skaber det meste af deres omsætning via målrettede reklamer i stedet for at opkræve tilmeldingsgebyrer fra deres brugere. Annoncører kan have stor gavn af de personoplysninger, som dagligt afsløres på disse websteder. Besiddelse af oplysninger om en brugers alder, køn, placering og interesser gør dem i stand til at nå de »rigtige« personer med deres reklamer.

Europarådets ministerudvalg vedtog en henstilling om beskyttelse af menneskerettigheder i forbindelse med sociale netværkstjenester ([1016]), som i et særskilt afsnit vedrører databeskyttelse og blev suppleret i 2018 af en anden henstilling om internetformidleres roller og ansvarsområder ([1017]).

Eksempel: Nora er meget glad, da hendes partner friede til hende. Hun vil gerne dele de gode nyheder med hendes venner og familie og beslutter at skrive et følelsesbetonet opslag på et socialt netværk, hvor hun giver udtryk for hendes glæde og ændrer hendes forholdsstatus til »forlovet«. I de efterfølgende dage ser Nora nu reklamer for bryllupskjoler og blomsterbutikker, når hun logger ind på hendes konto. Hvorfor gør hun det?

([1014]) Europa-Kommissionen (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

([1015]) Artikel 29-Gruppen (2009), *Udtalelse 5/2009 om internetbaserede sociale netværksaktiviteter*, WP 163, 12. juni 2009, s. 4.

([1016]) Europarådet, Ministerudvalget, Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services, 4. april 2012.

([1017]) Europarådet, Ministerudvalget, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries, 7. marts 2018.

Da blomster- og bryllupskjoleproducenterne oprettede en reklame på Facebook, valgte de bestemte parametre, hvorudfra de kunne nå personer som Nora. Siden Noras profil angiver, at hun er en kvinde, forlovet og bor i Paris tæt på det område, hvor blomster- og bryllupskjolebutikkerne er placeret, får hun omgående reklamerne at se.

Tingenes internet

Tingenes internet repræsenterer det næste skridt inden for internettets udvikling: web 3.0-epoken. Med Tingenes internet kan enheder være forbundet og interagere med andre enheder via internettet. Dette gør indbyrdes forbindelse mellem genstande og personer mulig via kommunikationsnetværk og giver dem mulighed for at rapportere omkring deres status og/eller omgivelsernes status ([1018]). Tingenes internet og forbundne enheder er allerede en realitet og forventes at vokse væsentligt i de næste år med oprettelsen og den videre udvikling af intelligente enheder, som vil føre til intelligente byer, intelligente hjem og intelligente virksomheder.

Eksempel: Tingenes internet kan især være til gavn for sundhedsplejen. Virksomheder har allerede oprettet enheder, sensorer og applikationer, som tillader overvågning af en patients helbred. Via brug af en alarmknap, som kan bæres på kroppen, og andre trådløse, som er sensorer placeret i hjemmet, er det muligt at spore den daglige rutine for ældre, der bor alene, og udsende alarmer, hvis alvorlige forstyrrelser af deres daglige program opdages. Sensorer til falddetektion bruges f.eks. i stor grad af ældre. Disse sensorer kan nøjagtigt detektere fald og meddele den pågældende persons læge og/eller familie om faldet.

Eksempel: Barcelona er et af de mest velkendte eksempler på en intelligent by. Siden 2012 har byen implementeret brugen af innovative teknologier, som har været rettet mod at skabe et intelligent system for offentlig transport, affaldshåndtering, parkering og gadebelysning. Byen bruger f.eks. intelligente skraldespande til at forbedre affaldshåndtering. Disse gør det muligt at overvåge affaldsniveauer og dermed optimere indsamlingsruter. Når skraldespandene er næsten fulde, udsender de signaler via mobilkommunikationsnetværket, der sendes til softwareapplikationen, som

([1018]) Europa-Kommissionen, Kommissionens arbejdsdokument, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19. april 2016.

affaldshåndteringsvirksomheden benytter. Virksomheden kan dermed planlægge den bedste rute til affaldsindsamling, hvor der kun prioriteres og/eller planlægges tømning af de skraldespande, som faktisk skal tømmes.

10.2.2. Afvejning af fordele og risici

Den omfattende udvidelse og succes af sociale netværkstjenester i det seneste årti antyder, at de har **væsentlige fordele**. Målrettede reklamer (som beskrevet i det fremhævede eksempel) er en særdeles nyskabende måde for virksomheder at nå deres publikum på, hvor de tilbydes et mere specifikt marked. Det kan også være i forbrugernes interesse at få vist reklamer, som er mere relevante og interessante. Vigtigst af alt kan sociale netværkstjenester og sociale medier have en positiv virkning på samfundet og på gennemførelse af ændringer. De giver brugere mulighed for at kommunikere, interagere, organisere grupper og begivenheder omkring de emner, som påvirker dem.

På tilsvarende vis forventes Tingenes internet at have væsentlige fordele for økonomien og er en del af EU's strategi om at udvikle et digitalt indre marked. Inden for EU forventes det i 2020, at antallet af forbindelser via Tingenes internet vil stige til seks milliarder. Denne udvidede konnektivitet forventes at medføre vigtige økonomiske fordele igennem udviklingen af innovative tjenester og applikationer, bedre sundhedspleje, bedre forståelse af forbrugeres behov og øget effektivitet.

Grundet de enorme mængder personoplysninger, som genereres af brugere på sociale medier og derefter behandles af tjenesteudbyderne, medfører udvidelsen af sociale netværkstjenester samtidig en **voksende bekymring** om de måder, hvorpå privatliv og personoplysninger kan beskyttes. Sociale netværkstjenester kan udgøre en trussel mod retten til privatlivets fred og retten til ytringsfrihed. Sådanne trusler kan omfatte: en mangel på juridiske og proceduremæssige garantier vedrørende processer, der kan føre til udelukkelse af brugere; utilstrækkelig beskyttelse af børn og unge mod skadeligt indhold eller adfærd; manglende respekt for andres rettigheder; mangel på privatlivsvenlige standardindstillinger og mangel på gennemsigtighed omkring de formål, hvortil personoplysninger indsamles og behandles ([1019]). Europæisk databeskyttelseslovgivning har prøvet at reagere på de privatlivs-/databeskyttelsesmæssige udfordringer, som sociale medier har givet anledning

([1019]) Europarådet, Ministerudvalget, Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services, 4. april 2012.

til. Principper som samtykke, privatliv/databeskyttelse gennem design og gennem standardindstillinger og enkeltpersoners rettigheder er særligt vigtige i forbindelse med sociale medier og netværkstjenester.

I forbindelse med Tingenes internet medfører den enorme mængde personoplysninger, som genereres fra de forskellige forbundne enheder, også risici for privatliv og databeskyttelse. Selvom gennemsigtighed er et vigtigt princip inden for europæisk databeskyttelseslovgivning grundet de mange forbundne enheder, er det ikke altid klart, hvem som er i stand til indsamle, få adgang til og benytte oplysningerne, der er indsamlet fra enheder forbundet via Tingenes internet ([1020]). Under EU-retten og Europarådets retsorden fastlægger gennemsigtighedsprincippet dog en forpligtelse for dataansvarlige om at holde de registrerede informeret i et klart og enkelt sprog omkring, hvordan deres oplysninger anvendes. De gældende risici, regler, garantier og rettigheder for behandlingen af registreredes personoplysninger skal præciseres for disse. Enheder forbundet via Tingenes internet og de mange omfattede behandlingsaktiviteter og oplysninger kan også vanskeliggøre kravet om klart og informeret samtykke til databehandling – når en sådan behandling er baseret på samtykke. Enkeltpersoner mangler ofte forståelsen for den tekniske funktion af en sådan behandling og derfor konsekvenserne af deres samtykke.

En anden stor bekymring er sikkerhed, da forbundne enheder er særligt sårbare over for sikkerhedsrisici. Forbundne enheder har forskellige sikkerhedsniveauer. Da de fungerer uden for den almindelige IT-infrastruktur, kan de mangle regnekraft og lagringskapacitet til at indeholde sikkerhedssoftware eller benytte teknikker, såsom kryptering, pseudonymisering eller anonymisering, til at beskytte brugernes personoplysninger.

Eksempel: I Tyskland har lovgivere besluttet at forbyde et legetøj forbundet til internettet efter stærke bekymringer omkring legetøjets virkning på børns ret til respekt for deres privatliv. Lovgivere mente, at en dukke ved navn Cayla, som var forbundet til internettet, udgjorde skjult aflytningsudstyr. Dukken fungerede ved at sende spørgsmål spurgt af det barn, som leger med den, til en app på en digital enhed, som oversatte denne lydsekvens til tekst og ledte efter et svar på internettet. Appen sendte derefter et svar til dukken, som sagde det til barnet. Igennem denne dukke kunne kommunikationer

([1020]) Den Europæiske Tilsynsførende for Databeskyttelse (2017), *Understanding the Internet of Things*.

fra barnet samt voksne i nærheden optages og videresendes til appen. Hvis dukkens producent ikke havde truffet tilstrækkelige sikkerhedstiltag, kunne enhver bruge dukken til at aflytte samtalerne.

10.2.3. Problemstillinger vedrørende databeskyttelse

Samtykke

I Europa er behandlingen af personoplysninger kun lovlig, hvis den tillades under europæisk databeskyttelseslovgivning. For udbydere af sociale netværkstjenester udgør de registreredes samtykke generelt et retsgrundlag for databehandling. Samtykke skal afgives frivilligt og være specifik, informeret og utvetydig (se afsnit 4.1.1.) ([1021]). »Frivilligt« betyder grundlæggende, at registrerede skal have mulighed for at træffe et reelt og ægte valg. Samtykke er »specifik« og »informeret«, når den er letforståelig og tydeligt og præcist beskriver databehandlingens fulde omfang, formål og konsekvenser. I forbindelse med sociale medier kan der sættes spørgsmålstegn ved, om samtykke er frivilligt, specifikt og informeret for alle de behandlingstyper, som udføres af udbyderen af de sociale netværkstjenester og tredjeparter

Eksempel: Enkeltpersoner skal, for at blive medlem af og få adgang til en social netværkstjeneste, godkende forskellige former for behandling af deres personoplysninger, ofte uden at de præsenteres med de fornødne specifikationer eller alternativer. Et eksempel ville være kravet om at afgive et samtykke til at modtage adfærdsbaserede reklamer for at tilmelde sig en social netværkstjeneste. Som Artikel 29-Gruppen bemærker følgende i dennes udtalelse om definitionen af samtykke: »I betragtning af den betydning, som visse sociale netværk har fået, vil nogle kategorier af brugere (som f.eks. teenagere) acceptere at modtage adfærdsbaserede reklamer for at undgå risikoen for at blive delvist udelukket fra socialt samspil. Brugeren bør stilles i en situation, hvor han har mulighed for at afgive et frivilligt og specifikt samtykke om at modtage adfærdsbaserede reklamer uafhængigt af adgangen til den sociale netværkstjeneste ([1022])«.

([1021]) Generel forordning om databeskyttelse, artikel 4 og artikel 7 og den moderniserede konvention 108, artikel 5.

([1022]) Artikel 29-Gruppen (2011), *Udtalelse 15/2011 om definitionen af samtykke*, WP 187, Bruxelles, 13. juli 2011, s. 18.

Under den generelle forordning om databeskyttelse kan personoplysninger for børn under 16 år principielt ikke behandles på baggrund af deres samtykke ([1023]). Hvis samtykke er et krav for behandlingen, skal det gives af barnets forældre eller værge. Børn er særligt beskyttet grundet det faktum, at de kan være mindre opmærksomme over de risici og konsekvenser, som er involveret i databehandlingen. Dette er meget vigtigt i forbindelse med sociale medier, da børn er mere sårbare over for nogle af de negative følger, som brugen af sociale medier kan have, såsom cybermobning, onlinestalking eller identitetstyveri.

Sikkerhed og privatliv/databeskyttelse gennem design og gennem standardindstillinger

Behandlingen af personoplysninger indebærer sikkerhedsrisici, da der er en konstant mulighed for sikkerhedsbrud, som fører til den hændelige eller ulovlige destruktion, tab, ændring, uautoriseret adgang til eller offentliggørelse af de behandlede personoplysninger. Under europæisk databeskyttelseslovgivning skal dataansvarlige og databehandleren gennemføre passende tekniske og organisatoriske foranstaltninger med det formål at forhindre uautoriseret indgriben i databehandlingsaktiviteter. Udbydere af sociale netværkstjenester, som er omfattet af europæiske databeskyttelsesregler, skal også overholde denne forpligtelse.

Principperne for privatliv/databeskyttelse gennem design og gennem standardindstillinger kræver, at dataansvarlige opretholder sikkerheden ved deres produkters design og automatisk benytter passende indstillinger for privatliv og databeskyttelse. Dette betyder, at når en person beslutter at blive medlem af et socialt netværk, må tjenesteudbyderen ikke automatisk gøre alle oplysninger om den nye bruger af tjenesten tilgængelige for alle sine brugere. Ved tilslutning til tjenesten skal standardindstillingerne for privatliv og databeskyttelse være udformet således, at oplysninger kun kan tilgås af enkeltpersonens udvalgte kontakter. Det skal kun være muligt at give adgang til andre personer end dem i listen, efter at brugeren manuelt har valgt at ændre standardindstillingerne for privatliv og databeskyttelse. Dette kan også have en virkning i tilfælde, hvor et databrud finder sted på trods af de fastlagte sikkerhedsforanstaltninger. I sådanne tilfælde skal tjenesteudbydere meddele de påvirkede brugere, hvis det med sandsynlighed medfører en høj risiko for den registreredes rettigheder og frihedsrettigheder ([1024]).

([1023]) Se generel forordning om databeskyttelse, artikel 8. EU-medlemsstater kan ved lov fastlægge en lavere alder, hvis denne ikke er under 13 år.

([1024]) *Ibid*., artikel 34.

Privatliv/databeskyttelse gennem design og gennem standardindstillinger er særligt vigtigt i forbindelse med sociale netværkstjenester, da deling af personoplysninger på sociale medier medfører yderligere sikkerhedsrisici, udover de risici for uautoriseret adgang, som er tilstede i de fleste behandlingstyper. Disse skyldes ofte enkeltpersoners manglende forståelse af *hvem*, som har adgang til deres oplysninger, og hvordan disse personer kan bruge dem. Med den udbredte anvendelse af sociale medier er antallet af hændelser med og ofre for identitetstyveri steget.

Eksempel: Identitetstyveri er et fænomen, hvormed en person opnår oplysninger, data eller dokumenter, som tilhører en anden person (ofret), og derefter bruger disse oplysninger til at imitere ofret for at anskaffe sig varer og tjenester i ofrets navn. Vi kan bruge Poul som eksempel. Han har en konto på et websted for et socialt medie. Poul er lærer og aktivt medlem af sit lokalsamfund, meget udadvendt og ikke særligt bekymret over indstillingerne for privatliv og databeskyttelse i sin konto på det sociale medie. Han har en stor liste over kontakter, og nogle af disse er personer, han ikke nødvendigvis kender personligt. Da han arbejder på en stor skole og har været meget populær som træner for skolens fodboldhold, tænker han, at disse personer sandsynligvis er forældre eller har et tilhørsforhold til skolen. Pouls e-mailadresse og fødselsdato er vist på hans konto på det sociale medie. Desuden laver Poul regelmæssige opslag med billeder af hans hund, Toby, som er ledsaget af kommentarer som »Mig og Toby på vores morgenløbetur«. Poul har ikke tænkt over, at et af de mest populære sikkerhedsspørgsmål til at beskytte ens e-mailkonto eller mobiltelefon er: »Hvad er dit kæledyrs navn?«. Ved brug af de oplysninger, som er tilgængelige på Pouls profil på det sociale medie, kan Niels nemt hacke Pouls konti.

Enkeltpersoners rettigheder

Udbydere af sociale netværkstjenester skal respektere enkeltpersoners rettigheder (se afsnit 6.1.), herunder retten til at blive oplyst om behandlingens formål, og hvordan personoplysninger kan benyttes til direkte markedsføring. Enkeltpersoner skal også tildeles adgang til de personoplysninger, som de har genereret på platformen til det sociale netværk, og de skal have mulighed for at anmode om sletning heraf. Selv når personer har afgivet samtykke til behandlingen af personoplysninger og uploadet oplysninger online, skal de have mulighed for at bede om at »blive glemt«, hvis de ikke længere ønsker at modtage det sociale netværks tjenester. Retten til dataportabilitet giver brugere yderligere muligheder for at modtage en kopi af de

personoplysninger, de har oplyst til udbyderen af sociale netværkstjenester, på et struktureret, almindeligt anvendt, maskinlæsbart format og for at overføre deres oplysninger fra én udbyder af sociale netværkstjenester til en anden ([1025]).

Dataansvarlige

Et svært spørgsmål, som ofte opstår i forbindelse med sociale medier, er spørgsmålet om, hvem den dataansvarlige er: Altså hvem er personen, som er forpligtet til og ansvarlig for at overholde databeskyttelsesreglerne. Udbydere af sociale netværkstjenester betragtes som dataansvarlige i medfør af europæisk databeskyttelseslovgivning. Dette følger af den brede definition af »dataansvarlig« og det faktum, at disse tjenesteudbydere fastsætter formålet med og midlerne til behandlingen af personoplysningerne, som deles af enkeltpersoner. Dataansvarlige skal under EU-retten, hvis de tilbyder tjenester til registrerede i EU, overholde bestemmelserne i den generelle forordning om databeskyttelse, selv hvis de ikke er etableret i EU.

Kan brugere af sociale netværkstjenester også betragtes som dataansvarlige? Når enkeltpersoner behandler personoplysninger »som led i rent personlige eller familiemæssige aktiviteter«, finder databeskyttelsesregler ikke anvendelse. Dette er i europæisk databeskyttelseslovgivning betegnet som undtagelsen for familiemæssige aktiviteter. I nogle tilfælde kan en bruger af en social netværkstjeneste dog ikke være omfattet af undtagelsen for familiemæssige aktiviteter.

Brugere deler deres personoplysninger frivilligt over internettet. Oplysninger, som deles online, indeholder dog ofte personoplysninger om andre personer.

Eksempel: Poul har en konto på en meget populær platform til et socialt netværk. Poul prøver at blive skuespiller og bruger sin konto til at lave opslag med billeder, videoer og beskeder, hvor han forklarer sin lidenskab for kunst. Da popularitet er vigtigt for hans fremtid, har han besluttet, at hans profil ikke kun skal være tilgængelig for hans egen kontaktliste men alle internetbrugere, uanset om de er brugere af netværket eller ej. Kan Poul lave opslag med billeder og videoer med sig selv og sin ven Sara uden hendes samtykke? Som folkeskolelærer forsøger Sara at holde sit privatliv adskilt fra hendes arbejdsgiver, hendes studerende og deres forældre. Der kunne opstå en situation, hvor Sara, som ikke bruger sociale netværk, får at vide

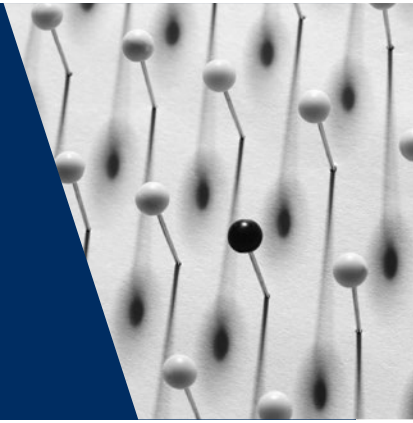
([1025]) Generel forordning om databeskyttelse, artikel 21.

fra deres fælles bekendte, Niels, at Poul har offentliggjort et billede af hende fra en fest på internettet. I så fald vil Pouls databehandling ikke høre under EU-retten, da den er omfattet af undtagelsen for familiemæssige aktiviteter.

Det er dog stadig vigtigt, at brugere er opmærksomme på og tænker over, at offentliggørelse af oplysninger om andre personer uden deres samtykke kan krænke disse personers rettigheder til privatliv og databeskyttelse. Selv i tilfælde, hvor undtagelsen for familiemæssige aktiviteter gælder – hvis en bruger for eksempel har en profil, som kun offentliggøres for en liste over kontakter, denne har udvalgt – kan brugeren stadig være ansvarlig ved offentliggørelse af personoplysninger om andre. Selvom databeskyttelsesregler ikke finder anvendelse, hvis undtagelsen for familiemæssige aktiviteter er gældende, kan der opstå forpligtelser som følge af anvendelsen af andre nationale regler, såsom injurier eller krænkelse af personlige rettigheder. Endelig er det kun brugerne af de sociale netværkstjenester, der er beskyttet af undtagelsen for familiemæssige aktiviteter: Dataansvarlige og databehandlere, som tilbyder midlerne til en sådan privat behandling, er omfattet af europæisk databeskyttelseslovgivning ([1026]).

Med reformen af direktivet om databeskyttelse inden for elektronisk kommunikation vil de regler om databeskyttelse, privatliv og sikkerhed, som finder anvendelse for udbydere af telekommunikationstjenester under de nuværende lovrammer, også finde anvendelse for maskine-til-maskine-kommunikationer og elektroniske kommunikationstjenester, herunder, f.eks., »over the top«-tjenester.

([1026]) *Ibid.*, betragtning 18.



Yderligere materiale

Kapitel 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Wien, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. »Four fundamental rights: finding the balance«, *International Data Privacy Law*, bind 6, nr. 3, s. 195–209.

EDRi, *An introduction to data protection*, Bruxelles.

Frowein, J. og Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. og Gellert, G. (2012), »The fundamental right of data protection in the European Union: in search of an uncharted right«, *International Review of Law, Computers and Technology*, bind 26(1), s. 73–82.

Grabenwarter, C. og Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. og Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. og Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), »EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation«.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Kokott, J. og Sobotta, C. (2013), »The distinction between privacy and data protection in the case law of the CJEU and the ECtHR«, *International Data Privacy Law*, bind 3, nr. 4, s. 222-228.

Kranenborg, H. (2015), »Google and the Right to be Forgotten«, *European Data Protection Law Review*, bind 1, nr. 1, s. 70-79.

Lynskey, O. (2014), »Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order«, *International and Comparative Law Quarterly*, bind 63, nr. 3, s. 569-97.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. og Hofstätter, T. (2012), *All human rights for all — Vienna manual on human rights*, Antwerpen, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. og Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruxelles, Emile Bruylant.

Simitis, S. (1997), »Die EU-Datenschutz-Richtlinie — Stillstand oder Anreiz?«, *Neue Juristische Wochenschrift*, nr. 5, s. 281-288.

Warren, S. og Brandeis, L. (1890), »The right to privacy«, *Harvard Law Review,* bind 4, nr. 5, s. 193-220.

White, R. og Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Kapitel 2

Acquisty, A., og Gross R. (2009), »Predicting Social Security numbers from public data«, *Proceedings of the National Academy of Science*, 7. juli 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., og Blondel V. D. (2013), »Unique in the Crowd: the Privacy Bounds of Human Mobility«, *Nature Scientific Reports*, bind 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. og Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), »Broken promises of privacy: Responding to the surprising failure of anonymization«, *UCLA Law Review*, bind 57, nr. 6, s. 1701-1777.

Samarati, P. og Sweeney, L. (1998), »Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression«, teknisk rapport SRI-CSL-98-04.

Sweeney, L. (2002), »K-Anonymity: A Model for Protecting Privacy« *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, bind 10, nr. 5, s. 557-570.

Tinnefeld, M., Buchner, B. og Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), Anonymisation: managing data protection risk. *Code of practice*.

Kapitel 3 til 6

Brühann, U. (2012), »Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr« i: Grabitz, E., Hilf, M. og Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. og Kaye, J. (2010), »Revoking consent: a »blind spot« in data protection law?«, *Computer Law & Security Review*, bind 26, nr. 3 s. 273-283.

Dammann, U. og Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. og Papakonstantinou, V. (2012), »The Police and Criminal Justice Data Protection Directive: Comment and Analysis«, *Computers & Law Magazine of SCL*, bind 22, nr. 6, s. 1-5.

De Hert, P. og Papakonstantinou, V. (2012), »The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals«, *Computer Law & Security Review*, bind 28, nr. 2, s. 130-142.

Feretti, Federico (2012), »A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously«, *European Review of Private Law*, bind 20, nr. 2, s. 473-506.

FRA ((Den Europæiske Unions Agentur for Grundlæggende Rettigheder) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Den Europæiske Unions Publikationskontor (Publikationskontoret).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (konferenceudgave), Wien, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publikationskontoret.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. og Saxby, S. (2011), »30 years on – The review of the Council of Europe Data Protection Convention 108«, *Computer Law & Security Review*, bind 27, nr. 3, s. 223-231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, Privacy Impact Assessment.

Kapitel 7

Artikel 29-Gruppen (2005), *Arbejdsdokument om en ensartet fortolkning af artikel 26, stk. 1, i direktiv 95/46/EF af 24. oktober 1995*.

Den Europæiske Tilsynsførende for Databeskyttelse (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. og Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kapitel 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

De Hert, P. og Papakonstantinou, V. (2012), »The Police and Criminal Justice Data Protection Directive: Comment and Analysis«, *Computers & Law Magazine of SCL*, bind 22, nr. 6, s. 1-5.

Drewer, D. og Ellermann, J. (2012), »Europol's data protection framework as an asset in the fight against cybercrime«, *ERA Forum*, bind 13, nr. 3, s. 381-395.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Europol (2012), *Data Protection at Europol*, Luxembourg, Publikationskontoret.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. og De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. og Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), »Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem«, *European Law Review*, bind 36, nr. 5, s. 722-776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Kapitel 9

Büllesbach, A., Gijrath, S., Poullet, Y. og Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Poullet, Y. og De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. og Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Gutwirth, S., Leenes, R., De Hert, P. og Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Konstadinides, T. (2011), »Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem«, *European Law Review*, bind 36, nr. 5, s. 722-776.

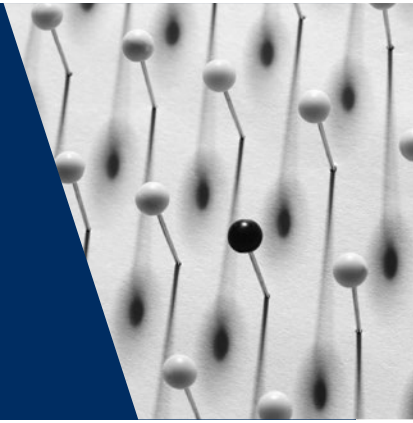
Rosemary, J. og Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Kapitel 10

El Emam, K. og Álvarez, C. (2015), »A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques«, *International Data Privacy Law*, bind 5, nr. 1, s. 73-87.

Mayer-Schönberger, V. og Cate, F. (2013), »Notice and consent in a world of Big Data«, *International Data Privacy Law*, bind 3, nr. 2, s. 67–73.

Rubistein, I. (2013), 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law*, bind 3, nr. 2, s. 74-87.



Retspraksis

Eksempler på Den Europæiske Menneskerettighedsdomstols retspraksis

Adgang til personoplysninger
Gaskin mod Det Forenede Kongerige, nr. 10454/83, 7. juli 1989
Godelli mod Italien, nr. 33783/09, 25. september 2012
K.H. m.fl. mod Slovakiet, nr. 32881/04, 28. april 2009
Leander mod Sverige, nr. 9248/81, 26. marts 1987
M.K. mod Frankrig, nr. 19522/09, 18. april 2013
Odièvre mod Frankrig [GC], nr. 42326/98, 13. februar 2003

Afvejning af databeskyttelse i forhold til ytringsfrihed og retten til information
Axel Springer AG mod Tyskland [GC], nr. 39954/08, 7. februar 2012
Bohlen mod Tyskland, nr. 53495/09, 19. februar 2015
Coudec og Hachette Filipacchi Associés mod Frankrig [GC], nr. 40454/07, 10. november 2015
Magyar Helsinki Bizottság mod Ungarn [GC], nr. 18030/11, 8. november 2016
Müller m.fl. mod Schweiz, nr. 10737/84, 24. maj 1988
Satakunnan Markkinapörssi Oy og Satamedia Oy mod Finland, nr. 931/13, 27. juni 2017
Vereinigung bildender Künstler mod Østrig, nr. 68354/01, 25. januar 2007
Von Hannover mod Tyskland (nr. 2) [GC], nr. 40660/08 og 60641/08, 7. februar 2012

Afvejning af databeskyttelse i forhold til religionsfrihed
Sinan Işık mod Tyrkiet, nr. 21924/05, 2. februar 2010

Udfordringer i forbindelse med databeskyttelse på internettet
K.U. mod Finland, nr. 2872/02, 2. december 2008

Den registreredes samtykke
Elberte mod Letland, nr. 61243/08, 13. januar 2015
Sinan Işık mod Tyrkiet, nr. 21924/05, 2. februar 2010
Y mod Tyrkiet, nr. 648/10, 17. februar 2015

Korrespondance
Amann mod Schweiz [GC], nr. 27798/95, 16. februar 2000
Association for European Integration and Human Rights og Ekimdzhiev mod Bulgarien, nr. 62540/00, 28. juni 2007
Bernh Larsen Holding AS m.fl. mod Norge, nr. 24117/08, 14. marts 2013
Cemalettin Canli mod Tyrkiet, nr. 22427/04, 18. november 2008
D.L. mod Bulgarien, nr. 7472/14, 19. maj 2016
Dalea mod Frankrig, nr. 964/07, 2. februar 2010
Gaskin mod Det Forenede Kongerige, nr. 10454/83, 7. juli 1989
Haralambie mod Rumænien, nr. 21737/03, 27. oktober 2009
Khelili mod Schweiz, nr. 16188/07, 18. oktober 2011
Leander mod Sverige, nr. 9248/81, 26. marts 1987
Malone mod Det Forenede Kongerige, nr. 8691/79, 2. august 1984
Rotaru mod Rumænien [GC], nr. 28341/95, 4. maj 2000
S. og Marper mod Det Forenede Kongerige [GC], nr. 30562/04 og 30566/04, 4. december 2008
Shimovolos mod Rusland, nr. 30194/09, 21. juni 2011
Silver m.fl. mod Det Forenede Kongerige, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marts 1983
The Sunday Times mod Det Forenede Kongerige, nr. 6538/74, 26. april 1979

Strafferegistre
Aycaguer mod Frankrig, nr. 8806/12, 22. juni 2017
B.B. mod Frankrig, nr. 5335/06, 17. december 2009
Brunet mod Frankrig, nr. 21010/10, 18. september 2014
M.K. mod Frankrig, nr. 19522/09, 18. april 2013
M.M. mod Det Forenede Kongerige, nr. 24029/07, 13. november 2012

Datasikkerhed
Haralambie mod Rumænien, nr. 21737/03, 27. oktober 2009
K.H. m.fl. mod Slovakiet, nr. 32881/04, 28. april 2009

DNA-databaser
S. og Marper mod Det Forenede Kongerige [GC], nr. 30562/04 og 30566/04, 4. december 2008

GPS-data
Uzun mod Tyskland, nr. 35623/05, 2. september 2010

Helbredsoplysninger
Avilkina m.fl. mod Rusland, nr. 1585/09, 6. juni 2013
Biriuk mod Litauen, nr. 23373/03, 25. november 2008
I mod Finland, nr. 20511/03, 17. juli 2008
L.H. mod Letland, nr. 52019/07, 29. april 2014
L.L. mod Frankrig, nr. 7508/02, 10. oktober 2006
M.S. mod Sverige, nr. 20837/92, 27. august 1997
Szuluk mod Det Forenede Kongerige, nr. 36936/05, 2. juni 2009
Y mod Tyrkiet, nr. 648/10, 17. februar 2015
Z mod Finland, nr. 22009/93, 25. februar 1997

Identitet
Ciubotaru mod Moldova, nr. 27138/04, 27. april 2010
Godelli mod Italien, nr. 33783/09, 25. september 2012
Odièvre mod Frankrig [GC], nr. 42326/98, 13. februar 2003

Information om erhvervsmæssige aktiviteter
G.S.B. mod Schweiz, nr. 28601/11, 22. december 2015
M.N. m.fl. mod San Marino, nr. 28005/12, 7. juli 2015
Michaud mod Frankrig, nr. 12323/11, 6. december 2012
Niemietz mod Tyskland, nr. 13710/88, 16. december 1992

Opfangelse af kommunikation
Amann mod Schweiz [GC], nr. 27798/95, 16. februar 2000
Brito Ferrinho Bexiga Villa-Nova mod Portugal, nr. 69436/10, 1. december 2015
Copland mod Det Forenede Kongerige, nr. 62617/00, 3. april 2007
Halford mod Det Forenede Kongerige, nr. 20605/92, 25. juni 1997
Iordachi m.fl. mod Moldova, nr. 25198/02, 10. februar 2009

Kopp mod Schweiz, nr. 23224/94, 25. marts 1998
Liberty m.fl. mod Det Forenede Kongerige, nr. 58243/00, 1. juli 2008
Malone mod Det Forenede Kongerige, nr. 8691/79, 2. august 1984
Mustafa Sezgin Tanrıkulu mod Tyrkiet, nr. 27473/06, 18. juli 2017
Pruteanu mod Rumænien, nr. 30181/05, 3. februar 2015
Szuluk mod Det Forenede Kongerige, nr. 36936/05, 2. juni 2009

Forpligtelser for »duty bearers«
B.B. mod Frankrig, nr. 5335/06, 17. december 2009
I mod Finland, nr. 20511/03, 17. juli 2008
Mosley mod Det Forenede Kongerige, nr. 48009/08, 10. maj 2011

Personoplysninger
Amann mod Schweiz [GC], nr. 27798/95, 16. februar 2000
Bernh Larsen Holding AS m.fl. mod Norge, nr. 24117/08, 14. marts 2013
Uzun mod Tyskland, nr. 35623/05, 2010

Fotos
Sciacca mod Italien, nr. 50774/99, 11. januar 2005
Von Hannover mod Tyskland, nr. 59320/00, 24. juni 2004

Retten til at blive glemt
Satakunnan Markkinapörssi Oy og Satamedia Oy mod Finland, nr. 931/13, 27. juni 2017
Segerstedt-Wiberg m.fl. mod Sverige, nr. 62332/00, 6. juni 2006

Ret til indsigelse
Leander mod Sverige, nr. 9248/81, 26. marts 1987
M.S. mod Sverige, nr. 20837/92, 27. august 1997
Mosley mod Det Forenede Kongerige, nr. 48009/08, 10. maj 2011
Rotaru mod Rumænien [GC], nr. 28341/95, 4. maj 2000
Sinan Işık mod Tyrkiet, nr. 21924/05, 2. februar 2010

Følsomme oplysninger
Brunet mod Frankrig, nr. 21010/10, 18. september 2014
I mod Finland, nr. 20511/03, 17. juli 2008
Michaud mod Frankrig, nr. 12323/11, 6. december 2012
S. og Marper mod Det Forenede Kongerige [GC], nr. 30562/04 og 30566/04, 4. december 2008

Tilsyn og håndhævelse (forskellige aktørers rolle, herunder tilsynsmyndigheder)
I mod Finland, nr. 20511/03, 17. juli 2008
K.U. mod Finland, nr. 2872/02, 2. december 2008
Von Hannover mod Tyskland, nr. 59320/00, 24. juni 2004
Von Hannover mod Tyskland (nr. 2) [GC], nr. 40660/08 og 60641/08, 7. februar 2012

Overvågningsmetoder
Allan mod Det Forenede Kongerige, nr. 48539/99, 5. november 2002
Association for European Integration and Human Rights og Ekimdzhiev mod Bulgarien, nr. 62540/00, 28. juni 2007
Bărbulescu mod Rumænien [GC], nr. 61496/08, 5. september 2017
D.L. mod Bulgarien, nr. 7472/14, 19. maj 2016
Dragojević mod Kroatien, nr. 68955/11, 15. januar 2015
Karabeyoğlu mod Tyrkiet, nr. 30083/10, 7. juni 2016
Klass m.fl. mod Tyskland, nr. 5029/71, 6. september 1978
Roman Zakharov mod Rusland [GC], nr. 47143/06, 4. december 2015
Rotaru mod Rumænien [GC], nr. 28341/95, 4. maj 2000
Szabo og Vissy mod Ungarn, nr. 37138/14, 12. januar 2016
Taylor-Sabori mod Det Forenede Kongerige, nr. 47114/99, 22. oktober 2002
Uzun mod Tyskland, nr. 35623/05, 2. september 2010
Versini-Campinchi og Crasnianski mod Frankrig, nr. 49176/11, 16. juni 2016
Vetter mod Frankrig, nr. 59842/00, 31. maj 2005
Vukota-Bojić mod Schweiz, nr. 61838/10, 18. oktober 2016

Videoovervågning
Köpke mod Tyskland (dec.), nr. 420/07, 5. oktober 2010
Peck mod Det Forenede Kongerige, nr. 44647/98, 28. januar 2003

Stemmeprøver
P.G. og J.H. mod Det Forenede Kongerige, nr. 44787/98, 25. september 2001
Wisse mod Frankrig, nr. 71611/01, 20. december 2005

Eksempler på Den Europæiske Unions Domstols retspraksis

Retspraksis vedrørende databeskyttelsesdirektivet

Forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) og Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado*, 24. november 2011

[Korrekt gennemførelse af databeskyttelsesdirektivets artikel 7, litra f), — »andres legitime interesser« — i national lovgivning]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) mod Netlog NV*, 16. februar 2012

[Forpligtelser for udbydere af sociale netværk til at forhindre netværksbrugeres ulovlige brug af musik og audiovisuelle værker]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce mod Salvatore Manni*, 9. marts 2017

[Retten til sletning af personoplysninger; retten til at gøre indsigelse mod behandling]

C-553/07, *College van burgemeester en wethouders van Rotterdam mod M. E. E. Rijkeboer*, 7. maj 2009

[Den registreredes ret til indsigt]

C-101/01, *Straffesag mod Bodil Lindqvist*, 6. november 2003

[Særlige kategorier af personoplysninger]

C-543/09, *Deutsche Telekom AG mod Bundesrepublik Deutschland*, 5. maj 2011

[Nødvendigheden af fornyet samtykke]

Forenede sager C-293/12 og C-594/12, *Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl.* og *Kärntner Landesregierung m.fl.* [GC], 8. april 2014

[Overtrædelse af EU's primære lov ved datalagringsdirektivet; lovlig behandling; formål og opbevaringsbegrænsning]

C-518/07, *Europa-Kommissionen mod Forbundsrepublikken Tyskland* [GC], 9. marts 2010

[De nationale tilsynsmyndigheders uafhængighed]

C-288/12 , *Europa-Kommissionen mod Ungarn* [GC], 8. april 2014
[Berettigelsen af at afskedige den nationale tilsynsmyndighed for databeskyttelse]

C-614/10 , *Europa-Kommissionen mod Republikken Østrig* [GC], 16. oktober 2012
[De nationale tilsynsmyndigheders uafhængighed]

C-212/13, *František Ryneš mod Úřad pro ochranu osobních údajů*, 11. december 2014
[Begreberne »databehandling« og »registeransvarlig« (nu kaldet dataansvarlig)]

C-131/12, *Google Spain SL og Google Inc. mod Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [GC], 13. maj 2014
[Ansvaret for udbydere af søgemaskiner til efter anmodning fra den registrerede at undlade at vise personoplysninger i søgeresultaterne; databeskyttelsesdirektivets anvendelsesområde; begrebet »databehandling«; betydningen af »registeransvarlig« (nu kaldet dataansvarlig); afvejning af databeskyttelse med ytringsfrihed; retten til at blive glemt]

C-524/06, *Heinz Huber mod Bundesrepublik Deutschland* [GC], 16. december 2008
[Berettigelsen i at besidde oplysninger om udlændinge i et statistisk register]

C-473/12, *Institut professionnel des agents immobiliers (IPI) mod Geoffrey Englebert m.fl.*, 7. november 2013.
[Retten til at blive underrettet om behandling af personoplysninger]

C-362/14, *Maximillian Schrems mod Data Protection Commissioner* [GC], 6. oktober 2015
[Princippet om lovlig behandling; grundlæggende rettigheder; ugyldighedserklæringen af safe harbour-beslutningen; de uafhængige tilsynsmyndigheders beføjelser]

C-291/12, *Michael Schwarz mod Stadt Bochum*, 17. oktober 2013
[Anmodning om præjudiciel afgørelse; område med frihed, sikkerhed og retfærdighed; biometrisk pas; fingeraftryk; retsgrundlag; proportionalitet]

C-582/14, *Patrick Breyer mod Bundesrepublik Deutschland*, 19. oktober 2016
[Begrebet »personoplysninger«; opbevaring hos en udbyder af online-medietjenester; national lovgivning, der ikke tillader en hensyntagen til den legitime interesse, som den dataansvarlige forfølger]

C-434/16, *Peter Nowak mod Data Protection Commissioner*, afgørelse fra generaladvokat J. Kokott, 20. juli 2017

[Begrebet personoplysninger; indsigt i egen prøvebesvarelse; rettelser og kommentarer]

T-462/12 R, *Pilkington Group Ltd mod Europa-Kommissionen*, kendelse afsagt af Rettens præsident, 11. marts 2013

C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU* [GC], 29. januar 2008

[Begrebet »personoplysninger«; internetudbyderes forpligtelse om at afsløre identiteten af brugere af KaZaA-fildelingsprogrammer til foreninger for intellektuel ejendomsret]

Forenede sager C-465/00, C-138/01 og C-139/01, *Rechnungshof mod Österreichischer Rundfunk m.fl.* og *Christa Neukomm og Jospeh Lauermann mod Österreichischer Rundfunk*, 20. maj 2003

[Proportionaliteten af retslige forpligtelser om at offentliggøre oplysninger om indkomstforholdene for ansatte i visse kategorier af institutioner, som er relateret til den offentlige sektor]

C-70/10, *Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. november 2011

[Informationssamfundet; ophavsrettigheder; internet; peer-to-peer-software; internetudbyder; etablering af et system til filtrering af elektronisk kommunikation med henblik på at hindre udveksling af filer, der udgør en krænkelse af ophavsretten; manglende generel forpligtelse til at overvåge udvekslingen af oplysninger]

C-201/14, *Smaranda Bara m.fl. mod Casa Națională de Asigurări de Sănătate m.fl.*, 1. oktober 2015

[Retten til at blive underrettet om behandling af personoplysninger]

Forenede sager C-203/15 og C-698/15, *Tele2 Sverige AB mod Post- och telestyrelsen og Secretary of State for the Home Department mod Tom Watson m.fl.* [GC], 21. december 2016

[Fortrolighed i forbindelse med elektronisk kommunikation; udbydere af elektroniske kommunikationstjenester; pligt vedrørende generel og udifferentieret lagring af trafikdata og lokaliseringsdata; ingen forudgående kontrol foretaget af en domstol eller af en uafhængig administrativ myndighed; Den Europæiske Unions charter om grundlæggende rettigheder; forenelighed med EU-retten]

C-73/07, *Tietosuojavaltuutettu mod Satakunnan Markkinapörssi Oy og Satamedia Oy* [GC], 16. december 2008

[Begrebet »i journalistisk øjemed« i henhold til artikel 9 i databeskyttelsesdirektivet]

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde mod Rīgas pašvaldības SIA »Rīgas satiksme«*, 4. maj 2017

[Princippet om lovlig behandling: legitim interesse forfulgt af tredjemand]

Forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen* [GC], 9. november 2010

[Begrebet »personoplysninger«; proportionaliteten af den retlige forpligtelse om at offentliggøre personoplysninger om modtagerne af støtte fra visse europæiske landbrugsfonde]

C-230/14, *Weltimmo s.r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. oktober 2015

[De nationale tilsynsmyndigheders beføjelser]

C-342/12, *Worten – Equipamentos para o Lar SA mod Autoridade para as Condições de Trabalho (ACT)*, 30. maj 2013

[Begrebet »personoplysninger«, arbejdstidsregister, principper vedrørende oplysningernes pålidelighed og vedrørende grundlaget for behandling af personoplysninger, adgang for den nationale myndighed med ansvar for tilsyn med arbejdsvilkårene; arbejdsgiverens forpligtelse til at stille arbejdstidsregisteret til rådighed på en måde, der muliggør umiddelbar aflæsning]

Forenede sager C-141/12 og C-372/12, *YS mod Minister voor Immigratie, Integratie en Asiel* og *Minister voor Immigratie, Integratie en Asiel mod M og S*, 17. juli 2014

[Omfanget af den registreredes ret til indsigt; beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger; begrebet »personoplysninger«; oplysninger vedrørende en ansøger om opholdstilladelse og en juridisk analyse indeholdt i et administrativt dokument til forberedelse af afgørelsen; Den Europæiske Unions charter om grundlæggende rettigheder]

Retspraksis vedrørende direktiv (EU) 2016/681

Domstolens udtalelse 1/15 (Store Afdeling), 26. juli 2017

[Retsgrundlag; udkast til aftale mellem Canada og Den Europæiske Union om overførsel og behandling af passagerlisteoplysninger; aftaleudkastets forenelighed med artikel 16 i TEUF og artikel 7 og 8 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder]

Retspraksis vedrørende forordningen om databeskyttelse inden for EU-institutionerne

C-615/13 P, *ClientEarth og Pesticide Action Network Europe (PAN Europe) mod Den Europæiske Fødevaresikkerhedsautoritet (EFSA) og Europa-Kommissionen*, 16. juli 2015

[Aktindsigt]

C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd.* [GC], 29. juni 2010

[Aktindsigt]

Retspraksis vedrørende direktiv 2002/58/EF

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB og Storyside AB mod Perfect Communication Sweden AB*, 19. april 2012

[Ophavsret og beslægtede rettigheder; behandling af oplysninger via internettet; krænkelse af en enerettighed; lydbøger stillet til rådighed ved hjælp af en FTP-server via internettet gennem en af en internetudbyder leveret IP-adresse; påbud til en internetudbyder om at give oplysninger om navn og adresse på brugeren af IP-adressen]

C-70/10, *Scarlet Extended SA mod Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. november 2011

[Informationssamfundet; ophavsrettigheder; internet; peer-to-peer-software; internetudbyder; etablering af et system til filtrering af elektronisk kommunikation med henblik på at hindre udveksling af filer, der udgør en krænkelse af ophavsretten; manglende generel forpligtelse til at overvåge udvekslingen af oplysninger]

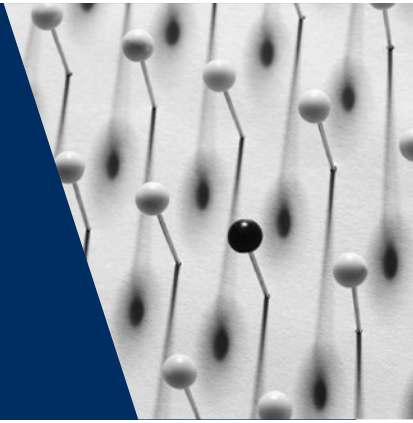
C-536/15, *Tele2 (Netherlands) BV m.fl. mod Autoriteit Consument en Markt (ACM)*, 15. marts 2017

[Princippet om forbud mod forskelsbehandling; tilrådighedsstillelse af personoplysninger om abonnenterne med henblik på levering af offentligt tilgængelige nummeroplysningstjenester og abonnentfortegnelser; abonnentens samtykke; sondring efter den medlemsstat, i hvilken den offentligt tilgængelige nummeroplysningstjeneste eller abonnentfortegnelse leveres]

Forenede sager C-203/15 og C-698/15, *Tele2 Sverige AB mod Post- och telestyrelsen* og *Secretary of State for the Home Department mod Tom Watson m.fl.* [GC], 21. december 2016

[Fortrolighed i forbindelse med elektronisk kommunikation; udbydere af elektroniske kommunikationstjenester; pligt vedrørende generel og udifferentieret lagring af

trafikdata og lokaliseringsdata; ingen forudgående kontrol foretaget af en domstol eller af en uafhængig administrativ myndighed; Den Europæiske Unions charter om grundlæggende rettigheder; forenelighed med EU-retten]



Liste over sager

Den Europæiske Unions Domstols retspraksis

Den Europæiske Menneskerettighedsdomstols retspraksis

Nationale domstoles retspraksis

En stor mængde yderligere oplysninger om Den Europæiske Unions Agentur for Grundlæggende Rettigheder er tilgængelige på internettet. De kan findes på FRA's hjemmeside, fra.europa.eu.

Yderligere oplysninger om Den Europæiske Menneskerettighedsdomstols retspraksis findes på Domstolens hjemmeside: echr.coe.int. HUDOC-søgeportalen giver adgang til domme og afgørelser på engelsk og/eller fransk, oversættelser til andre sprog, månedlige oplysningsblade om retspraksis, pressemeddelelser samt øvrige oplysninger om Domstolens arbejde.

Sådan får man fat i Europarådets publikationer

»Council of Europe Publishing« udarbejder publikationer inden for alle organisationens arbejdsområder, herunder menneskerettigheder, jura, sundhed, etik, sociale anliggender, miljøet, uddannelse, kultur, sport, unge og arkitektonisk kulturarv. Bøger og elektroniske publikationer fra det omfattende katalog kan bestilles på internettet (http://book.coe.int/).

En virtuel læsesal giver brugerne mulighed for vederlagsfrit at læse uddrag af nyudgivne hovedværker eller hele teksten af visse officielle dokumenter.

Oplysninger om og hele teksten af Europarådets konventioner findes på webstedet for Europarådets Treaty Office: http://conventions.coe.int/

Sådan kontakter du EU

Personligt

Der findes flere hundrede Europe Direct-informationscentre i hele EU. Find dit nærmeste center på: https://europa.eu/european-union/contact_da

Pr. telefon eller e-mail

Europe Direct er en tjeneste, der besvarer spørgsmål om EU. Kontakt Europe Direct:
— på gratisnummer: 00 800 6 7 8 9 10 11 (visse operatører tager betaling for disse opkald)
— på følgende nummer: +32 22999696 eller
— pr. e-mail: https://europa.eu/european-union/contact_da

Sådan finder du oplysninger om EU

Online

Oplysninger om EU er tilgængelige på alle EU's officielle sprog på Europawebstedet: https://europa.eu/european-union/index_da

EU-publikationer

Du kan downloade eller bestille EU-publikationer gratis eller mod betaling på: https://op.europa.eu/da/publications. Du kan bestille flere eksemplarer af de gratis publikationer ved at kontakte Europe Direct eller dit lokale informationscenter (se https://europa.eu/european-union/contact_da).

EU-ret og relaterede dokumenter

Du kan nemt få adgang til EU's juridiske oplysninger (herunder al EU-ret siden 1951) på alle officielle EU-sprog på EUR-Lex: http://eur-lex.europa.eu

Åbne data fra EU

EU's portal for åbne data (http://data.europa.eu/euodp/da) giver adgang til datasæt fra EU. Dataene kan downloades og genanvendes gratis til både kommercielle og ikkekommercielle formål.

doi:10.2811/834732 TK-05-17-225-DA-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Den hurtige udvikling inden for informations- og kommunikationsteknologi fremhæver det øgede behov for solid beskyttelse af personoplysninger – en ret, der er sikret ved både EU's og Europarådets instrumenter. Beskyttelse af denne vigtige rettighed indebærer nye og væsentlige udfordringer, da teknologiske fremskridt udvider mulighederne for f.eks. overvågning, opfangelse af kommunikation og lagring af data. Denne håndbog har til formål at give jurister, som ikke er specialister inden for databeskyttelse, kendskab til dette nye juridiske område. Den giver en oversigt over EU's og Europarådets gældende retlige rammer. Den forklarer vigtig retspraksis og opsummerer vigtige afgørelser truffet af både EU-Domstolen og Den Europæiske Menneskerettighedsdomstol. Derudover fremfører den hypotetiske scenarier, der fungerer som praktiske illustrationer af de forskellige problemer, som opstår inden for dette område, der er under konstant udvikling.

FRA — DEN EUROPÆISKE UNIONS AGENTUR FOR GRUNDLÆGGENDE RETTIGHEDER
Schwarzenbergplatz 11 — 1040 Wien — Østrig
Tlf. +43 (1) 580 30-0 — Fax +43 (1) 580 30-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

DEN EUROPÆISKE MENNESKERETTIGHEDSDOMSTOL EUROPARÅDET
67075 Strasbourg Cedex — Frankrig
Tlf. +33 (0) 3 88 41 20 18 — Fax +33 (0) 3 88 41 27 30
echr.coe.int — publishing@echr.coe.int — twitter.com/ECHR_CEDH

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE
Rue Wiertz 60 — 1047 Bruxelles — Belgien
Tlf. +32 2 283 19 00
edps.europa.eu — edps@edps.europa.eu — twitter.com/EU_EDPS

Den Europæiske Unions Publikationskontor

ISBN 978-92-871-9810-5 (Europarådet)
ISBN 978-92-9461-344-8 (FRA)