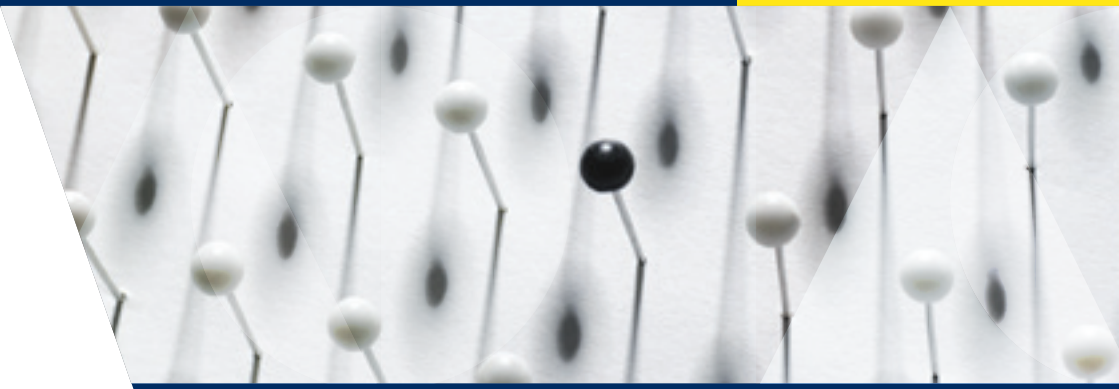
HÅNDBOG



Håndbog om europæisk databeskyttelseslovgivning

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

Manuskriptet til denne håndbog blev færdiggjort i april 2014.
Senere opdateringer offentliggøres på webstedet for Den Europæiske Unions Agentur for Grundlæggende Rettigheder (fra.europa.eu), på Europarådets websted http://coe.int/dataprotection, på webstedet for Den Europæiske Menneskerettighedsdomstol under menuen »Case-Law« på: http://echr.coe.int.

Europe Direct er en service, der har til formål at hjælpe med at besvare Deres spørgsmål om Den Europæiske Union.

Frikaldsnummer (*):

00 800 6 7 8 9 10 11

(*) Oplysningerne er gratis ligesom de fleste opkald (nogle operatører, telefonbokse eller hoteller kan dog kræve penge for opkaldet).

Foto (titelblad og inde): © iStockphoto

Yderligere oplysninger om EU fås på internet via Europaserveren (http://europa.eu)

Luxembourg: Den Europæiske Unions Publikationskontor, 2015

ISBN 978-92-871-9949-2 (Europarådet)
ISBN 978-92-9239-495-0 (FRA)
doi:10.2811/73615

Printed in Belgium

Trykt på klorfrit genbrugspapir (PCF)

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

Håndbog om europæisk databeskyttelseslovgivning

Forord

Denne håndbog om europæisk databeskyttelseslovgivning er udarbejdet i fællesskab af Den Europæiske Unions Agentur for Grundlæggende Rettigheder (FRA) og Europarådet sammen med Den Europæiske Menneskerettighedsdomstols Justitskontor. Det er den tredje i en serie af juridiske håndbøger, der er udarbejdet i fællesskab af FRA og Europarådet. I marts 2011 blev den første håndbog offentliggjort, og den omhandlede europæisk ligestillingslovgivning, og i juni 2013 blev den anden håndbog om europæisk lovgivning vedrørende asyl, grænser og immigration offentliggjort.

Vi har besluttet at fortsætte samarbejdet om et særdeles aktuelt emne, som påvirker os alle i vores hverdag, nemlig beskyttelsen af personoplysninger. Europa har et af verdens mest omfattende systemer, som er baseret på Europarådets konvention 108, EU-instrumenter samt Den Europæiske Menneskerettighedsdomstols (ECtHR) og EU-Domstolens retspraksis.

Formålet med denne håndbog er at øge bevidstheden om og kendskabet til databeskyttelsesreglerne i EU's og Europarådets medlemsstater. Det er hensigten, at den skal fungere som et referencegrundlag for læserne. Den henvender sig til retlige aktører uden ekspertviden, dommere, nationale databeskyttelsesmyndigheder og andre personer, der beskæftiger sig med databeskyttelse.

Med Lissabontraktatens ikrafttrædelse i december 2009 blev EU's charter om grundlæggende rettigheder juridisk bindende, og dermed fik retten til beskyttelse af personoplysninger status som en separat grundlæggende rettighed. En bedre forståelse af Europarådets konvention 108 og EU's instrumenter, som banede vejen for databeskyttelse i Europa, samt EU-Domstolens og ECtHR retspraksis er afgørende for beskyttelsen af denne grundlæggende rettighed.

Vi vil gerne takke Ludwig Boltzmann Institute of Human Rights for dets bidrag i forbindelsen med udarbejdningen af udkastet til denne håndbog. Vi vil også gerne udtrykke vores taknemmelighed til den Europæisk tilsynsførende for databeskyttelse for dets kommentarer i udkastsfasen. Vi vil særligt gerne takke Europa-Kommissionens databeskyttelseenhed for forberedelserne til denne håndbog. Endelig vil vi gerne takke Datatilsynet i Danmark, som har gennemlæst og kommenteret nærværende oversættelse.

Philippe Boillat

Generaldirektør
Human Rights and Rule of Law
Europarådet

Morten Kjaerum

Direktør
Den Europæiske Unions Agentur
for Grundlæggende Rettigheder

Indholdsfortegnelse

Forkortelser og akronymer

BCR	Binding corporate rule (bindende virksomhedsregel)
CCTV	Closed circuit television (kameraovervågning)
CETS	Council of Europe Treaty Series (Europarådets traktatserie)
Charter	Den Europæiske Unions charter om grundlæggende rettigheder
CIS	Customs information system (toldinformationssystem)
CoE	Europarådet
CRM	Customer relations management (forvaltning af kunderelationer)
C-SIS	Det centrale Schengeninformationssystem
EAW	European Arrest Warrant (europæisk arrestordre)
ECtHR	Den Europæiske Menneskerettighedsdomstol
EDPS	Den Europæiske Tilsynsførende for Databeskyttelse
EF	Det Europæiske Fællesskab
EFTA	Den Europæiske Frihandelssammenslutning
EMK	Den europæiske menneskerettighedskonvention
ENISA	Det Europæiske Agentur for Net- og Informationssikkerhed
ENU	National Europolenhed
ESMA	Den Europæiske Værdipapir- og Markedstilsynsmyndighed
eTEN	Transeuropæiske telenet
EU	Den Europæiske Union
EU-Domstolen	Den Europæiske Unions Domstol (før december 2009: De Europæiske Fællesskabers Domstol, EF-Domstolen)
eu-LISA	Det Europæiske Agentur for den Operationelle Forvaltning af Store It-systemer
EuroPriSe	European Privacy Seal (europæisk datasikkerhedsmærkning)
EØS	Det Europæiske Økonomiske Samarbejdsområde
FN	De Forenede Nationer

FRA	Den Europæiske Unions Agentur for Grundlæggende Rettigheder
GPS	Globalt positioneringssystem
JSB	Joint Supervisory Body (Den Fælles Kontrolinstans)
Konvention 108	Konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (Europarådet)
Ngo	Ikkestatslig organisation
N-SIS	Det nationale Schengeninformationssystem
OECD	Organisationen for Økonomisk Samarbejde og Udvikling
PIN	Personligt identifikationsnummer
PNR	Passagerliste
SEPA	Fælles eurobetalingsområde
SIS	Schengeninformationssystem
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEU	Traktaten om Den Europæiske Union
TEUF	Traktaten om Den Europæiske Unions funktionsmåde
UDHR	Verdenserklæringen om menneskerettigheder
VIS	Visuminformationssystem

Sådan anvendes denne håndbog

Denne håndbog giver en oversigt over lovgivningen vedrørende databeskyttelse i forhold til Den Europæiske Union (EU) og Europarådet.

Håndbogen har til formål at bistå jurister, der ikke er specialiseret i databeskyttelse. Den henvender sig til advokater, dommere eller andre jurister og til alle, der arbejder for andre organer, herunder ikke-statslige organisationer (ngo'er), som står over for juridiske spørgsmål vedrørende databeskyttelse.

Den omhandler først og fremmest EU-lovgivningens og den europæiske menneskerettighedskonventions bestemmelser om databeskyttelse, og den forklarer, hvordan dette område er reguleret i EU-retten, den europæiske menneskerettighedskonvention (EMK) og Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108) og andre instrumenter fra Europarådet. I hvert kapitel vises der først en tabel med de gældende bestemmelser, herunder eksempler på vigtig retspraksis under de to separate europæiske retsordener. Derefter præsenteres de relevante love i disse to europæiske systemer separat i det omfang, de er relevante for hvert emne. Derved kan læseren se, hvor de to retsordener konvergerer, og hvor de er forskellige.

Tabellerne i begyndelsen af hvert kapital viser de emner, der er omhandlet i det pågældende kapitel, og angiver de gældende retlige bestemmelser og andet relevant materiale, som f.eks. retspraksis. Emnernes rækkefølge kan adskille sig fra rækkefølgen i selve teksten i kapitlet, hvis det giver en mere præcis præsentation af kapitlets indhold. Tabellerne dækker både Europarådets konventioner og EU-retten. Dette vil hjælpe brugerne med at finde de oplysninger, der er relevante for deres situation, især hvis de kun er omfattet af Europarådets retsorden.

Jurister i tredjelande, som er medlemmer af Europarådet og er part i den europæiske menneskerettighedskonvention (EMK) og konvention 108, kan se de oplysninger, der er relevante for deres eget land, ved at gå direkte til afsnittene vedrørende Europarådet. Jurister i EU's medlemsstater skal anvende begge afsnit, da disse lande er bundet af begge retsordener. Hvis der er brug for yderligere oplysninger, er der anført en liste over referencer til mere specialiseret materiale i afsnittet "Yderligere materiale" i håndbogen.

Europarådets retsorden præsenteres ved korte henvisninger til udvalgte sager ved Den Europæiske Menneskerettighedsdomstol (Menneskerettighedsdomstolen). De

er udvalgt mellem Menneskerettighedsdomstolens mange domme og afgørelser vedrørende databeskyttelse.

EU-retten findes i vedtagne retsakter, traktaternes relevante bestemmelser og Den Europæiske Unions charter om grundlæggende rettigheder som fortolket ved Den Europæiske Unions Domstols retspraksis (EU-Domstolen; før 2009: EF-Domstolen).

Den retspraksis, der beskrives eller citeres i denne håndbog, er eksempler på vigtig retspraksis ved både Menneskerettighedsdomstolen og EU-Domstolen. Retningslinjerne sidst i håndbogen kan hjælpe læseren med at søge efter retspraksis på internettet.

De praktiske illustrationer med hypotetiske scenarier er anført i tekstbokse for yderligere at illustrere den praktiske anvendelse af de europæiske databeskyttelsesregler, især i de tilfælde, hvor der ikke findes specifik retspraksis ved Menneskerettighedsdomstolen eller EU-Domstolen.

Håndbogen indledes med en kort beskrivelse af de to retsordeners rolle som fastlagt ved den europæiske menneskerettighedskonvention (EMK) og EU-retten (kapitel 1). Kapitel 2 til 8 omhandler følgende emner:

- databeskyttelsesterminologi
- de centrale principper i den europæiske lovgivning om databeskyttelse
- reglerne i den europæiske lovgivning om databeskyttelse
- de registreredes rettigheder og håndhævelsen heraf
- grænseoverskridende dataudveksling
- databeskyttelse i forbindelse med politi og retsvæsen
- andre specifikke europæiske databeskyttelsesregler.

1

Kontekst og baggrund for den europæiske lovgivning om databeskyttelse

EU	Omhandlede emner	Europarådet
Retten til databeskyttelse		
Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (*databeskyttelsesdirektivet*), EFT 1995 L 281		EMK, artikel 8 (retten til respekt for privatliv og familieliv, hjem og kommunikation) Konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108)
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*, 2010	**Generelt**	
EU-Domstolen, C-73/07, *Tietosuojavaltuutettu mod Satakunnan Markkinapörssi Oy og Satamedia Oy*, 2008	**Ytringsfrihed**	Menneskerettighedsdomstolen, *Axel Springer AG mod Tyskland*, 2012 Menneskerettighedsdomstolen, *Mosley mod Det Forenede Kongerige*, 2011
	Frihed for kunst og videnskab	Menneskerettighedsdomstolen, *Vereinigung bildender Künstler mod Østrig*, 2007
EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU*, 2008	**Beskyttelse af ejendomsret**	
EU-Domstolen, C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd*, 2010	**Aktindsigt**	Menneskerettighedsdomstolen, *Társaság a Szabadságjogokért mod Ungarn*, 2009

1.1. Retten til databeskyttelse

Hovedpunkter

- Ifølge artikel 8 i EMK er retten til beskyttelse mod indsamling og registrering af personoplysninger en del af retten til respekt for privatliv og familieliv, hjem og kommunikation.
- Europarådets konvention 108 er det første internationalt retligt bindende instrument, som udtrykkeligt omhandler databeskyttelse.
- I EU-retten blev databeskyttelse første gang reguleret ved databeskyttelsesdirektivet.
- I EU-retten anerkendes databeskyttelse som en grundlæggende rettighed.

En ret til beskyttelse af en persons privatsfære mod indtrængen fra andre, især fra staten, blev første gang fastlagt i et internationalt retligt instrument ved artikel 12 i FN's menneskerettighedserklæring fra 1948 om respekt for privatliv og familieliv[1]. Menneskerettighedserklæringen påvirkede udviklingen af andre menneskerettighedsinstrumenter i Europa.

1.1.1. 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 den europæiske menneskerettighedskonvention (EMK), som trådte i kraft i 1953.

Landene har en international forpligtelse til at overholde den europæiske menneskerettighedskonvention. Alle Europarådets medlemsstater har nu indarbejdet eller gennemført den europæiske menneskerettighedskonvention i deres nationale ret, og det kræver, at de handler i overensstemmelse med konventionens bestemmelser.

For at sikre, at de kontraherende parter overholder deres forpligtelser i henhold til den europæiske menneskerettighedskonvention, blev Den Europæiske

1 De Forenede Nationers verdenserklæring om menneskerettighederne (menneskerettighedserklæringen), 10. december 1948.

Menneskerettighedsdomstol (Menneskerettighedsdomstolen) etableret i Strasbourg, Frankrig, i 1959. Menneskerettighedsdomstolen sikrer, at landene overholder deres forpligtelser i henhold til konventionen, ved at behandle klager fra personer, grupper af personer, ngo'er eller juridiske personer over overtrædelser af konventionen. I 2013 havde Europarådet 47 medlemsstater, hvoraf 28 også er EU-medlemsstater. En sagsøger ved Menneskerettighedsdomstolen behøver ikke være statsborger i en af medlemsstaterne. Menneskerettighedsdomstolen kan også behandle mellemstatslige sager, der anlægges af en eller flere af Europarådets medlemsstater mod en anden medlemsstat.

Retten til beskyttelse af personoplysninger er en del af de rettigheder, der er sikret ved artikel 8 i den europæiske menneskerettighedskonvention, som garanterer retten til respekt for privatliv og familieliv, hjem og kommunikation og fastlægger de omstændigheder, hvorunder begrænsninger af denne rettighed tillades[2].

I sin retspraksis har Menneskerettighedsdomstolen undersøgt adskillige sager, der har involveret databeskyttelse, ikke mindst tilfælde vedrørende aflytning[3], forskellige former for overvågning[4] og beskyttelse mod offentlige myndigheders lagring af personoplysninger[5]. Den har præciseret, at artikel 8 i EMK ikke kun forpligter landene til at undlade at træffe foranstaltninger, 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[6]. Mange af disse sager er beskrevet i detaljer i de relevante kapitler.

1.1.2. Europarådets konvention 108

Med indførelsen af informationsteknologi i 1960'erne opstod der et stigende behov for mere detaljerede regler, der kunne beskytte enkeltpersoners (personlige) data. I midten af 1970'erne vedtog Europarådets Ministerudvalg en række resolutioner

2 Europarådet, den europæiske menneskerettighedskonvention (EMK), CETS nr. 005, 1950.

3 Se f.eks. Menneskerettighedsdomstolen, *Malone mod Det Forenede Kongerige*, nr. 8691/79, 2. august 1984, Menneskerettighedsdomstolen, *Copland mod Det Forenede Kongerige*, nr. 62617/00, 3. april 2007.

4 Se f.eks. Menneskerettighedsdomstolen, *Klass m.fl. mod Tyskland*, nr. 5029/71, 6. september 1978, Menneskerettighedsdomstolen, *Uzun mod Tyskland*, nr. 35623/05, 2. september 2010.

5 Se f.eks. Menneskerettighedsdomstolen, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987, Menneskerettighedsdomstolen, *S. og Marper mod Det Forenede Kongerige*, nr. 30562/04 og 30566/04, 4. december 2008.

6 Se f.eks. Menneskerettighedsdomstolen, *I. mod Finland*, nr. 20511/03, 17. juli 2008, Menneskerettighedsdomstolen, *K.U. mod Finland*, nr. 2872/02, 2. december 2008.

om beskyttelse af personoplysninger på grundlag af artikel 8 i EMK[7]. I 1981 blev en konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108)[8] åbnet for undertegnelse. Konvention 108 var og er stadig det eneste retligt bindende internationale instrument vedrørende databeskyttelse.

Konvention 108 finder anvendelse på enhver behandling, der udføres af både den private sektor og offentlige myndigheder, som f.eks. retsvæsnet samt politi og anklagemyndigheden. Konventionen beskytter det enkelte menneske mod misbrug i forbindelse med indsamling og behandling af personoplysninger og har samtidig til formål at regulere grænseoverskridende udveksling af personoplysninger. Hvad angår indsamling og behandling af personoplysninger, vedrører konventionens principper især rimelig og lovlig indsamling og automatisk behandling af personoplysninger, der lagres til nærmere bestemte og legitime formål, og som ikke må anvendes på en måde, der er uforenelig med disse formål, og ikke må lagres i længere tid end nødvendigt. De vedrører også kvaliteten af personoplysninger, herunder at de skal være relevante, tilstrækkelige og ikke omfatte mere, end hvad der kræves til i forhold til at opfylde de formål, de er lagret til.

Ud over at sikre indsamlingen og behandlingen af personoplysninger 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.

Selv om konventionen sikrer fri udveksling af personoplysninger mellem de stater, der er parter i konventionen, indfører den også visse begrænsninger for videregivelse af oplysninger til stater, hvis retssystem ikke yder tilsvarende beskyttelse.

7 Europarådet, Ministerudvalget (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, Ministerudvalget (1974), resolution (74)29 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger i den offentlige sektor, 20. september 1974.

8 Europarådet, konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, CETS nr. 108, 1981.

For yderligere at udvikle de generelle principper og regler, der er fastlagt ved konvention 108, har Europarådets Ministerudvalg vedtaget en række henstillinger, som ikke er retligt bindende (se kapitel 7 og 8).

Alle EU's medlemsstater har ratificeret konvention 108. I 1999 blev konvention 108 ændret, så EU blev part[9]. I 2001 blev der vedtaget en tillægsprotokol til konvention 108, som indførte bestemmelser om grænseoverskridende videregivelse af personoplysninger til lande, der ikke er kontraherende part i konventionen, nemlig såkaldte tredjelande, og om obligatorisk oprettelse af nationale databeskyttelsesmyndigheder.[10]

Fremtidsudsigter

Efter en beslutning om at ajourføre konvention 108 blev der gennemført en offentlig høring i 2011, som gjorde det muligt at bekræfte dette arbejdes to hovedmål, nemlig at styrke beskyttelsen af privatlivets fred på det digitale område og styrke konventionens opfølgningsmekanisme.

Konvention 108 kan tiltrædes af lande, som ikke er medlem af Europarådet, herunder ikke-europæiske lande. Konventionens potentiale som en universel standard og dens åbne karakter kan være et grundlag for at fremme databeskyttelse på globalt plan.

Indtil videre er 45 af de 46 kontraherende parter i konvention 108 Europarådets medlemsstater. Uruguay, der er det første ikke-europæiske land, tiltrådte i august 2013, og Marokko, som Ministerudvalget har opfordret til at tiltræde konvention 108, er ved at formalisere tiltrædelsen.

1.1.3. EU's databeskyttelseslovgivning

EU-retten består af traktater og afledt EU-ret. Traktaterne, navnlig traktaten om Den Europæiske Union (TEU) og traktaten om Den Europæiske Unions funktionsmåde (TEUF), er blevet godkendt af alle EU's medlemsstater og kaldes også "EU's primære

9 Europarådet, ændring af konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (ETS nr. 108), som De Europæiske Fællesskaber kan tiltræde, vedtaget af Ministerudvalget i Strasbourg, 15. juni 1999, artikel 23, stk. 2, i konvention 108 som ændret.

10 Europarådet, 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. 181, 2001.

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".

EU's primære retlige instrument vedrørende databeskyttelse er 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*)[11] Det blev vedtaget i 1995 – et tidspunkt, hvor flere medlemsstater allerede havde vedtaget nationale databeskyttelseslove. Den frie bevægelighed for varer, personer, tjenesteydelser og kapital 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.

Da databeskyttelsesdirektivet blev vedtaget for at harmonisere[12] databeskyttelseslovgivningen på nationalt plan, er direktivet lige så specifikt som de (dengang) eksisterende nationale databeskyttelseslove. Domstolen har sagt, at "at direktiv 95/46 [...] har til formål at gøre beskyttelsen af det enkelte menneskes rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger ensartet i alle medlemsstater. [...] [A]t tilnærmelsen af de nationale lovgivninger, der finder anvendelse på området, ikke må medføre en forringelse af den beskyttelse, disse yder, men at den tværtimod skal have til formål at sikre et højt beskyttelsesniveau inden for Unionen. [H]armoniseringen af de nævnte nationale lovgivninger [er] ikke begrænset til en minimumsharmonisering, men fører til en harmonisering, der i princippet er fuldstændig.[13] Medlemsstaterne har derfor kun begrænset manøvrefrihed, når de gennemfører direktivet.

Databeskyttelsesdirektivet har til formål at gennemføre de principper bag retten til privatlivets fred, der allerede er indeholdt i konvention 108, og at udvide dem. Alle 15 EU-medlemsstater i 1995 var også kontraherende parter i konvention 108, og det udelukker modstridende regler i de to retlige instrumenter. Databeskyttelsesdirektivet udnytter dog den mulighed for at indføre yderligere instrumenter vedrørende beskyttelse, der er fastlagt ved artikel 11 i konvention 108. Indførelsen af uafhængigt tilsyn som et instrument til at forbedre overensstemmelsen med

11 Databeskyttelsesdirektivet, EFT 1995 L 281, s. 31.

12 Se f.eks. databeskyttelsesdirektivet, betragtning 1, 4, 7 og 8.

13 Domstolens forenede sager C-468/10 og C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) mod Administración del Estado,* 24. november 2011, præmis 28-29.

databeskyttelsesreglerne viste sig f.eks. at være et vigtigt bidrag til den effektive gennemførelse af den europæiske databeskyttelseslovgivning. (Dette instrument blev derfor overført til Europarådets retsorden i 2001 ved tillægsprotokollen til konvention 108.)

Det territoriale anvendelsesområde for databeskyttelsesdirektivet går ud over de 28 EU-medlemsstater og omfatter også de tredjelande, der er medlem af Det Europæiske Økonomiske Samarbejdsområde (EØS)[14], dvs. Island, Liechtenstein og Norge.

EU-Domstolen i Luxembourg har kompetence til at afgøre, om en medlemsstat har opfyldt sine forpligtelser i henhold til databeskyttelsesdirektivet, og træffe præjudicielle afgørelser vedrørende gyldigheden og fortolkningen af direktivet med det formål at sikre, at det gennemføres effektivt og ensartet i medlemsstaterne. En vigtig undtagelse fra databeskyttelsesdirektivets anvendelsesområde er den familiemæssige undtagelse, dvs. behandling, som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter[15]. En sådan behandling betragtes generelt som en del af private personers frihedsrettigheder.

Ligesom den primære EU-ret, der var gældende, da databeskyttelsesdirektivet blev vedtaget, er direktivets materielle anvendelsesområde begrænset til forhold vedrørende det indre marked. Uden for dets anvendelsesområde er først og fremmest spørgsmål vedrørende politisamarbejde og strafferetligt samarbejde. Databeskyttelse i forbindelse med disse spørgsmål er omhandlet i forskellige retlige instrumenter, som er udførligt beskrevet i kapitel 7.

Eftersom databeskyttelsesdirektivet kun kunne omhandle EU-medlemsstater, var der behov for et yderligere retligt instrument for at sikre databeskyttelse i forbindelse med behandling af personoplysninger, der foretages af EU's institutioner og organer. 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 (*forordningen om databeskyttelse inden for EU-institutionerne*) opfylder dette formål[16].

14 Aftale om Det Europæiske Økonomiske Samarbejdsområde, EFT 1994 L 1, som trådte i kraft den 1. januar 1994.

15 Databeskyttelsesdirektivet, artikel 3, stk. 2, andet led.

16 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 2001 L 8.

Desuden er der, selv på de områder, der er omfattet af databeskyttelsesdirektivet, ofte behov for mere detaljerede bestemmelser om databeskyttelse for at opnå den nødvendige klarhed i forhold til andre legitime interesser. To eksempler er direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (*direktivet om databeskyttelse inden for elektronisk kommunikation*)[17] og direktiv 2006/24/EF 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 (*datalagringsdirektivet* ophævet den 8. april 2014)[18]. Andre eksempler er omhandlet i kapitel 8. Sådanne bestemmelser skal være i overensstemmelse med databeskyttelsesdirektivet.

Den Europæiske Unions charter om grundlæggende rettigheder

De Europæiske Fællesskabers oprindelige traktater omhandlede ikke menneskerettighederne eller deres beskyttelse. Efterhånden som sager med påstande om krænkelser af menneskerettighederne blev indbragt for den daværende EF-Domstol inden for rammerne af EU-retten, blev der udviklet en ny tilgang. For at beskytte personer blev grundlæggende rettigheder gjort til en del af europæisk rets almindelige principper. I henhold til EU-Domstolen afspejler disse almindelige principper indholdet af de bestemmelser om menneskerettigheder, der findes i nationale forfatninger og menneskerettighedstraktater, herunder den europæiske menneskerettighedskonvention. EU-Domstolen fastslog, 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.

17 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 2002 L 201.

18 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 (*datalagringsdirektivet*), EUT 2006 L 105, ophævet den 8. april 2014.

Chartret var oprindeligt kun et politisk dokument, men det blev retligt bindende[19] som primær EU-ret (se artikel 6, stk. 1, i TEU) med Lissabontraktatens ikrafttræden den 1. december 2009[20].

Den primære EU-ret giver også EU generel kompetence til at fastsætte regler om databeskyttelse (artikel 16 i TEUF).

Chartret sikrer ikke kun respekt for privatliv og familieliv (artikel 7), men fastlægger også retten til beskyttelse af personoplysninger (artikel 8) og ophøjer derved udtrykkeligt denne beskyttelse til samme niveau som en grundlæggende rettighed i EU-retten. Både EU-institutioner og medlemsstater 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 sikrer chartrets artikel 8, stk. 3, at gennemførelsen af disse principper er underlagt en uafhængig myndigheds kontrol.

Fremtidsudsigter

I januar 2012 fremsatte Europa-Kommissionen forslag til en databeskyttelsesreformpakke, idet den bekendtgjorde, at der var behov for at modernisere de nuværende databeskyttelsesregler som følge af den hastige teknologiske udvikling og globaliseringen. Reformpakken består af et forslag til en generel forordning om databeskyttelse[21], der skal erstatte databeskyttelsesdirektivet, og det nye databeskyttelsesdirektiv[22], som skal omhandle databeskyttelse i forbindelse med

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

20 Se konsoliderede udgaver af De Europæiske Fællesskaber (2012), traktaten om Den Europæiske Union, EUT 2012 C 326, og De Europæiske Fællesskaber (2012), traktaten om Den Europæiske Unions funktionsmåde, EUT 2012 C 326.

21 Europa-Kommissionen (2012), *forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)*, KOM(2012) 11 endelig, Bruxelles, den 25. januar 2012.

22 Europa-Kommissionen (2012), *forslag til 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 (generelt direktiv om databeskyttelse)*, KOM(2012) 10 endelig, Bruxelles, den 25. januar 2012.

politimæssigt og retligt samarbejde i straffesager. På tidspunktet for offentliggørelsen af denne håndbog gennemførtes der drøftelser af reformpakken.

1.2. Afvejning af rettigheder

Hovedpunkt

- Retten til databeskyttelse er ikke en absolut ret. Den skal afvejes i forhold til andre rettigheder.

Den grundlæggende ret til beskyttelse af personoplysninger, jf. chartrets artikel 8, "udgør imidlertid ikke en absolut forrettighed, men skal ses i sammenhæng med sin funktion i samfundet"[23]. I henhold til chartrets artikel 52, stk. 1, kan der derfor indføres begrænsninger i udøvelsen af de rettigheder, der er fastlagt ved chartrets artikel 7 og 8, såfremt disse begrænsninger er fastlagt i lovgivningen, respekterer disse rettigheders og friheders væsentligste indhold og 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[24].

I EMK er databeskyttelse garanteret ved artikel 8 (retten til respekt for privatliv og familieliv), og som i chartret skal anvendelsesområdet for andre konkurrerende rettigheder respekteres, når denne ret gøres gældende. I artikel 8, stk. 2, i EMK anføres følgende: "Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund [...] for at beskytte andres rettigheder og friheder".

Som følge deraf har både Menneskerettighedsdomstolen og EU-Domstolen gentagne gange udtalt, at en afvejning i forhold til andre rettigheder er nødvendig, når

23 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*, 9. november 2010, præmis 48.

24 *Ibid.*, præmis 50.

artikel 8 i EMK og chartrets artikel 8 anvendes og fortolkes[25]. Flere vigtige eksempler viser, hvordan denne afvejning foretages.

1.2.1. Ytringsfrihed

En af de rettigheder, der med sandsynlighed kan komme i konflikt med retten til databeskyttelse, er retten til ytringsfrihed.

Ytringsfrihed er beskyttet ved 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". Artikel 11 svarer til artikel 10 i EMK. I det omfang chartret indeholder rettigheder svarende til dem, der er sikret ved EMK, har de i henhold til chartrets artikel 52, stk. 3, "samme betydning og omfang som i konventionen". De begrænsninger, der lovligt kan indføres for den ret, der er garanteret ved chartrets artikel 11, kan derfor ikke overstige dem, der er fastlagt ved artikel 10, stk. 2, i EMK, dvs. at de skal være foreskrevet ved lov og nødvendige i et demokratisk samfund "for at beskytte andres [...] rygte eller rettigheder". Dette koncept dækker retten til databeskyttelse.

Forholdet mellem beskyttelse af personoplysninger og ytringsfrihed er omhandlet i databeskyttelsesdirektivets artikel 9, som har titlen "Behandling af personoplysninger og ytringsfriheden"[26]. I denne artikel anføres, at 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.

25 Menneskerettighedsdomstolen, *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*, 29. januar 2008, præmis 68. Se også Europarådet (2013), Den Europæiske Menneskerettighedsdomstols retspraksis vedrørende beskyttelse af personoplysninger, DP (2013), som findes på: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

26 Databeskyttelsesdirektivet, artikel 9.

Eksempel: I sagen *Tietosuojavaltuutettu mod Satakunnan Markkinapörssi Oy and Satamedia Oy*[27] blev EU-Domstolen anmodet om at fortolke databeskyttelsesdirektivets artikel 9 og definere forholdet mellem databeskyttelse og pressefrihed. Domstolen skulle undersøge Markkinapörssi og Satamedias offentliggørelse af skatteoplysninger om omkring 1,2 millioner fysiske personer, som lovligt var indhentet fra de finske myndigheder. Domstolen skulle navnlig afgøre, om behandling af personoplysninger, som skattemyndighederne havde offentliggjort, og som foretages for at give mobiltelefonbrugere mulighed for at modtage skatteoplysninger om andre fysiske personer, skal anses for aktiviteter, som udelukkende finder sted i journalistisk øjemed. Efter at have afgjort, at Satakunnans aktiviteter var "behandling af personoplysninger" som defineret i databeskyttelsesdirektivets artikel 3, stk. 1, fortolkede Domstolen direktivets artikel 9. Domstolen bemærkede først den betydning, ytringsfriheden har i ethvert demokratisk samfund, og fastslog, at de begreber, som er knyttet hertil, herunder begrebet i journalistisk øjemed, skal fortolkes vidt. Den konstaterede derefter, at undtagelser fra og begrænsninger af beskyttelsen af oplysninger skal holdes inden for det strengt nødvendige for at opnå en afbalanceret afvejning af de to grundlæggende rettigheder. I den pågældende sag fandt Domstolen, at aktiviteter som dem, Markkinapörssi og Satamedia 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 altså, 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.

Med hensyn til foreningen af retten til databeskyttelse med retten til ytringsfrihed har Menneskerettighedsdomstolen afsagt en række skelsættende domme.

Eksempel: I sagen *Axel Springer AG mod Tyskland*[28] fastslog Menneskerettighedsdomstolen, at et forbud, som en national domstol havde pålagt ejeren af en avis, der ønskede at offentliggøre en artikel om anholdelsen og domfældelsen af en kendt skuespiller, var i strid med artikel 10 i EMK. Menneskerettig-

27 EU-Domstolen, C-73/07, *Tietosuojavaltuutettu mod Satakunnan Markkinapörssi Oy og Satamedia Oy*, 16. december 2008, præmis 56, 61 og 62.

28 Menneskerettighedsdomstolen, *Axel Springer AG mod Tyskland* [GC], nr. 39954/08, 7. februar 2012, præmis 90 og 91.

hedsdomstolen gentog de kriterier, som den havde fastlagt i sin retspraksis for afvejning af retten til ytringsfrihed i forhold til retten til respekt for privatlivet:

- For det første med hensyn til, om den pågældende offentliggjorte artikel var af almen interesse: Anholdelsen og domfældelsen af en person var en del af en offentlig retshandling og dermed af samfundsmæssig interesse.

- For det andet med hensyn til, om den berørte person var en offentlig figur: Den berørte person var en skuespiller, der var tilstrækkeligt kendt til at blive betegnet som en offentlig figur.

- For det tredje med hensyn til, hvordan oplysningerne var blevet fremskaffet, og om de var pålidelige: Oplysningerne var blevet udleveret af den offentlige anklager, og rigtigheden af oplysningerne i begge offentliggørelser blev ikke anfægtet af parterne.

Menneskerettighedsdomstolen fastslog derfor, at de begrænsninger med hensyn til offentliggørelse, der var blevet pålagt selskabet, ikke havde været rimelige i forhold til det legitime mål om at beskytte sagsøgerens privatliv. Domstolen konkluderede derfor, at den europæiske menneskerettighedskonventions artikel 10 var blevet overtrådt.

Eksempel: I sagen *Von Hannover mod Tyskland (nr. 2)*[29] fandt Menneskerettighedsdomstolen, at der ikke havde været tale om en krænkelse af retten til respekt for privatlivet i henhold til artikel 8 i EMK, da prinsesse Caroline af Monaco blev nægtet et forbud mod offentliggørelsen af et foto af hende og hendes mand, der var blevet taget under en skiferie. Fotoet var ledsaget af en artikel, der bl.a. omhandlede prins Rainiers dårlige helbred. Menneskerettighedsdomstolen konkluderede, at de nationale domstole nøje havde afvejet de offentliggørende virksomheders ret til ytringsfrihed i forhold til sagsøgernes ret til respekt for deres privatliv. De nationale domstoles betegnelse af prins Rainiers sygdom som en aktuel begivenhed kunne ikke betragtes som urimelig, og Menneskerettighedsdomstolen accepterede, at fotoet set i forbindelse med artiklen i en vis grad bidrog til en debat af almen interesse. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 ikke var blevet overtrådt.

29 Menneskerettighedsdomstolen, *Von Hannover mod Tyskland (nr. 2)* [GC], nr. 40660/08 og 60641/08, 7. februar 2012, præmis 118 og 124.

I Menneskerettighedsdomstolens retspraksis er et af de afgørende kriterier i forbindelse med afvejningen af disse rettigheder, hvorvidt den anfægtede ytring bidrager til en debat af samfundsmæssig interesse.

Eksempel: I sagen *Mosley mod Det Forenede Kongerige*[30] offentliggjorde en national ugeavis intime fotos af sagsøgeren. Han påberåbte sig derefter en krænkelse af artikel 8 i EMK, fordi 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, der kunne krænke en persons ret til privatliv. Selv om sådant materiale generelt blev offentliggjort med henblik på underholdning snarere end undervisning, var offentliggørelsen uden tvivl omfattet af artikel 10 i EMK, som dog viger for kravene i artikel 8 i EMK, 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 afkølende virkning, som et anmeldelseskrav kunne have, tvivlen om dets effektivitet og de brede muligheder for skøn på området konkluderede Menneskerettighedsdomstolen, at et retligt bindende anmeldelseskrav ikke var påkrævet i henhold til artikel 8. Domstolen konkluderede derfor, at den europæiske menneskerettighedskonventions artikel 8 ikke var blevet overtrådt.

Eksempel: I sagen *Biriuk mod Litauen*[31] krævede sagsøgeren erstatning fra et dagblad, fordi det havde offentliggjort en artikel om, at hun var hiv-positiv. Oplysningerne var angiveligt blevet bekræftet af læger på det lokale hospital. Menneskerettighedsdomstolen vurderede, at den pågældende artikel ikke bidrog til en debat af almen interesse, og gentog, at beskyttelse af personoplysninger, herunder navnlig helbredsoplysninger, er af afgørende betydning for, at en person kan udøve sin ret til respekt for privatliv og familieliv som sikret ved artikel 8 i EMK. Domstolen lagde især vægt på, at hospitalspersonale i henhold til avisartiklen i klar strid med dets tavshedspligt havde givet oplysninger om sagsøgerens hiv-infektion. Som følge deraf havde staten ikke beskyttet sagsøgerens ret til respekt for sit privatliv. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

30 Menneskerettighedsdomstolen, *Mosley mod Det Forenede Kongerige*, nr. 48009/08, 10. maj 2011, præmis 129 og 130.

31 Menneskerettighedsdomstolen, *Biriuk mod Litauen*, nr. 23373/03, 25. november 2008.

1.2.2. Aktindsigt

Informationsfrihed i henhold til chartrets artikel 11 og artikel 10 i EMK beskytter retten til ikke kun at udbrede, men også at *modtage* information. Betydningen af gennemsigtig forvaltning for et demokratisk samfunds funktionsmåde anerkendes i stigende grad. I de sidste to årtier er retten til aktindsigt i de dokumenter, som myndighederne er i besiddelse af, blevet anerkendt som en vigtig ret for enhver EU-borger og enhver fysisk eller juridisk person med bopæl eller hjemsted 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*)[32]. **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*)[33]. 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". Ifølge chartrets artikel 52, stk. 2, udøves retten til aktindsigt også på de betingelser og med de begrænsninger, der er nævnt i artikel 15, stk. 3, i TEUF. Denne ret kan komme i konflikt med retten til databeskyttelse, hvis aktindsigt i et dokument afslører andre personers personoplysninger. 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.

Eksempel: I sagen *Kommissionen mod Bavarian Lager*[34] 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 (*databeskyttelsesforordningen*). 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 bri-

32 Europarådet, Ministerudvalget (2002), henstilling 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.

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

34 EU-Domstolen, C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd.*, 29. juni 2010, præmis 60, 63, 76, 78 og 79.

tiske 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 databeskyttelsesforordningen. Da Bavarian Lager ikke kunne acceptere dette, indbragte virksomheden sagen for Retten, som annullerede Kommissionens beslutning ved dom af 8. november 2007 (sag T-194/04, *Bavarian Lager mod Kommissionen*) 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 databeskyttelsesforordningen 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 databeskyttelsesforordningen.

Ifølge denne dom skal der være en specifik og berettiget begrundelse for at gribe ind i retten til databeskyttelse, for så vidt angår aktindsigt. Retten til aktindsigt tilsidesætter ikke automatisk retten til databeskyttelse[35].

Et særligt aspekt af en begæring om aktindsigt blev behandlet i den følgende sag ved Menneskerettighedsdomstolen.

Eksempel: I sagen *Társaság a Szabadságjogokért mod Ungarn*[36] havde sagsøgeren, en menneskerettighedsorganisation, anmodet forfatningsdomstolen om aktindsigt i information vedrørende en verserende sag. Uden at høre det parlamentsmedlem, der havde anlagt den pågældende sag, afslog forfatningsdomstolen begæringen om aktindsigt med den begrundelse, at klager, der var indbragt for domstolen, kun kunne fremlægges for tredjemand med klagerens samtykke. De nationale domstole fastholdt dette afslag med den begrundelse, at beskyttelsen af sådanne personoplysninger ikke kunne tilsidesættes af andre legitime interesser, herunder aktindsigt i myndighedsinformationer. Sagsøgeren havde fungeret som en "social vagthund", hvis aktiviteter berettigede til samme beskyttelse som den beskyttelse, medierne nyder. I forhold til pressefriheden har Menneskerettighedsdomstolen konsekvent fastholdt, at offentligheden har ret til at få udleveret information af almen interesse. De informationer, sagsøgeren ønskede, var "klare og tilgængelige" og krævede ikke indsamling af personoplysninger. Under sådanne omstændigheder var staten forpligtet til ikke at hindre den udlevering af informationer, som sagsøgeren ønskede. Menneskerettighedsdomstolen fandt således, at hindringer, der har til formål at hindre aktindsigt i information af samfundsmæssig interesse, kan afholde parter, der arbejder i medierne eller tilknyttede områder, fra at udføre deres vigtige rolle som "offentlighedens vagthund". Domstolen konkluderede,

35 Se dog Den Europæiske Tilsynsførende for Databeskyttelses detaljerede overvejelser fra 2011 i "*Public access to documents containing personal data after the* Bavarian Lager *ruling*" Bruxelles, den 24. marts 2011, som findes på: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 Menneskerettighedsdomstolen, *Társaság a Szabadságjogokért mod Ungarn*, nr. 37374/05, 14. april 2009, præmis 27 og 36-38.

at den europæiske menneskerettighedskonventions artikel 10 var blevet overtrådt.

I EU-retten er betydningen af gennemsigtighed klart fastlagt. Princippet om gennemsigtighed er fastlagt ved artikel 1 og 10 i TEU og artikel 15, stk. 1, i TEUF. [37] I henhold til betragtning 2 i forordning (EF) nr. 1049/2001 giver åbenheden borgerne bedre mulighed for at deltage i beslutningsprocessen, sikrer forvaltningen en større legitimitet og effektivitet og gør den mere ansvarlig over for borgerne i et demokratisk system[38].

Følger man denne argumentation, kræver Rådets forordning (EF) nr. 1290/2005 om finansiering af den fælles landbrugspolitik og Kommissionens forordning (EF) nr. 259/2008 om gennemførelsesbestemmelser hertil, at der offentliggøres oplysninger om modtagerne af midler fra visse EU-fonde på landbrugsområdet og de beløb, hver støttemodtager har modtaget[39]. Offentliggørelsen skal bidrage til at kontrollere, at forvaltningen anvender de offentlige midler korrekt. Flere støttemodtagere har anfægtet proportionaliteten af denne offentliggørelse.

Eksempel: I sagen *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen*[40] 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.

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

37 EU (2012), konsoliderede udgaver af traktaten om Den Europæiske Union (TEU) og traktaten om Den Europæiske Unions funktionsmåde (TEUF), EUT 2012 C 326.

38 EU-Domstolen, C-41/00 P, *Interporc Im- und Export GmbH mod Europa-Kommissionen*, 6. marts 2003, præmis 39, og EU-Domstolen, C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd.*, 29. juni 2010, præmis 54.

39 Rådets forordning (EF) nr. 1290/2005 af 21. juni 2005 om finansiering af den fælles landbrugspolitik, EUT 2005 L 209, og 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 2008 L 76.

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

almindelighed og et indgreb i deres ret til beskyttelse af deres personoplysninger i særdeleshed.

Domstolen fandt, at et sådant indgreb i de rettigheder, der er fastlagt ved 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 EU's midler. EU-Domstolen fastslog dog, at offentliggørelsen af navnene på fysiske personer, som modtager EU-landbrugsstøtte fra de 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. Domstolen erklærede derfor EU-bestemmelserne om offentliggørelsen af oplysninger vedrørende modtagere af støtte fra de europæiske landbrugsfonde for delvist ugyldige.

1.2.3. 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. Den udøves under overholdelse af chartrets artikel 1 (Den menneskelige værdighed). Menneskerettighedsdomstolen finder, at friheden for kunst er beskyttet ved artikel 10 i den europæiske menneskerettighedskonvention (EMK)[41]. Den ret, der er sikret ved chartrets artikel 13, kan underkastes de begrænsninger, der er tilladt ifølge artikel 10 i EMK[42].

Eksempel: I sagen *Vereinigung bildender Künstler mod Østrig*[43] 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 forbud og imødekom hans begæring. Menneskerettighedsdomstolen gentog, at artikel 10 i EMK finder anvendelse på formidling af idéer, der støder, chokerer eller forstyrrer staten eller en del af befolkningen. Alle, der havde oprettet, udført,

41 Menneskerettighedsdomstolen, *Müller m.fl. mod Schweiz*, nr. 10737/84, 24. maj 1988.

42 Forklaringer til chartret om grundlæggende rettigheder, EUT 2007 C 303.

43 Menneskerettighedsdomstolen, *Vereinigung bildender Künstler mod Østrig*, nr. 68345/01, 25. januar 2007, især præmis 26 og 34.

distribueret eller udstillet kunstværker, havde bidraget til udvekslingen af idéer og holdninger, og staten var forpligtet til ikke uden grund at begrænse deres ytringsfrihed. Maleriet var en kollage og kun anvendte fotos af personernes hoveder, og deres kroppe var malet på en urealistisk og overdrevet måde, som tydeligvis ikke havde til formål at afspejle eller ligne virkeligheden, og Menneskerettighedsdomstolen 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 Menneskerettighedsdomstolen, at det ubegrænsede forbud mod yderligere udstilling af maleriet var uforholdsmæssigt. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 10 var blevet overtrådt.

Med hensyn til videnskab tages der i den europæiske lovgivning om databeskyttelse højde for videnskabens særlige værdi for samfundet. De generelle begrænsninger for anvendelsen af personoplysninger er derfor blevet indskrænket. Databeskyttelsesdirektivet og konvention 108 tillader begge lagring af data til videnskabelige formål, når de ikke længere er nødvendige til det formål, de oprindeligt tjente, da de blev indsamlet. Den efterfølgende anvendelse af personoplysninger til videnskabelige formål betragtes endvidere ikke som et uforeneligt formål. Mere detaljerede bestemmelser, herunder de fornødne garantier, for at forene de videnskabelige forskningsinteresser med retten til databeskyttelse udvikles gennem den nationale ret (se også afsnit 3.3.3 og 8.4).

1.2.4. Beskyttelse af ejendomsret

Ejendomsretten er omhandlet i artikel 1 i den første protokol til den europæiske menneskerettighedskonvention og i chartrets artikel 17, stk. 1. Et vigtigt aspekt af ejendomsretten 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[44]. Der har været sager, hvor 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*[45] vedrørte en spansk internetudbyders, Telefónica, afslag på at meddele Promusicae – en ikkekommerciel sammenslutning af musikproducenter og udgivere af musik og audiovisuelle optagelser – personlige oplysninger vedrørende benyttelse af internettet via opkoblinger 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 2000/31, 2001/29 og 2004/48 set i relation til chartrets artikel 17 og 47. Domstolen konkluderede, at disse tre direktiver og direktiv 2002/58 (direktivet om databeskyttelse inden for elektronisk kommunikation) 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 dels beskyttelsen af privatlivets fred, dels beskyttelsen 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

44 Menneskerettighedsdomstolen, *Ashby Donald m.fl. mod Frankrig*, nr. 36769/08, 10. januar 2013.

45 EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU*, 29. januar 2008, præmis 54 og 60.

af 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"[46].

46 *Ibid.*, præmis 65 og 68. Se også EU-Domstolen, C-360/10, *SABAM mod Netlog N.V.*, 16. februar 2012.

2

Databeskyttelses-terminologi

EU	Omhandlede emner	Europarådet
Personoplysninger		
Databeskyttelsesdirektivet, artikel 2, litra a). EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen*, 9. november 2010 EU-Domstolen, C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU*, 29. januar 2008	**Juridisk definition**	Konvention 108, artikel 2, litra a) Menneskerettigheds-domstolen, *Bernh Larsen Holding AS m.fl. mod Norge*, nr. 24117/08, 14. marts 2013
Databeskyttelsesdirektivet, artikel 8, stk. 1 EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003	**Særlige kategorier af personoplysninger (følsomme oplysninger)**	Konvention 108, artikel 6
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra e)	**Anonymiserede og pseudonymiserede oplysninger**	Konvention 108, artikel 5, litra e) Konvention 108, forklarende rapport, artikel 42
Behandling af personoplysninger		
Databeskyttelsesdirektivet, artikel 2, litra b) EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003	**Definitioner**	Konvention 108, artikel 2, litra c)
Brugere af personoplysninger		
Databeskyttelsesdirektivet, artikel 2, litra d)	**Den registeransvarlige**	Konvention 108, artikel 2, litra d) Henstilling om profilering, artikel 1, litra g)*

EU	Omhandlede emner	Europarådet
Databeskyttelsesdirektivet, artikel 2, litra e) EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003	**Registerfører**	Henstilling om profilering, artikel 1, litra h)
Databeskyttelsesdirektivet, artikel 2, litra g)	**Modtager**	Konvention 108, tillægsprotokol, artikel 2, stk. 1
Databeskyttelsesdirektivet, artikel 2, litra f)	**Tredjemand**	
Samtykke		
Databeskyttelsesdirektivet, artikel 2, litra h) EU-Domstolen, C-543/09, *Deutsche Telekom AG mod Tyskland*, 5. maj 2011	**Definition af og krav til gyldigt samtykke**	Henstilling om medicinske oplysninger, artikel 6, og diverse efterfølgende henstillinger

Note: * *Europarådet, Ministerudvalget (2010), henstilling 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").
- En person er identificerbar, hvis yderligere oplysninger kan indhentes uden urimelig indsats, således at den registrerede kan identificeres.
- 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 databeskyttelsesdirektivet, som kræver øget beskyttelse og derfor er underlagt særlige regler.
- Oplysninger er anonymiserede, hvis de ikke længere indeholder identifikatorer, og oplysninger er pseudonymiserede, hvis identifikatorerne er krypterede.
- Pseudonymiserede oplysninger er personoplysninger, hvorimod anonymiserede oplysninger ikke er personoplysninger.

2.1.1. Vigtigste aspekter af begrebet personoplysninger

I både **EU-retten** og **Europarådets retsorden** defineres "personoplysninger" som information om en identificeret eller identificerbar fysisk person[47], dvs. information om en person, hvis identitet umiddelbart fremgår eller som minimum kan fastslås ved at indhente yderligere oplysninger.

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

En person

Retten til databeskyttelse er udviklet på grundlag af retten til respekt for privatlivet. Konceptet privatliv vedrører mennesker. Fysiske personer er derfor de primære objekter for databeskyttelse. Desuden er kun *levende mennesker* beskyttet af den europæiske databeskyttelseslovgivning ifølge udtalelse fra Artikel 29-Gruppen[48].

Menneskerettighedsdomstolens retspraksis vedrørende artikel 8 i EMRKviser, at det kan være vanskeligt fuldstændigt af adskille forhold vedrørende privatliv og erhvervsmæssig virksomhed[49].

Eksempel: I sagen *Amann mod Schweiz*[50] aflyttede myndighederne et forretningsmæssigt telefonopkald til sagsøgeren. På grundlag af dette opkald undersøgte myndighederne sagsøgeren og udfyldte et kort om ansøgeren til det schweiziske socialsikringsregister. Selv om aflytningen vedrørte et forretningsmæssigt telefonopkald, fandt Menneskerettighedsdomstolen, at lagringen af data om telefonopkaldet vedrørte sagsøgerens privatliv. Den fastslog, at udtrykket "privatlivet" ikke skal fortolkes indskrænkende, navnlig fordi respekten for privatlivet omfattede retten til at indgå og udvikle forhold med andre mennesker. Der var desuden i princippet ikke er nogen grund til, at erhvervsmæssig eller forretningsmæssig virksomhed skulle være udelukket fra

47 Databeskyttelsesdirektivet, artikel 2, litra a), konvention 108, artikel 2, litra a).

48 Artikel 29-Gruppen (2007), udtalelse 4/2007 om begrebet personoplysninger, WP 136, 20. juni 2007, s. 22.

49 Se f.eks. Menneskerettighedsdomstolen, *Rotaru mod Rumænien* [GC], nr. 28341/95, 4. maj 2000, præmis 43, Menneskerettighedsdomstolen, *Niemietz mod Tyskland*, 13710/88, 16. december 1992, præmis 29.

50 Menneskerettighedsdomstolen, *Amann mod Schweiz* [GC], nr. 27798/95, 16. februar 2000, præmis 65.

begrebet "privatlivet". En så bred fortolkning svarer til fortolkningen i konvention 108. Menneskerettighedsdomstolen fandt videre, at indgrebet i sagsøgerens tilfælde ikke var i overensstemmelse med loven, da den nationale lovgivning ikke omfattede specifikke og detaljerede bestemmelser om indsamling, registrering og lagring af oplysninger. Domstolen konkluderede derfor, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Hvis forhold vedrørende erhvervsmæssig virksomhed også kan være underlagt databeskyttelse, er det tvivlsomt, om databeskyttelse kun gælder for fysiske personer. De rettigheder, der følger af den europæiske menneskerettighedskonvention, gælder ikke kun for fysiske personer, men for alle.

Menneskerettighedsdomstolen har afsagt domme i sager anlagt af juridiske personer med påstande om krænkelse af deres ret til beskyttelse af deres data omhandlet i artikel 8 i EMRK. Domstolen behandlede dog sagen med udgangspunkt i retten til respekt for hjem og kommunikation og ikke med udgangspunkt i retten til respekt for privatliv:

Eksempel: *Bernh Larsen Holding AS m.fl. mod Norge*[51] 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.

Menneskerettighedsdomstolen 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 iEMRK. 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 den europæiske menneskerettighedskonventions artikel 8 ikke var blevet overtrådt.

51 Menneskerettighedsdomstolen, *Bernh Larsen Holding AS m.fl. mod Norge*, nr. 24117/08, 14. marts 2013. Se dog også Menneskerettighedsdomstolen, *Liberty m.fl. mod Det Forenede Kongerige*, nr. 58243/00, 1. juli 2008.

I henhold til konvention 108 vedrører databeskyttelse primært beskyttelsen af fysiske personer. Kontraherende parter kan dog udvide databeskyttelsen til juridiske personer, f.eks. erhvervsvirksomheder og sammenslutninger, i deres nationale lovgivning. **EU's databeskyttelseslovgivning** dækker generelt ikke beskyttelsen af juridiske personer i forbindelse med behandlingen af oplysninger, som vedrører dem. De nationale lovgivere kan frit regulere dette område[52].

> Eksempel: I sagen *Volker og Markus Schecke GbR og Hartmut Eifert mod Land Hessen*[53] 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 [...]"[54].

En persons identificerbarhed

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

- hvis en person identificeres i den pågældende information, eller
- hvis en person 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. Menneskerettighedsdomstolen har gentagne gange udtalt, at begrebet "personoplysninger" ifølge den europæiske menneskerettighedskonvention er det samme som i konvention 108, især for så vidt angår betingelsen vedrørende identificerede eller identificerbare personer[55].

52 Databeskyttelsesdirektivet, betragtning 24.

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

54 *Ibid.*, præmis 52.

55 Se Menneskerettighedsdomstolen, *Amann mod Schweiz* [GC], nr. 27798/95, 16. februar 2000, præmis 65.

De juridiske definitioner af personoplysninger præciserer ikke yderligere, hvor en person anses for at være identificeret[56]. 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. Undtagelsesvis kan andre identifikatorer have samme virkning som et navn. For offentlige figurer kan det f.eks. være nok at nævne personens stilling, f.eks. formand for Europa-Kommissionen.

Eksempel: I sagen *Promusicae*[57] 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 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 som omhandlet i artikel 2, første afsnit, i direktiv 2002/58, sammenholdt med artikel 2, litra b), i direktiv 95/46".

Da mange navne ikke er unikke, kræves der i nogle tilfælde yderligere identifikatorer for at sikre, at en person ikke forveksles med en anden. Ofte anvendes fødselsdato og -sted. Nogle lande har desuden indført personnumre for bedre at kunne skelne mellem borgerne. Biometriske data, som f.eks. fingeraftryk, digitale fotos eller irisscanninger, 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 avanceret 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[58]. I henhold til databeskyttelsesdirektivets betragtning 26 er det afgørende, om rimelige midler til identifikation er

56 Se også Menneskerettighedsdomstolen, *Odièvre mod Frankrig* [GC], nr. 42326/98, 13. februar 2003, og Menneskerettighedsdomstolen, *Godelli mod Italien*, nr. 33783/09, 25. september 2012.

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

58 Databeskyttelsesdirektivet, artikel 2, litra a).

tilgængelige for og anvendes af de forventede brugere af informationen, herunder tredjepartsmodtagere (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. Nummerplader for myndigheden oplysninger om anonyme personer. Den lokale myndighed har ikke beføjelse til at få adgang til motorkøretøjsregistret for at finde frem til bilejerens eller førerens identitet.

Denne argumentation er ikke i overensstemmelse med databeskyttelsesdirektivets 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.

I henhold til Europarådets retsorden skal identificerbarhed forstås på en lignende måde. I artikel 1, stk. 2, i henstillingen om betalingsoplysninger[59] anføres det f.eks., at en person ikke anses for at være "identificerbar", hvis identifikation kræver en uforholdsmæssig mængde tid, omkostninger eller arbejde.

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.

59 Europarådet, Ministerudvalget (1990), henstilling nr. R Rec(90) 19 om beskyttelse af personoplysninger, der anvendes ved betaling og andre tilknyttede handlinger, 13. september 1990.

at gå ind i et sikkerhedsområde eller hæve penge på 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, ved at anmode om oplysninger, der kun bør kendes af personen med en bestemt identitet eller bemyndigelse, f.eks. et personligt identifikationsnummer (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 og chipkort, evt. kombineret med PIN-koder, er elektroniske signaturer et middel, der kan identificere og autentificere en person i forbindelse med elektronisk kommunikation.

Karakteren af personoplysninger

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

> Eksempel: En overordnets vurdering af en medarbejders indsats, som er lagret i medarbejderens dossier, er personoplysninger, 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*[60] fandt Menneskerettighedsdomstolen, at udtrykket "personoplysninger" ikke er begrænset til forhold inden for en persons privatsfære (se afsnit 2.1.1). Denne betydning af udtrykket "personoplysninger" er også relevant for databeskyttelsesdirektivet:

> Eksempel: I sagen *Volker og Markus Schecke GbR og Hartmut Eifert mod Land Hessen*[61] tilkendegav EU-Domstolen, at det i denne forbindelse er "uden betyd-

60 Se Menneskerettighedsdomstolen, *Amann mod Schweiz*, nr. 27798/95, 16. februar 2000, præmis 65.

61 Forenede sager C-92/09 og C-93/09, *Volker og Markus Schecke GbR og Hartmut Eifert mod Land Hessen*, 9. november 2010, præmis 59.

ning, at de offentliggjorte oplysninger vedrører erhvervsmæssig virksomhed […]. Den Europæiske Menneskerettighedsdomstol har i denne henseende på grundlag af fortolkningen af konventionens artikel 8 fastslået, at udtrykket "privatlivet" ikke skal fortolkes indskrænkende, og at der ikke er nogen grund til, at erhvervsmæssig eller forretningsmæssig virksomhed skulle være udelukket fra begrebet "privatlivet"".

Oplysninger vedrører også personer, hvis indholdet af informationen indirekte afslører oplysninger om en person. I nogle tilfælde, hvor der er en tæt forbindelse mellem en genstand eller en begivenhed – f.eks. en mobiltelefon, en bil eller et uheld – på den ene side og en person – f.eks. ejeren, brugeren eller offeret – på den anden, bør information om genstanden eller begivenheden også betragtes som personoplysninger.

Eksempel: I sagen *Uzun mod Tyskland*[62] blev sagsøgeren og en anden mand sat under overvågning via en GPS-anordning, som var anbragt i den anden mands bil, fordi de var under mistanke for at være involveret i bombeangreb. I dette tilfælde fastslog Menneskerettighedsdomstolen, at overvågningen af sagsøgeren via GPS udgjorde et indgreb i hans privatliv, jf. artikel 8 i EMK. GPS-overvågningen var dog sket i overensstemmelse med lovgivningen og var rimelig i forhold til det legitime formål, nemlig at efterforske flere mordforsøg. Overvågningen var derfor nødvendig i et demokratisk samfund. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 ikke var blevet overtrådt.

Oplysningernes form

Den form, hvori personoplysninger lagres eller anvendes, er ikke relevant, når det afgøres, om databeskyttelseslovgivningen finder anvendelse. Skriftlig eller mundtlig kommunikation kan indeholde personoplysninger, og det samme gælder billeder[63], herunder videoovervågning[64], og lyd[65]. Elektronisk registrerede oplysninger og

62 Menneskerettighedsdomstolen, *Uzun mod Tyskland*, nr. 35623/05, 2. september 2010.

63 Menneskerettighedsdomstolen, *Von Hannover mod Tyskland*, nr. 59320/00, 24. juni 2004, og Menneskerettighedsdomstolen, *Sciacca mod Italien*, nr. 50774/99, 11. januar 2005.

64 Menneskerettighedsdomstolen, *Peck mod Det Forenede Kongerige*, nr. 44647/98, 28. januar 2003, Menneskerettighedsdomstolen, *Köpke mod Tyskland*, nr. 420/07, 5. oktober 2010.

65 Databeskyttelsesdirektivet, betragtning 16 og 17, Menneskerettighedsdomstolen, *P.G. og J.H. mod Det Forenede Kongerige*, nr. 44787/98, 25. september 2001, præmis 59 og 60, Menneskerettighedsdomstolen, *Wisse mod Frankrig*, nr. 71611/01, 20. december 2005.

oplysninger på papir kan være personoplysninger. Selv celleprøver af menneskeligt væv kan være personoplysninger, idet de registrerer en persons dna.

2.1.2. Særlige kategorier af personoplysninger

I henhold til EU-retten og **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. Behandling af disse særlige kategorier af oplysninger ("følsomme oplysninger") tillades derfor kun, hvis der gives specifikke garantier.

Ved definitionen af følsomme oplysninger udpeges følgende kategorier i både konvention 108 (artikel 6) og databeskyttelsesdirektivet (artikel 8):

- personoplysninger om racemæssig eller etnisk baggrund
- personoplysninger om politisk, religiøs eller filosofisk overbevisning
- oplysninger om helbredsforhold og seksuelle forhold.

> Eksempel: I sagen *Bodil Lindqvist*[66] tilkendegav EU-Domstolen, at "angivelsen af den omstændighed, at en person har beskadiget sin fod og er delvis sygemeldt, udgør en personoplysning om helbredsforhold i den forstand, hvori udtrykket er anvendt i artikel 8, stk. 1, i direktiv 95/46".

Databeskyttelsesdirektivet betegner endvidere "fagforeningsmæssigt tilhørsforhold" som en følsom oplysning, da denne information kan være en stærk indikator for politisk overbevisning eller tilknytning.

I konvention 108 betragtes personoplysninger vedrørende straffedomme også som følsomme.

I henhold til artikel 8, stk. 7, i databeskyttelsesdirektivet bestemmer EU's medlemsstater "på hvilke betingelser et nationalt identifikationsnummer eller andre almene midler til identifikation kan gøres til genstand for behandling".

66 EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003, præmis 51.

2.1.3. Anonymiserede og pseudonymiserede oplysninger

I overensstemmelse med det princip om begrænset lagring af personoplysninger, der er fastlagt ved både databeskyttelsesdirektivet og konvention 108 (og som drøftes i yderligere detaljer i kapitel 3), må personoplysninger ikke "opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt"[67]. Som følge deraf skal personoplysninger anonymiseres, hvis en registeransvarlig ønsker at lagre dem, efter at de er blevet forældet og ikke længere tjener deres oprindelige formål.

Anonymiserede oplysninger

Oplysninger er anonymiserede, hvis alle identificerende elementer er blevet fjernet fra et sæt personoplysninger. Informationen må ikke indeholde elementer, som med en rimelig indsats kan bruges til igen at identificere den pågældende person[68]. Hvis oplysninger er blevet anonymiseret, er de ikke længere personoplysninger.

Hvis personoplysninger ikke længere tjener deres oprindelige formål, men opbevares i en personaliseret form i historisk, statistisk eller videnskabeligt øjemed, er det tilladt i henhold til databeskyttelsesdirektivet og konvention 108, såfremt der gives tilstrækkelige garantier mod misbrug[69].

Pseudonymiserede oplysninger

Personoplysninger indeholder identifikatorer, som f.eks. navn, fødselsdato, køn og adresse. Når personoplysninger er pseudonymiserede, er identifikatorerne erstattet af et pseudonym. Pseudonymisering opnås ved kryptering af identifikatorerne i personoplysninger.

Pseudonymiserede oplysninger er ikke udtrykkeligt nævnt i de juridiske definitioner i hverken konvention 108 eller databeskyttelsesdirektivet. I den forklarende rapport til konvention 108 anføres det dog i artikel 42, at kravet om tidsfrister for opbevaring af oplysninger i deres navnesammenkædede form ikke betyder, at

67 Databeskyttelsesdirektivet, artikel 6, stk. 1, litra e), og konvention 108, artikel 5, litra e).

68 *Ibid.*, betragtning 26.

69 *Ibid.*, artikel 6, stk. 1, litra e), og konvention 108, artikel 5, litra e).

oplysningerne efter en vis periode uigenkaldeligt skal adskilles fra navnet på den person, de vedrører, men, at det ikke må være muligt umiddelbart at sammenkæde oplysningerne og identifikatorerne. Dette er en virkning, der kan opnås ved at pseudonymisere oplysningerne. For alle, der ikke er i besiddelse af krypteringsnøglen, kan pseudonymiserede oplysninger kun identificeres med besvær. Forbindelsen til en identitet findes dog stadig i form af pseudonymet og krypteringsnøglen. Genidentifikation er let for alle, der har ret til at anvende krypteringsnøglen. Det skal sikres, at krypteringsnøgler kun kan anvendes af bemyndigede personer.

Da pseudonymisering af oplysninger er et af de vigtigste hjælpemidler til at opnå databeskyttelse på et større område, hvor anvendelsen af personoplysninger ikke kan undgåsfuldstændigt, skal funktionsmåden og virkningen af denne foranstaltning forklares i yderligere detaljer.

Eksempel: Sætningen "Carl Sørensen, født den 3. april 1967, er far til fire børn, to drenge og to piger" kan f.eks. pseudonymiseres på følgende måde:

"C.S. 1967 er far til fire børn, to drenge og to piger", eller

"324 er far til fire børn, to drenge og to piger", eller

"YESz320l er far til fire børn, to drenge og to piger".

Brugere, der får adgang til disse pseudonymiserede oplysninger, har normalt ikke mulighed for at identificere "Carl Sørensen, født den 3. april 1967" ud fra "324" eller "YESz3201". Pseudonymiserede oplysninger vil derfor være bedre beskyttet mod misbrug.

Det første eksempel er dog mindre sikkert. Hvis sætningen "C.S. 1967 er far til fire børn, to drenge og to piger" anvendes i en lille landsby, hvor Carl Sørensen bor, kan det være let at genkende hr. Sørensen. Pseudonymiseringsmetoden har betydning for effektiviteten af databeskyttelsen.

Personoplysninger med krypterede identifikatorer anvendes i mange sammenhænge som en metode til at hemmeligholde identiteten af personer. Dette er især nyttigt, hvis registeransvarlige skal sikre, at de arbejder med de samme registrerede, men ikke har brug for eller ikke burde have adgang til de registreredes virkelige identiteter. Dette er f.eks. tilfældet, når en forsker studerer forløbet af en

sygdom hos patienter, hvis identitet kun kendes af det sygehus, hvor de behandles, og som forskeren modtager de pseudonymiserede journaler fra. Pseudonymisering er derfor et stærkt led i teknologier til beskyttelse af privatlivet. Metoden kan være et vigtigt element ved indførelsen af løsninger af typen "privacy by design", dvs. løsninger, hvor databeskyttelse er indbygget i selve de avancerede databehandlingssystemer.

2.2. Databehandling

Hovedpunkter

- Udtrykket "behandling" henviser primært til elektronisk behandling.
- I henhold til EU-retten henviser "behandling" desuden 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.

I konvention 108 og databeskyttelsesdirektivet omhandler databeskyttelse primært elektronisk databehandling.

I **Europarådets retsorden** anerkendes det dog i definitionen af elektronisk behandling, at ikke-elektronisk anvendelse af personoplysninger kan være påkrævet i visse faser mellem elektroniske operationer. I **EU-retten** er elektronisk databehandling ligeledes defineret som "operationer med eller uden brug af elektronisk databehandling, som personoplysninger gøres til genstand for"[70].

Eksempel: I sagen *Bodil Lindqvist*[71] fastslog EU-Domstolen, 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".

70 Konvention 108, artikel 2, litra c), og databeskyttelsesdirektivet, artikel 2, litra b), og artikel 3, stk. 1.

71 EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003, præmis 27.

Ikke-elektronisk databehandling kræver også databeskyttelse. I **EU-retten** er databeskyttelse på ingen måde begrænset til elektronisk databehandling. Databeskyttelse gælder således i EU-retten for behandlingen af personoplysninger i et ikke-elektronisk register, dvs. et særligt struktureret papirregister[72]. Databeskyttelse er her udvidet af følgende grunde:

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

- Opbevaring af personoplysninger i strukturerede papirregistre gør det nemt at omgå de begrænsninger, der ved lov er fastsat for elektronisk databehandling[73].

I **Europarådets retsorden omhandler** konvention 108 primært elektronisk databehandling[74]. Den tillader dog, at beskyttelsen ved national lovgivning udvides til ikke-elektronisk behandling. Mange parter i konvention 108 har benyttet denne mulighed og har fremsat erklæringer herom til Europarådets generalsekretær[75]. Udvidelse af databeskyttelse i medfør af en sådan erklæring skal vedrøre alle former for ikke-elektronisk databehandling og kan ikke begrænses til behandling i ikke-elektroniske registre[76].

For så vidt angår arten af omfattede behandlinger, skal begrebet "behandling" forstås på en omfattende måde i henhold til **både EU-retten og Europarådets retsorden**: "»behandling af personoplysninger« (»behandling«) enhver operation eller række af operationer - med eller uden brug af elektronisk databehandling - som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring samt blokering, slettelse eller tilintetgørelse"[77]. Udtrykket "behandling" omfatter også operationer, hvorved ansvaret for data overføres fra én registeransvarlig til en anden.

72 Databeskyttelsesdirektivet, artikel 3, stk. 1.

73 *Ibid.*, betragtning 27.

74 Konvention 108, artikel 2, litra b.

75 Se erklæringer fremsat i medfør af konvention 108, artikel 3, stk. 2, litra c).

76 Se ordlyden af konvention 108, artikel 3, stk. 2.

77 Databeskyttelsesdirektivet, artikel 2, litra b). Se også konvention 108, artikel 2, litra c).

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

Arbejdsgivere skal fremsende personalets lønoplysninger til skattemyndighederne. Denne fremsendelse af data udgør også "behandling", således som dette udtryk er defineret i konvention 108 og databeskyttelsesdirektivet. 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. Retsgrundlaget er normalt en del af bestemmelserne i de nationale skattelove. Uden sådanne bestemmelser ville videregivelsen af sådanne oplysninger udgøre ulovlig behandling.

2.3. Brugerne af personoplysninger

Hovedpunkter

- Enhver, der beslutter at behandle andres personoplysninger, er en "registeransvarlig" i henhold til databeskyttelseslovgivningen. Hvis flere tager denne beslutning sammen, kan de være "fælles registeransvarlige".
- En "registerfører" er en juridisk særskilt enhed, der behandler personoplysninger på den registeransvarliges vegne.
- En registerfører bliver registeransvarlig, hvis han eller hun anvender oplysninger til sine egne formål og ikke følger en registeransvarligs instrukser.
- Alle, der modtager oplysninger fra en registeransvarlig, er en "modtager".
- En "tredjemand" er en fysisk eller juridisk person, der ikke handler under den registeransvarliges instrukser (og ikke er den registrerede).
- En "tredjemandsmodtager" er en person eller enhed, der er juridisk adskilt fra den registeransvarlige, men som modtager personoplysninger fra den registeransvarlige.

2.3.1. Registeransvarlige og registerførere

At være registeransvarlig eller registerfører medfører primært et juridisk ansvar for at overholde de respektive forpligtelser, der følger af databeskyttelseslovgivningen. Kun parter, der kan drages til ansvar efter den gældende lovgivning, kan derfor

påtage sig disse roller. I den private sektorer er dette normalt en fysisk eller juridisk person. I den offentlige sektor er det normalt en myndighed. Andre enheder, som f.eks. organer eller institutioner, der ikke har status som juridisk person, kan kun være registeransvarlige eller registerførere, hvis det er tilladt i henhold til særskilte juridiske bestemmelser.

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

I koncerner udgør moderselskabet og hvert datterselskab, som er særskilte juridiske personer, særskilte registeransvarlige eller registerførere. Denne særskilte juridiske status betyder, at videregivelsen af oplysninger mellem medlemmerne af en koncern kræver et særskilt retsgrundlag. Der er ingen særrettigheder, der tillader, at personoplysninger som sådan udveksles mellem de særskilte juridiske enheder i en koncern.

I den sammenhæng skal privatpersoners rolle nævnes. I henhold til **EU-retten** er privatpersoner ikke omfattet af databeskyttelsesdirektivets bestemmelser, når de behandler oplysninger om andre som led i rent personlige eller familiemæssige aktiviteter. De betragtes ikke som registeransvarlige[78].

Retspraksis viser dog, at databeskyttelseslovgivningen stadig finder anvendelse, når en privatperson i forbindelse med brug af internettet offentliggør oplysninger om andre.

Eksempel: EU-Domstolen fastholdt i sagen *Bodil Lindqvist*[79], 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 direktiv 95/46"[80].

78 Databeskyttelsesdirektivet, betragtning 12, og artikel 3, stk. 2, sidste led.

79 EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003.

80 *Ibid.*, præmis 27.

Denne form for behandling af personoplysninger udgør ikke rent personlige eller familiemæssige aktiviteter, som er uden for databeskyttelsesdirektivets anvendelsesområde, 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"[81].

Den registeransvarlige

I EU-retten defineres en registeransvarlig som den, "der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger"[82]. En registeransvarligs afgørelse fastlægger, hvorfor og hvordan oplysninger skal behandles. **I Europarådets retsorden** nævner definitionen af "registeransvarlig" desuden, at en registeransvarlig afgør, hvilke kategorier af personoplysninger der bør opbevares[83].

Konvention 108 henviser i sin definition af en registeransvarlig til endnu et aspekt af ansvar for registre, der skal tages i betragtning. Denne definition omhandler også spørgsmålet om, hvem der lovligt må behandle visse personoplysninger til et bestemt formål. Hvis angiveligt ulovlig behandling finder sted, og den registeransvarlige skal udpeges, betragtes den person eller enhed, som f.eks. en virksomhed eller en myndighed, der traf afgørelse om, at de pågældende oplysninger skulle behandles, uanset om den i henhold til loven havde ret til at gøre det[84], som den registeransvarlige. En anmodning om sletning skal derfor altid rettes til den "faktiske" registeransvarlige.

Fælles kontrol

I henhold til databeskyttelsesdirektivets definition af "registeransvarlig" kan der være flere juridisk særskilte enheder, der sammen eller i fællesskab handler som registeransvarlig. Det betyder, at de sammen træffer afgørelse om at behandle data

81 *Ibid.*, præmis 47.

82 Databeskyttelsesdirektivet, artikel 2, litra d).

83 Konvention 108, artikel 2, litra d).

84 Se også Artikel 29-Gruppen (2010), *udtalelse 1/2010 om begreberne "registeransvarlig" og "registerfører"*, WP 169, Bruxelles, den 16. februar 2010, s. 15.

til et fælles formål[85]. Dette tillades dog kun i tilfælde, hvor der er et særligt retsgrundlag for den fælles behandling til et fælles formål.

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

Bestemmelserne fastlægger ikke udtrykkeligt, om fælles kontrol kræver, at det fælles formål er det samme for hver af de registeransvarlige, eller om det er tilstrækkeligt, at deres formål kun overlapper delvist. Der findes dog endnu ingen relevant retspraksis på europæisk plan, og der er heller ingen klarhed med hensyn til de ansvarsmæssige følger. I henhold til Artikel 29-Gruppen bør begrebet fælles kontrol fortolkes bredere, således at der opnås en vist fleksibilitet, som kan imødegå den stigende kompleksitet, der i dag opleves i forbindelse med databehandling[86]. Et tilfælde, der involverer SWIFT (Worldwide Interbank Financial Telecommunication) illustrerer gruppens holdning.

Eksempel: I SWIFT-sagen anvendte de europæiske bankinstitutter indledningsvis SWIFT som registerfører til at foretage dataoverførsler i forbindelse med banktransaktioner. SWIFT videregav sådanne banktransaktionsdata, som var lagret i et center for elektroniske tjenester i USA, til det amerikanske finansministerium uden udtrykkeligt at have fået ordre til at gøre dette fra de europæiske bankinstitutter, der benyttede tjenesten. Ved evalueringen af lovligheden af denne situation konkluderede Artikel 29-Gruppen, at de europæiske bankinstitutter, der benyttede SWIFT, og SWIFT selv skulle betragtes som fælles registeransvarlige, som over for de europæiske kunder var ansvarlige for fremlæggelsen af deres personoplysninger til de amerikanske myndigheder[87]. Ved at træffe afgørelse om fremlæggelsen havde SWIFT – ulovligt – påtaget sig rollen som registeransvarlig. Bankinstitutterne havde tydeligvis misligholdt deres forpligtelse til at føre tilsyn med registerføreren og kunne derfor ikke helt fritages

85 Databeskyttelsesdirektivet, artikel 2, litra d).

86 Artikel 29-Gruppen (2010), *udtalelse 1/2010 om begreberne "registeransvarlig" og "registerfører"*, WP 169, Bruxelles, den 16. februar 2010, s. 19.

87 Artikel 29-Gruppen (2006), *udtalelse 10/2006 om behandling af personoplysninger af Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Bruxelles, den 22. november 2006.

for deres ansvar som registeransvarlige. Denne situation betyder, at parterne er fælles registeransvarlige.

Registerfører

En registerfører defineres **i EU-retten** som den, der behandler personoplysninger på den registeransvarliges vegne[88]. De aktiviteter, der overlades til en registerfører, kan være begrænset til en meget specifik opgave eller sammenhæng eller kan være ganske generel og omfattende.

I Europarådets retsorden defineres en registerfører på samme måde som i EU-retten.

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

Eksempler: Virksomheden Everready er specialiseret i databehandling i forbindelse med administration af personaleoplysninger for andre virksomheder. I denne funktion er Everready registerfører.

Når Everready behandler oplysninger om sine egne medarbejdere, er virksomheden dog den registeransvarlige for databehandling, der har til formål at opfylde virksomhedens forpligtelser som arbejdsgiver.

Forholdet mellem registeransvarlig og registerfører

Den registeransvarlige defineres således som den, der afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Eksempel: Direktøren for virksomheden Sunshine beslutter, at virksomheden Moonlight, som har specialiseret sig i markedsanalyse, skal udføre en markedsanalyse på baggrund af Sunshines kundedata. Selv om opgaven med at afgøre hjælpemidlerne til at foretage behandlingen uddelegeres til Moonlight, er virksomheden Sunshine stadig den registeransvarlige, og Moonlight er kun

88 Databeskyttelsesdirektivet, artikel 2, litra e).

registerfører, idet Moonlight i henhold til aftalen kun må anvende Sunshines kundedata til de formål, som Sunshine fastlægger.

Hvis beføjelsen til at afgøre, med hvilke hjælpemidler behandlingen foretages, uddelegeres til en registerfører, skal den registeransvarlige stadig kunne blande sig i registerførerens beslutninger med hensyn til hjælpemidler til behandling. Det overordnede ansvar ligger stadig hos den registeransvarlige, som skal føre tilsyn med registerførerne for at sikre, at deres beslutninger er i overensstemmelse med databeskyttelseslovgivningen. En aftale, som forbyder den registeransvarlige at blande sig i registerførerens beslutninger, ville derfor sandsynligvis medføre, at parterne ville blive betragtet som fælles registeransvarlige og således delte det fælles juridiske ansvar som registeransvarlig.

Hvis en registerfører ikke overholder de begrænsninger for anvendelsen af oplysninger, som den registeransvarlige har fastlagt, bliver registerføreren registeransvarlig, for så vidt vedkommende overtræder den registeransvarliges instrukser. Dette vil sandsynligvis gøre registerføreren til en registeransvarlig, der handler ulovligt. Den oprindelige registeransvarlige skal til gengæld forklare, hvordan det var muligt for registerføreren at overtræde sit mandat. I henhold til Artikel 29-Gruppen er der ofte tale om fælles kontrol i sådanne tilfælde, at det sikrer den bedste beskyttelse af de registreredes interesser[89]. En vigtig følge af fælles kontrol bør være solidarisk hæftelse, således at de registrerede får flere retsmidler.

Der kan også være problemer i forbindelse med ansvarsfordelingen, når en registeransvarlig er en lille virksomhed, og registerføreren 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 skal fastholdes[90].

Af hensyn til klarheden og gennemsigtigheden bør detaljerne om forholdet mellem en registeransvarlig og en registerfører registreres i en skriftlig kontrakt[91]. Hvis en

89 Artikel 29-Gruppen (2010), *udtalelse 1/2010 om begreberne "registeransvarlig" og "r1egisterfører"*, WP 169, Bruxelles, den 16. februar 2010, s. 25, og Artikel 29-Gruppen (2006), *udtalelse 10/2006 om behandling af personoplysninger af Society for Worldwide Interbank Financial Telecommunication (SWIFT),* WP 128, Bruxelles, den 22. november 2006.

90 Artikel 29-Gruppen (2010), *udtalelse 1/2010 om begreberne "registeransvarlig" og "registerfører" 1/2010 om begreberne "registeransvarlig" og "registerfører",* WP 169, Bruxelles, den 16. februar 2010, s. 26.

91 Databeskyttelsesdirektivet, artikel 17, stk. 3 og 4.

sådan kontrakt ikke forefindes, er det et brud på den registeransvarliges forpligtelse til at fremlægge skriftlig dokumentation for parternes gensidige ansvar, og det kan medføre sanktioner[92].

Registerførere kan vælge at uddelegere visse opgaver til yderligere underkontraherede registerførere. Dette er tilladt i henhold til lovgivningen og afhænger i detaljer af kontraktbestemmelserne mellem den registeransvarlige og registerføreren, herunder om den registeransvarliges godkendelse er nødvendig i hvert enkelt tilfælde, eller om underretning alene er tilstrækkelig.

I Europarådets retsorden gælder fortolkningen af begreberne registeransvarlig og registerfører, jf. ovennævnte, fuldt ud, som det fremgår af de henstillinger, der er udarbejdet på grundlag af konvention 108[93].

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 registeransvarlige og dermed deres bemyndigelse til at få adgang til de personoplysninger, som den registeransvarlige ligger inde med.

En "tredjemand" er en part, som er juridisk adskilt fra den registeransvarlige. Fremlæggelse af oplysninger for en tredjemand kræver derfor altid et særskilt retsgrundlag. I henhold til databeskyttelsesdirektivets artikel 2, litra f), er en tredjemand "enhver anden fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ end den registrerede, den registeransvarlige, registerføreren og de personer under den registeransvarliges eller registerførerens direkte myndighed, der er beføjet til at behandle oplysningerne". Det betyder, at personer, der arbejder for en organisation, som er juridisk adskilt fra den registeransvarlige – selv om den 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"[94].

92 Artikel 29-Gruppen (2010), *udtalelse 1/2010 om begreberne "registeransvarlig" og "registerfører"*, WP 169, Bruxelles, den 16. februar 2010, s. 27.

93 Se eksempelvis henstilling om profilering, artikel 1.

94 Artikel 29-Gruppen (2010), *udtalelse 1/2010 om begreberne "registeransvarlig" og "registerfører"*, WP 169, Bruxelles, den 16. februar 2010, s. 31.

"Modtager" er et bredere udtryk end "tredjemand". I henhold til databeskyttelsesdirektivets artikel 2, litra g), er en modtager "den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, hvortil oplysningerne meddeles, uanset om der er tale om en tredjemand". Modtageren kan være en person uden for den registeransvarliges eller registerførerens organisation – og er så en tredjemand – eller en person inden for den registeransvarliges eller registerførerens organisation, som f.eks. en medarbejder eller en anden division inden for samme virksomhed eller myndighed.

Sondringen mellem modtagere og tredjemænd er kun vigtig på grund af betingelserne for lovlig fremlæggelse af oplysninger. En registeransvarligs eller registerførers medarbejdere kan uden yderligere juridiske krav være modtagere af personoplysninger, hvis de er involveret i den registeransvarliges eller registerførerens behandlingsaktiviteter. En tredjemand, som er juridisk adskilt fra den registeransvarlige eller registerføreren, er på den anden side ikke beføjet til at anvende de personoplysninger, der behandles af den registeransvarlige, medmindre der foreligger et særligt retsgrundlag i et konkret tilfælde. "Tredjemandsmodtagere" af oplysninger skal derfor altid have et retsgrundlag for lovligt at modtage personoplysninger.

Eksempel: En registerførers 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 registerførerens instrukser.

Hvis den samme medarbejder beslutter at bruge de oplysninger, som han eller hun kan få adgang til som registerførerens medarbejder, til egne formål og sælger dem til en anden virksomhed, handler medarbejderen som en tredjemand. Den pågældende medarbejder følger ikke længere registerførerens (arbejdsgiverens) instrukser. Som tredjemand skal medarbejderen have et retsgrundlag for at få adgang til og sælge oplysningerne. I dette eksempel har medarbejderen bestemt ikke et sådant retsgrundlag, og vedkommendes handlinger er derfor ulovlige.

2.4. Samtykke

Hovedpunkter

- Samtykke som retsgrundlag for behandling af personoplysninger skal være frivilligt, specifikt og givet på et velinformeret grundlag.
- Samtykke skal være givet utvetydigt. Samtykke kan være givet udtrykkeligt eller underforstået ved at handle på en måde, som ikke efterlader tvivl om, at den registrerede accepterer behandlingen af vedkommendes personoplysninger.
- Behandling af følsomme oplysninger på grundlag af samtykke kræver udtrykkeligt samtykke.
- Samtykke kan til enhver tid trækkes tilbage.

Samtykke betyder "enhver frivillig, specifik og informeret viljetilkendegivelse"[95]. Det er i adskillige sager retsgrundlaget for legitim databehandling (se afsnit 4.1).

2.4.1. Elementerne i et gyldigt samtykke

I henhold til **EU-retten** skal tre kriterier opfyldes, for at et samtykke er gyldigt. Dette har til formål at sikre, at registrerede virkeligt havde til hensigt at acceptere anvendelsen af deres oplysninger:

- Den registrerede må ikke have været under pres, da vedkommende gav sit samtykke.
- Den registrerede skal være blevet behørigt informeret om formålet med og følgerne af samtykket.
- Omfanget af samtykket skal være rimeligt konkret.

Kun hvis alle disse krav er opfyldt, vil samtykket være gyldigt ifølge databeskyttelseslovgivningen.

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, som det fremgår af de henstillinger,

95 Databeskyttelsesdirektivet, artikel 2, litra h).

der er udarbejdet på grundlag af konvention 108[96]. Kravene til samtykke er de samme som kravene til en gyldig hensigtserklæring i europæisk civilret.

Yderligere civilretlige krav til et gyldigt samtykke, som f.eks. rets- og handleevne, gælder naturligvis også i forbindelse med databeskyttelse, da sådanne krav er grundlæggende juridiske forudsætninger. Ugyldigt samtykke fra personer, der ikke har rets- og handleevne, betyder, at der ikke er et retsgrundlag for at behandle oplysninger om sådanne personer.

Samtykket kan gives udtrykkeligt[97] eller underforstået. Ved udtrykkeligt samtykke er der ingen tvivl om den registreredes hensigt, og det kan gives mundtligt eller skriftligt. Underforstået samtykke udledes af omstændighederne. Ethvert samtykke skal gives på en utvetydig måde[98]. Det betyder, at der ikke må være urimelig tvivl om, at den registrerede ønskede at meddele sin accept af behandlingen af vedkommendes oplysninger. Manglende aktivitet kan ikke være baggrunden for et utvetydigt samtykke. Hvis følsomme oplysninger skal behandles, skal samtykke gives udtrykkeligt og utvetydigt.

Frivilligt samtykke

Der er kun tale om frivilligt samtykke, hvis den registrerede kan træffe et reelt valg, og der ikke er risiko for vildledning, manipulation, tvang eller væsentlige negative følger, hvis vedkommende ikke giver sit samtykke[99].

Eksempel: I mange lufthavne skal passagererne gå gennem kropsscannere for at komme til afgangsområdet[100]. Eftersom passagerernes personoplysninger behandles under scanningen, skal behandlingen opfylde et af de krav, der er anført i databeskyttelsesdirektivets artikel 7 (se afsnit 4.1.1). Det at gå gennem kropsscannere præsenteres nogle gange som en mulighed for passagererne, hvilket betyder, at deres samtykke hertil berettiger behandlingen. Passagerer kan dog frygte, at det vil udløse mistanke eller yderligere kontrol, f.eks. kropsvisitering, hvis de nægter at gå gennem kropsscanneren. Mange passagerer giver

96 Se eksempelvis konvention 108, henstilling vedrørende statistiske oplysninger, punkt 6.

97 Databeskyttelsesdirektivet, artikel 8, stk. 2.

98 *Ibid.*, artikel 7, litra a), og artikel 26, stk. 1.

99 Se også Artikel 29-Gruppen (2011), udtalelse 15/2011 om udtrykket samtykke, WP 187, Bruxelles, den 13. juli 2011, s. 12.

100 Dette eksempel er hentet fra *Ibid.*, s. 15.

deres samtykke til scanningen, fordi de derved undgår potentielle problemer eller forsinkelser. Et sådant samtykke er angiveligt ikke tilstrækkeligt frivilligt.

Et tilstrækkeligt retsgrundlag kan derfor kun findes i lovgivningsbestemmelser baseret på databeskyttelsesdirektivets artikel 7, litra e), som pålægger passagererne en forpligtelse til at samarbejde af hensyn til vigtige samfundsinteresser. Sådanne bestemmelser kan stadig omfatte et valg mellem scanning og kropsvisitering, men kun som en del af yderligere grænsekontrolforanstaltninger, som er påkrævet under særlige omstændigheder. Det er, hvad Europa-Kommissionen fastlagde i to forordninger om securityscannere i 2011[101].

Frivilligt samtykke kan også være truet, hvis der er tale om subordination med betydelig økonomisk eller anden forskel mellem den registeransvarlige, som indhenter samtykket, og den registrerede, som giver sit samtykke[102].

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 klart, at offentliggørelsen af et foto i en medarbejderfortegnelse ikke i sig selv har negative følger, og fordi medarbejderen næppe vil opleve negative følger fra arbejdsgiverens side, hvis han eller hun ikke ønsker at få sit foto offentliggjort i medarbejderfortegnelsen.

101 Kommissionens forordning (EU) nr. 1141/2011 af 10. november 2011 om ændring af forordning (EF) nr. 272/2009 om supplering af de fælles grundlæggende normer for civil luftfartssikkerhed, for så vidt angår anvendelsen af securityscannere i EU's lufthavne, EUT 2011 L 293, og Kommissionens gennemførelsesforordning (EU) nr. 1147/2011 af 11. november 2011 om ændring af forordning (EU) nr. 185/2010 om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed, EUT 2011 L 294.

102 Se også Artikel 29-Gruppen (2001), udtalelse 8/2001 om behandling af personoplysninger i ansættelsesforhold, WP 48, Bruxelles, den 13. september 2001, og 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, den 25. november 2005.

Det betyder dog ikke, at et samtykke aldrig kan være gyldigt under omstændigheder, hvor det vil have negative følger, hvis samtykke ikke gives. Hvis det forhold, at der ikke gives samtykke til at modtage et kundekort fra et supermarked, kun betyder, at kunden ikke modtager rabat på bestemte varer, er samtykket stadig et gyldigt retsgrundlag for behandling af personoplysninger om de kunder, der har givet samtykke til at modtage et sådant kort. Der er ikke tale om subordination mellem virksomheden og kunden, og følgerne af ikke at give sit samtykke er ikke tilstrækkeligt alvorlige for den registrerede til at forhindre et frit valg.

Når tilstrækkeligt vigtige varer eller tjenester kun kan erhverves, hvis visse personoplysninger fremlægges for tredjemand, kan den registreredes samtykke til fremlæggelsen af vedkommendes oplysninger på den anden side normalt ikke betragtes som en frivillig beslutning, og et sådant samtykke er derfor ikke gyldigt i henhold til databeskyttelseslovgivningen.

Eksempel: Passagerers accept af, at et flyselskab overfører såkaldte PNR-oplysninger (Passenger Name Records), dvs. oplysninger om deres identitet, menuvalg eller sundhedsproblemer, til immigrationsmyndighederne i et bestemt 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.

Informeret samtykke

Den registrerede skal have tilstrækkelig information, inden vedkommende træffer sit valg. Om den fremlagte information er tilstrækkelig, kan kun afgøres fra sag til sag. Normalt omfatter et informeret samtykke en præcis og letforståelig beskrivelse af det forhold, der kræver samtykke, og en kort gengivelse af følgerne af at give sit samtykke eller ikke at give sit samtykke. Sprogbrugen i denne information bør tilpasses målgruppen for informationen.

Informationen skal også være lettilgængelig for den registrerede. Det er vigtigt, at informationen er tilgængelig og synlig. I et onlinemiljø kan lagdelte informationer være en god løsning, hvis det giver den registrerede adgang til en mere omfattende udgave i tillæg til den kortfattede udgave.

Specifikt samtykke

For at være gyldigt skal et samtykke også være specifikt. Dette går hånd i hånd med kvaliteten af den information, der gives om genstanden for samtykke. 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.

Eksempel: I sagen *Deutsche Telekom AG*[103] behandlede EU-Domstolen spørgsmålet om, hvorvidt en telekommunikationsudbyder, der skulle videregive personoplysninger om abonnenter i medfør af artikel 12 i direktivet om databeskyttelse inden for elektronisk kommunikation[104], skulle indhente nyt samtykke fra de registrerede, da modtagerne ikke var nævnt, da samtykket blev givet.

EU-Domstolen fastslog, at nyt samtykke inden videregivelse af personoplysninger ikke var påkrævet i henhold til den nævnte artikel, fordi de registrerede i henhold til denne bestemmelse havde mulighed for kun at give samtykke til formålet med behandlingen, dvs. offentliggørelsen af deres oplysninger, og ikke kunne vælge mellem forskellige fortegnelser, hvori disse oplysninger eventuelt ville blive offentliggjort.

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"[105]. Det bemærkes, at "det er selve offentliggørelsen af personoplysninger i en nummerfortegnelse med et særligt formål, der kan være til ugunst for en abonnent"[106], og ikke den, der udarbejder denne fortegnelse.

103 EU-Domstolen, C-543/09, *Deutsche Telekom AG mod Tyskland*, 5. maj 2011, især præmis 53 og 54.

104 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 2002 L 201.

105 EU-Domstolen, C-543/09, *Deutsche Telekom AG mod Tyskland*, 5. maj 2011, især præmis 61.

106 *Ibid.*, især præmis 62.

2.4.2. Retten til at trække sit samtykke tilbage til enhver tid

Databeskyttelsesdirektivet nævner ikke en generel ret til at trække sit samtykke tilbage til enhver tid. Det antages dog generelt, at en sådan ret eksisterer, og at den registrerede frit skal kunne udøve den. Der bør ikke være krav om begrundelse for tilbagetrækningen, og der bør ikke være nogen risiko for negative følger ud over ophøret af eventuelle fordele, den registrerede måtte have opnået i forbindelse med den tidligere accepterede anvendelse af oplysninger.

Eksempel: En kunde accepterer at modtage reklamepost på en adresse, som han eller hun oplyser en registeransvarlig. Hvis kunden trækker sit samtykke tilbage, skal den registeransvarlige straks holde op med at sende reklamepost. Det må ikke medføre negative følger for kunden, som f.eks. gebyrer.

Hvis kunden modtog en rabat på 5 % på et hotelophold til gengæld for at acceptere, at vedkommendes oplysninger blev anvendt til reklamepost, bør tilbagetrækningen af samtykket til modtagelsen af reklamepost ikke betyde, at vedkommende senere skal tilbagebetale denne rabat.

3

De centrale principper i den europæiske lovgivning om databeskyttelse

EU	Omhandlede emner	Europarådet
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra a) og b) EU-Domstolen, C-524/06, *Huber mod Tyskland*, 16. december 2008 EU-Domstolen, forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen*, 9. november 2010	**Princippet om lovlig behandling**	Konvention 108, artikel 5, litra a) og b) Menneskerettighedsdomstolen, *Rotaru mod Rumænien* [GC], nr. 28341/95, 4. maj 2000 Menneskerettighedsdomstolen, *Taylor-Sabori mod Det Forenede Kongerige*, nr. 47114/99, 22. oktober 2002 Menneskerettighedsdomstolen, *Peck mod Det Forenede Kongerige*, nr. 44647/98, 28. januar 2003 Menneskerettighedsdomstolen, *Khelili mod Schweiz*, nr. 16188/07, 18. oktober 2011 Menneskerettighedsdomstolen, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra b)	**Princippet om formålsbestemthed**	Konvention 108, artikel 5, litra b)

EU	Omhandlede emner	Europarådet
	Principperne om datakvalitet	
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra c)	Proportionalitets-princippet	Konvention 108, artikel 5, litra c)
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra d)	Oplysningernes rigtighed	Konvention 108, artikel 5, litra d)
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra e)	Begrænset lagring af data	Konvention 108, artikel 5, litra e)
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra e)	Undtagelse for behandling i statistisk eller videnskabeligt øjemed	Konvention 108, artikel 9, stk. 3
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra a)	Princippet om rimelig behandling	Konvention 108, artikel 5, litra a) Menneskerettighedsdomstolen, *Haralambie mod Rumænien*, nr. 21737/03, 27. oktober 2009 Menneskerettighedsdomstolen, *K.H. m.fl. mod Slovakiet*, nr. 32881/04, 28. april 2009
Databeskyttelsesdirektivet, artikel 6, stk. 2	Princippet om ansvarlighed	

Principperne i artikel 5 i konvention 108 afspejler essensen af den europæiske databeskyttelseslovgivning. De fremgår også af databeskyttelsesdirektivets artikel 6, som er udgangspunktet for mere detaljerede bestemmelser i direktivets efterfølgende artikler. Alle senere bestemmelser om databeskyttelse, der vedtages af Europarådet eller på EU-plan, skal overholde disse principper, og de skal være udgangspunktet for enhver fortolkning af sådanne bestemmelser. Alle undtagelser fra og begrænsninger af disse centrale principper skal fastlægges på nationalt plan[107]. De skal være fastlagt ved lov, forfølge et legitimt formål og være nødvendige i et demokratisk samfund. Alle tre betingelser skal være opfyldt.

107 Konvention 108, artikel 9, stk. 2, og databeskyttelsesdirektivet, artikel 13.

3.1. Princippet om lovlig behandling

Hovedpunkter

- For at forstå princippet om lovlig behandling skal man tage udgangspunkt i betingelserne for lovlige begrænsninger af retten til databeskyttelse i lyset af chartrets artikel 52, stk. 1, og kravene til begrundede indgreb i artikel 8, stk. 2, i den europæiske menneskerettighedskonvention.
- Behandling af personoplysninger er kun lovlig, hvis den:
  - er i overensstemmelse med loven
  - forfølger et legitimt formål
  - er nødvendig i et demokratisk samfund for at opfylde det legitime formål.

I EU-retten og Europarådets konventioner om databeskyttelse er princippet om lovlig behandling det første princip, der nævnes. Det udtrykkes på næsten samme måde i artikel 5 i konvention 108 og i databeskyttelsesdirektivets artikel 6.

Ingen af disse bestemmelser definerer, hvad "lovlig behandling" er. For at forstå dette juridiske udtryk skal der henvises til begrundede indgreb i henhold til den europæiske menneskerettighedskonvention som fortolket i Menneskerettighedsdomstolens retspraksis og betingelserne for lovlige begrænsninger i chartrets artikel 52.

3.1.1. Kravene til begrundede indgreb i henhold til EMK

Behandlingen af personoplysninger kan udgøre et indgreb i den registreredes ret til respekt for privatlivet. Retten til respekt for privatlivet er dog ikke en absolut ret, men skal afvejes i forhold til og forenes med andre legitime interesser, uanset om det drejer sig om andre personers interesser (private interesser) eller samfundsmæssige interesser.

Statslige indgreb er begrundede på følgende betingelser:

I overensstemmelse med loven

I henhold til Menneskerettighedsdomstolens 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[108]. En regel betragtes som forudsigelig, hvis den er formuleret tilstrækkelig præcist til, at enhver person – om nødvendigt med passende rådgivning – kan regulere sin adfærd[109]. Kravene til retsgrundlagets klarhed afhænger i denne forbindelse af den konkrete sag[110].

Eksempel: I sagen *Rotaru mod Rumænien*[111] fastslog Menneskerettighedsdomstolen, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt, fordi rumænsk lovgivning tillod indsamling, registrering og arkivering af oplysninger, der havde betydning for den nationale sikkerhed, i hemmelige arkiver uden at fastlægge 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 overvågning, de omstændigheder, hvorunder sådanne foranstaltninger kunne træffes, eller den procedure, der skulle følges. Som følge af disse mangler konkluderede Menneskerettighedsdomstolen, at den rumænske lovgivning ikke opfyldte kravene om forudsigelighed i artikel 8 i EMK, og at den pågældende artikel var blevet overtrådt.

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

109 Menneskerettighedsdomstolen, *Amann mod Schweiz* [GC], nr. 27798/95, 16. februar 2000, præmis 56. Se også Menneskerettighedsdomstolen, *Malone mod Det Forenede Kongerige*, nr. 8691/79, 2. august 1984, præmis 66, Menneskerettighedsdomstolen, *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.

110 Menneskerettighedsdomstolen, *The Sunday Times mod Det Forenede Kongerige*, nr. 6538/74, 26. april 1979, præmis 49. Se også Menneskerettighedsdomstolen, *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.

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

Eksempel: I sagen *Taylor-Sabori mod Det Forenede Kongerige*[112] 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". Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Forfølgelse af et legitimt mål

Det legitime mål kan være en af de nævnte samfundsinteresser eller andres rettigheder og friheder.

Eksempel: I sagen *Peck mod Det Forenede Kongerige*[113] 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. Menneskerettighedsdomstolen 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 derfor, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Nødvendig i et demokratisk samfund

Menneskerettighedsdomstolen 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[114].

112 Menneskerettighedsdomstolen, *Taylor-Sabori mod Det Forenede Kongerige*, nr. 47114/99, 22. oktober 2002.

113 Menneskerettighedsdomstolen, *Peck mod Det Forenede Kongerige*, nr. 44647/98, 28. januar 2003, især præmis 85.

114 Menneskerettighedsdomstolen, *Leander mod Sverige*, nr. 9248/81, 11. juli 1985, præmis 58.

Eksempel: I sagen *Khelili mod Schweiz*[115] 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. Menneskerettighedsdomstolen 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 EMK. Domstolen fandt, at det var myndighedernes opgave at bevise rigtigheden af de oplysninger, der 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 den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Eksempel: I sagen *Leander mod Sverige*[116] fastslog Menneskerettighedsdomstolen, at sikkerhedsundersøgelse 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 Menneskerettighedsdomstolens konkluderede, at det svenske system til kontrol af medarbejdere opfyldte kravene i artikel 8, stk. 2, i den europæiske menneskerettighedskonvention. På grundlag af de brede muligheder for skøn, 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 den europæiske menneskerettighedskonventions artikel 8 ikke var blevet overtrådt.

115 Menneskerettighedsdomstolen, *Khelili mod Schweiz*, nr. 16188/07, 18. oktober 2011.

116 Menneskerettighedsdomstolen, *Leander mod Sverige*, nr. 9248/81, 11. juli 1985, præmis 59 og 67.

3.1.2. Betingelserne for lovlige begrænsninger i henhold til EU-chartret

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

I henhold til chartrets artikel 52, stk. 1, kan der kun indføres begrænsninger for udøvelsen af de rettigheder og friheder, der anerkendes ved chartret, og dermed for udøvelsen af retten til beskyttelse af personoplysninger, som f.eks. behandling af personoplysninger, såfremt disse:

- er fastlagt i lovgivningen
- respekterer disse rettigheders og friheders væsentligste indhold
- er nødvendige under iagttagelse af proportionalitetsprincippet
- faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

Eksempler: I *Volker und Markus Schecke GbR* [117] 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 de har modtaget disse midler, hyppigheden af en sådan modtagelse eller midlernes art og omfang, havde overskredet de grænser, som en overholdelse af proportionalitetsprincippet opstiller.

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

EU-Domstolen fandt det derfor nødvendigt at erklære visse bestemmelser i Rådets forordning (EF) nr. 1290/2005 for ugyldige og erklære forordning (EF) nr. 259/2008 for ugyldig i sin helhed[118].

Trods forskellige formuleringer svarer betingelserne for lovlig behandling i chartrets artikel 52, stk. 1, til artikel 8, stk. 2, i EMK. De betingelser, der opstilles i chartrets artikel 52, stk. 1, skal faktisk ses som værende i overensstemmelse med betingelserne i artikel 8, stk. 2, i EMK, idet det i chartrets artikel 52, stk. 3, i første punktum anføres, 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".

I sidste punktum i artikel 52, stk. 3, hedder det dog, at "[d]enne bestemmelse er ikke til hinder for, at EU-retten kan yde en mere omfattende beskyttelse". Når artikel 8, stk. 2, i EMK sammenlignes med chartrets artikel 52, stk. 3, første punktum, kan det kun betyde, at betingelserne for begrundede indgreb i medfør af artikel 8, stk. 2, i EMK er minimumskrav, for så vidt angår lovlige begrænsninger af retten til databeskyttelse i henhold til chartret. Som følge deraf kræver lovlig behandling af personoplysninger i henhold til EU-retten, at betingelserne i artikel 8, stk. 2, i EMK som minimum er opfyldt. Der kan dog fastlægges yderligere krav i særlige tilfælde i EU-retten.

Overensstemmelse mellem princippet om lovlig behandling i henhold til EU-retten og de relevante bestemmelser i den europæiske menneskerettighedskonvention fremmes yderligere af artikel 6, stk. 3, i TEU, som fastlægger, at de "grundlæggende rettigheder, som de er garanteret ved den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder [...] udgør generelle principper i EU-retten".

118 Rådets forordning (EF) nr. 1290/2005 af 21. juni 2005 om finansiering af den fælles landbrugspolitik, EUT 2005 L 209, og 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 2008 L 76.

3.2. Princippet om formålsbestemthed

Hovedpunkter

- Formålet med behandling af personoplysninger skal være fastlagt, inden behandlingen påbegyndes.
- I henhold til EU-retten skal formålet med behandlingen være udtrykkeligt angivet. I henhold til Europarådets retsorden overlades dette spørgsmål til den nationale lovgivning.
- Behandling til udefinerede formål er ikke i overensstemmelse med databeskyttelseslovgivningen.
- Yderligere anvendelse af oplysninger til et andet formål kræver et yderligere retsgrundlag, hvis det nye formål med behandling er uforeneligt med det oprindelige.
- Videregivelse af oplysninger til tredjemand er et nyt formål, der kræver et yderligere retsgrundlag.

Princippet om formålsbestemthed indebærer kort sagt, at lovligheden af behandlingen af personoplysninger afhænger af formålet med behandlingen[119]. Formålet skal være udtrykkeligt angivet af den registeransvarlige, inden behandlingen af personoplysninger påbegyndes[120]. **I henhold til EU-retten** skal dette ske ved en erklæring, dvs. ved anmeldelse, til den relevante tilsynsmyndighed eller som minimum ved, at den registeransvarlige gør sig det klart, hvad formålet med indsamlingen af oplysninger er.

Behandling af personoplysninger til udefinerede og/eller ubegrænsede formål er ulovlig.

Ethvert nyt formål med behandling af personoplysninger skal have et særskilt retsgrundlag og kan ikke baseres på, at oplysningerne oprindeligt blev indhentet eller behandlet til et andet legitimt formål. Legitim behandling er til gengæld begrænset til det oprindeligt angivne formål, og ethvert nyt formål med behandling kræver et særskilt nyt retsgrundlag. Videregivelse af oplysninger til tredjemand skal overvejes særligt nøje, da videregivelse normalt udgør et nyt formål og derfor kræver et retsgrundlag, som er adskilt fra formålet med indsamlingen af oplysninger.

119 Konvention 108, artikel 5, litra b), og databeskyttelsesdirektivet, artikel 6, stk. 1, litra b).

120 Se også Artikel 29-Gruppen (2013), udtalelse 03/2013 om begrænsning af formål, WP 203, Bruxelles, den 2. april 2013.

Eksempel: Et flyselskab indsamler oplysninger fra passagererne ved booking for at kunne operere flyvningen. Flyselskabet indsamler 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 end det oprindelige formål 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 konvention 108 og databeskyttelsesdirektivet begrebet forenelighed: Det er tilladt at anvende oplysninger til forenelige formål på grundlag af det oprindelige retsgrundlag. Det defineres dog ikke, hvad "forenelig" betyder, og begrebet overlades til fortolkning fra sag til sag.

Eksempel: Salg af virksomheden Sunshines kundedata, som den indsamlede i forbindelse med kundeplejeaktiviteter (CRM), til en markedsføringsvirksomhed, Moonlight, som ønsker at bruge disse data i andre virksomheders markedsføringskampagner, er et nyt formål, som er uforeneligt med CRM, der var virksomheden Sunshines oprindelige formål med indsamlingen af kundedata. Salget 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.

Databeskyttelsesdirektivet fastlægger udtrykkeligt, at "senere behandling af oplysninger i historisk, statistisk eller videnskabeligt øjemed anses ikke for at være uforenelig med disse formål, såfremt medlemsstaterne giver de fornødne garantier"[121].

Eksempler: Virksomheden Sunshine har indsamlet og lagret CRM-oplysninger om sine kunder. Senere brug af disse oplysninger i en statistisk analyse af

121 Et eksempel på sådanne nationale garantier er den østrigske databeskyttelseslov (*Datenschutzgesetz*), Østrigs lovtidende I nr. 165/1999, præmis 46, findes på engelsk på: www.dsk.gv.at/DocView.axd?CobId=41936.

kundernes indkøbsmønstre vil normalt kunne tillades, da statistiske analyser er et foreneligt formål.

Hvis de samme oplysninger blev videregivet til tredjemand, virksomheden Starlight, alene til statistiske formål, ville videregivelsen være tilladt, men kun såfremt der gives de fornødne garantier, f.eks. tilsløring af de registreredes identitet, idet identiteter normalt ikke er nødvendige til statistiske formål.

3.3. Principperne om datakvalitet

Hovedpunkter

- Principperne om datakvalitet skal overholdes af den registeransvarlige ved enhver behandling.
- Princippet om begrænset opbevaring af oplysninger kræver, at oplysninger slettes, så snart de ikke længere er nødvendige til det formål, de blev indsamlet til.
- Undtagelser fra princippet om begrænset opbevaring skal være fastlagt ved lov og kræver særlige garantier for beskyttelsen af de registrerede.

3.3.1. Proportionalitetsprincippet

Oplysninger, som skal behandles, skal være "tilstrækkelige og relevante og må ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og de formål, hvortil de senere behandles"[122]. De kategorier af oplysninger, der udvælges til behandling, skal være nødvendige for at opfylde det erklærede overordnede formål med behandlingen, og en registeransvarlig bør strengt begrænse indsamlingen af oplysninger til sådanne data, der er direkte relevante for det særlige formål med behandlingen.

I dag gør endnu et aspekt af proportionalitetsprincippet sig gældende: Ved hjælp af teknologier til beskyttelse af privatlivet kan anvendelsen af personoplysninger i nogle tilfælde helt undgås, eller der kan anvendes pseudonymiserede oplysninger, som sikrer en løsning, der tager hensyn til privatlivets fred. Dette er især hensigtsmæssigt i mere omfattende behandlingssystemer.

122 Konvention 108, artikel 5, litra c), og databeskyttelsesdirektivet, artikel 6, stk. 1, litra c).

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 proportionalitetsprincippet 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 transportsystemet på hvilket tidspunkt. Der ville ikke blive indsamlet personoplysninger, og det er den optimale løsning med hensyn til proportionalitetsprincippet, da dette princip medfører en forpligtelse til at minimere indsamlingen af personoplysninger.

3.3.2. Princippet om oplysningernes rigtighed

En registeransvarlig, der besidder personoplysninger, må ikke anvende disse oplysninger uden at træffe de nødvendige foranstaltninger for med rimelig sikkerhed at sikre, at oplysningerne er korrekte og ajourførte.

Forpligtelsen til at sikre oplysningernes rigtighed skal ses i sammenhæng med formålet med databehandlingen.

Eksempel: En møbelsælger har indsamlet oplysninger om kundernes identitet og adresser med henblik på fakturering. Seks måneder senere ønsker den samme virksomhed at indlede en markedsføringskampagne og ønsker at kontakte tidligere kunder. I den forbindelse ønsker virksomheden adgang til det nationale folkeregister, som sandsynligvis indeholder ajourførte adresseoplysninger, idet borgerne har pligt til at oplyse deres nuværende adresse til folkeregistret. Kun personer og enheder, der kan give en gyldig grund, har adgang til oplysningerne i dette register.

I denne situation kan virksomheden ikke bruge det argument, at oplysningerne skal være rigtige og om nødvendigt ajourførte, som begrundelse for, at den har ret til at indsamle nye adresseoplysninger om alle dens tidligere kunder fra folkeregistret. Oplysningerne blev indsamlet med henblik på fakturering. Til det formål er adressen på salgstidspunktet relevant. Der er intet retsgrundlag for at indsamle nye adresseoplysninger, da markedsføring ikke er en interesse, der tilsidesætter retten til databeskyttelse, og som derfor kan begrunde anvendelsen af registrets data.

Der kan også være tilfælde, hvor ajourføring af lagrede data ikke er tilladt, fordi lagringen af data primært har til formål at dokumentere begivenheder.

Eksempel: En medicinsk protokol må ikke ændres, dvs. "ajourføres", selv om de resultater, der nævnes i protokollen, senere viser sig at være forkerte. Under sådanne omstændigheder kan der kun indsættes tilføjelser til bemærkningerne i protokollen, hvis det tydeligt markeres, at de er tilføjet senere.

Der er på den anden side situationer, hvor regelmæssig kontrol af oplysningernes rigtighed, herunder ajourføring, er absolut nødvendig på grund af de potentielle problemer, der kan opstå for den registrerede, hvis oplysningerne ikke er rigtige.

Eksempel: Hvis en person ønsker at indgå en kontrakt med en bank, vil banken normalt kontrollere den potentielle kundes kreditværdighed. Til det formål findes der en række særlige databaser, som indeholder oplysninger om privatpersoners kreditvurdering. Hvis en sådan database indeholder ukorrekte eller forældede oplysninger om en person, kan denne person få alvorlige problemer. Registeransvarlige for sådanne databaser skal derfor yde en særlig indsats for at overholde princippet om rigtighed.

Oplysninger, der ikke vedrører fakta, men mistanker, f.eks. strafferetlig efterforskning, kan indsamles og lagres, hvis den registeransvarlige har retsgrundlag for at indsamle sådanne oplysninger, og mistanken er tilstrækkeligt begrundet.

3.3.3. Princippet om begrænset opbevaring af oplysninger

I henhold til databeskyttelsesdirektivets artikel 6, stk. 1, litra e), og artikel 5, litra e), i konvention 108 skal medlemsstaterne sikre, at personoplysninger "ikke må opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt". Oplysningerne skal derfor slettes, når disse formål er opfyldt.

I *S. og Marper* konkluderede Menneskerettighedsdomstolen, at de centrale principper i Europarådets relevante instrumenter og de andre kontraherende parters lov og praksis kræver, at opbevaringen af oplysninger står i forhold til formålet med indsamlingen og er tidsmæssigt begrænset, især på politiområdet[123].

Tidsbegrænsningen for lagring af personoplysninger gælder dog kun for oplysninger, der lagres i en form, der gør det muligt at identificere de registrerede. Lovlig lagring af oplysninger, som ikke længere er nødvendige, kan derfor ske ved at anonymisere eller pseudonymisere oplysningerne.

Opbevaring af oplysninger i historisk, statistisk eller videnskabeligt øjemed er udtrykkeligt undtaget fra princippet om begrænset opbevaring af oplysninger i henhold til databeskyttelsesdirektivet[124]. En sådan fortsat lagring og anvendelse af personoplysninger skal dog være ledsaget af særlige garantier, der er fastlagt i den nationale lovgivning.

3.4. Princippet om rimelig behandling

Hovedpunkter

- Rimelig behandling betyder, at behandlingen skal være gennemsigtig, især over for de registrerede.

123 Menneskerettighedsdomstolen, *S. og Marper mod Det Forenede Kongerige*, nr. 30562/04 og 30566/04, 4. december 2008. Se også f.eks. Menneskerettighedsdomstolen, *M.M. mod Det Forenede Kongerige*, nr. 24029/07, 13. november 2012.

124 Databeskyttelsesdirektivet, artikel 6, stk. 1, litra e).

- De registrerede skal kunne få kendskab til en behandlings eksistens og, når der indsamles oplysninger hos dem, få nøjagtige og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen.
- Medmindre det specifikt er tilladt ifølge loven, må der ikke ske hemmelig og skjult behandling af personoplysninger.
- De registrerede har ret til at få adgang til deres personoplysninger, uanset hvor de behandles.

Princippet om rimelig behandling vedrører primært forholdet mellem den registeransvarlige og den registrerede.

3.4.1. Gennemsigtighed

Dette princip pålægger den registeransvarlige en forpligtelse til at underrette de registrerede om, hvordan deres oplysninger anvendes.

Eksempel: I sagen *Haralambie mod Rumænien*[125] anmodede sagsøgeren om adgang til den sagsakt, som det hemmelige politi havde lagret om ham, men hans anmodning blev først imødekommet fem år senere. Menneskerettighedsdomstolen 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 procedure for aktindsigt i sådanne oplysninger. Menneskerettighedsdomstolen 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 den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Behandlingen skal forklares for de registrerede på en lettilgængelig måde, som sikrer, at de forstår, hvad der sker med deres oplysninger. En registreret har også ret til efter anmodning at blive underrettet af den registeransvarlige, hvis vedkommendes oplysninger behandles, og i så fald hvilke oplysninger det drejer sig om.

125 Menneskerettighedsdomstolen, *Haralambie mod Rumænien*, nr. 21737/03, 27. oktober 2009.

3.4.2. Opbygning af tillid

Registeransvarlige skal over for registrerede og offentligheden kunne dokumentere, at de vil behandle oplysninger på en lovlig og gennemsigtig måde. Behandling må ikke foretages i hemmelighed og må ikke have uforudsigelige negative følger. Registeransvarlige bør sikre, at kunder, klienter eller borgere oplyses om anvendelsen af deres oplysninger. Registeransvarlige skal endvidere så vidt muligt handle således, at de omgående imødekommer den registreredes ønsker, især hvis vedkommendes samtykke udgør retsgrundlaget for databehandlingen.

Eksempel: I sagen *K.H. m.fl. mod Slovakiet*[126] var sagsøgerne otte 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 deres patientjournaler, 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 EMK 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. Menneskerettighedsdomstolen 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 sagsøgeren effektiv aktindsigt i oplysninger vedrørende deres helbred. Domstolen konkluderede, at den europæiske menneskerettighedskonventions 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.

126 Menneskerettighedsdomstolen, *K.H. m.fl. mod Slovakiet*, nr. 32881/04, 6. november 2009.

Rimelig behandling betyder også, at registeransvarlige skal være parate til over for den registrerede at gå videre end de obligatoriske minimumskrav til tjenesten, hvis den registreredes legitime interesser kræver det.

3.5. Princippet om ansvarlighed

Hovedpunkter

- Ansvarlighed kræver, at registeransvarlige aktivt gennemfører foranstaltninger for at fremme og garantere databeskyttelse som led i deres databehandling.
- Registeransvarlige er ansvarlige for, at deres behandling er i overensstemmelse med databeskyttelseslovgivningen.
- Registeransvarlige skal til enhver tid over for de registrerede, offentligheden og tilsynsmyndighederne kunne påvise, at de overholder databeskyttelsesreglerne.

OECD (Organisationen for Økonomisk Samarbejde og Udvikling) vedtog i 2013 retningslinjer for beskyttelse af privatlivets fred, hvori man fremhævede, at registeransvarlige har et stort ansvar for at få databeskyttelse til at fungere i praksis. I retningslinjerne opstilles der et ansvarlighedsprincip, som fastlægger, at en registeransvarlig er ansvarlig for at overholde foranstaltninger, som gennemfører de væsentlige principper, der er nævnt i retningslinjerne[127].

Mens konvention 108 ikke omhandler de registeransvarliges ansvarlighed og grundlæggende overlader dette spørgsmål til den nationale lovgivning, fastlægger databeskyttelsesdirektivets artikel 6, stk. 2, at det "påhviler den registeransvarlige at sikre, at bestemmelserne i stk. 1 overholdes".

Eksempel: Et eksempel på lovgivning, som understreger princippet om ansvarlighed, er ændringen[128] af direktiv 2002/58/EF (direktivet om privatlivets fred)

127 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, artikel 14.

128 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, Direktivet 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 2009 L 337, s. 11.

fra 2009. I henhold til artikel 4 som ændret pålægges registeransvarlige en forpligtelse til at gennemføre en sikkerhedspolitik, dvs. 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[129] er essensen af ansvarlighed den registeransvarliges forpligtelse til:

- at gennemføre foranstaltninger, der – under normale omstændigheder – garanterer, at databeskyttelsesreglerne overholdes i forbindelse med behandling

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

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

129 Artikel 29-Gruppen, udtalelse 3/2010 om princippet om ansvarlighed, WP 173, Bruxelles, den 13. juli 2010.

4

Reglerne i den europæiske lovgivning om databeskyttelse

EU	Omhandlede emner	Europarådet
Regler om lovlig behandling af ikke-følsomme oplysninger		
Databeskyttelsesdirektivet, artikel 7, litra a)	Samtykke	Henstilling om profilering, artikel 3, stk. 4, litra b), og artikel 3, stk. 6
Databeskyttelsesdirektivet, artikel 7, litra b)	(Præ-)kontraktligt forhold	Henstilling om profilering, artikel 3, stk. 4, litra b)
Databeskyttelsesdirektivet, artikel 7, litra c)	Den registeransvarliges retlige forpligtelser	Henstilling om profilering, artikel 3, stk. 4, litra a)
Databeskyttelsesdirektivet, artikel 7, litra d)	Den registreredes vitale interesser	Henstilling om profilering, artikel 3, stk. 4, litra b)
Databeskyttelsesdirektivet, artikel 7, litra e), og artikel 8, stk. 4 EU-Domstolen, C-524/06, *Huber mod Tyskland*, 16. december 2008	Samfundsinteresser og offentlig myndighedsudøvelse	Henstilling om profilering, artikel 3, stk. 4, litra b)
Databeskyttelsesdirektivet, artikel 7, litra f), artikel 8, stk. 2 og 3 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	Andres legitime interesser	Henstilling om profilering, artikel 3, stk. 4, litra b)

EU	Omhandlede emner	Europarådet
Regler om lovlig behandling af følsomme oplysninger		
Databeskyttelsesdirektivet, artikel 8, stk. 1	Generelt forbud mod behandling	Konvention 108, artikel 6
Databeskyttelsesdirektivet, artikel 8, stk. 2, 3 og 4	Undtagelser fra det generelle forbud	Konvention 108, artikel 6
Databeskyttelsesdirektivet, artikel 8, stk. 5	Behandling af oplysninger om (straffe)domme	Konvention 108, artikel 6
Databeskyttelsesdirektivet, artikel 8, stk. 7	Behandling af identifikationsnumre	
Regler om behandlingssikkerhed		
Databeskyttelsesdirektivet, artikel 17	Forpligtelse til at fastsætte bestemmelser om sikker behandling	Konvention 108, artikel 7 Menneskerettighedsdomstolen, *I. mod Finland*, nr. 20511/03, 17. juli 2008
Direktivet om privatlivets fred, artikel 4, stk. 2	Anmeldelse af brud på datasikkerheden	
Databeskyttelsesdirektivet, artikel 16	Tavshedspligt	
Regler om gennemsigtighed ved behandling		
	Gennemsigtighed generelt	Konvention 108, artikel 8, litra a)
Databeskyttelsesdirektivet, artikel 10 og 11	Oplysningspligt	Konvention 108, artikel 8, litra a)
Databeskyttelsesdirektivet, artikel 10 og 11	Undtagelser fra oplysningspligten	Konvention 108, artikel 9
Databeskyttelsesdirektivet, artikel 18 og 19	Anmeldelse	Henstilling om profilering, artikel 9, stk. 2, litra a)
Regler om fremme af overensstemmelse		
Databeskyttelsesdirektivet, artikel 20	Forudgående kontrol	
Databeskyttelsesdirektivet, artikel 18, stk. 2	Personer med ansvar for beskyttelse af personoplysninger	Henstilling om profilering, artikel 8, stk. 3
Databeskyttelsesdirektivet, artikel 27	Adfærdskodekser	

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 konvention 108 at præcisere mulighederne 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. I overensstemmelse med principperne i dets artikel 6 fastlægger databeskyttelsesdirektivet et lag af detaljerede regler, som skal gennemføres nøje i national ret. Følgende bemærkninger vedrørende de detaljerede databeskyttelsesregler på europæisk plan vedrører derfor primært EU-retten.

4.1. Regler om lovlig behandling

Hovedpunkter

- Behandling af personoplysninger er lovlig, hvis:
  - behandlingen er baseret på den registreredes samtykke, eller
  - de registreredes vitale interesser kræver, at deres oplysninger behandles, eller
  - andres legitime interesser er grundlaget for behandlingen, men kun for så vidt de ikke tilsidesættes af andre interesser i at beskytte de registreredes grundlæggende rettigheder.
- Lovlig behandling af følsomme personoplysninger er underlagt særlige og strengere regler.

Databeskyttelsesdirektivet indeholder to forskellige regelsæt for lovlig behandling af oplysninger: et sæt for ikke-følsomme oplysninger i artikel 7 og et sæt for følsomme oplysninger i artikel 8.

4.1.1. Lovlig behandling af ikke-følsomme oplysninger

I henhold til direktiv 95/46, afdeling II ("Principper vedrørende grundlaget for behandling af oplysninger"), skal enhver behandling af personoplysninger, med forbehold af de undtagelser, der er fastsat ved artikel 13, først overholde de principper vedrørende datakvalitet, der er nævnt i direktivets artikel 6, og dernæst

et af de kriterier for at legitimere databehandling, der er nævnt i direktivets artikel 7[130]. Her forklares de tilfælde, der legitimerer behandling af ikke-følsomme personoplysninger.

Samtykke

I Europarådets retsorden nævnes samtykke ikke i hverken den europæiske menneskerettighedskonventions artikel 8 eller konvention 108. Det nævnes dog i Menneskerettighedsdomstolens retspraksis og flere henstillinger fra Europarådet. **I EU-retten** er samtykke som grundlag for legitim databeskyttelse klart fastlagt ved databeskyttelsesdirektivets artikel 7, litra a), og det nævnes også udtrykkeligt i chartrets artikel 8.

Kontraktligt forhold

Et andet grundlag for legitim behandling af personoplysninger **i EU-retten**, som nævnes i databeskyttelsesdirektivets artikel 7, litra b), er, om "behandlingen er nødvendig af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i". Denne bestemmelse omfatter også prækontraktlige forhold. En part ønsker f.eks. at indgå en kontrakt, men har endnu ikke gjort det, fordi der stadig er nogle kontroller, som skal foretages. Hvis en part skal behandle oplysninger til et sådant formål, er denne behandling legitim, såfremt den er "af hensyn til gennemførelse af foranstaltninger, der træffes på dennes anmodning forud for indgåelsen af en sådan kontrakt".

For så vidt angår **Europarådets retsorden**, nævnes beskyttelsen af andres rettigheder og friheder i artikel 8, stk. 2, i EMK som begrundelse for legitim begrænsning af retten til databeskyttelse.

Den registeransvarliges retlige forpligtelser

I **EU-retten** nævnes derefter udtrykkeligt et andet kriterium for legitimering af databehandling, nemlig hvis "behandlingen er nødvendig for at overholde en retlig forpligtelse, som gælder for den registeransvarlige" (databeskyttelsesdirektivets

130 EU-Domstolen, forenede sager C-465/00, C-138/01 og C-139/01, *Österreichischer Rundfunk m.fl.*, 20. maj 2003, præmis 65, EU-Domstolen, C-524/06, *Huber mod Tyskland*, 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.

artikel 7, litra c)). Denne bestemmelse omhandler registeransvarlige inden for den private sektor. De retlige forpligtelser for en registeransvarlig i den offentlige sektor er omfattet af direktivets artikel 7, litra e). Der er mange tilfælde, hvor registeransvarlige i den private sektor er retligt forpligtede til at behandle oplysninger om andre. Læger og hospitaler har f.eks. retlig pligt til at lagre oplysninger om behandlingen af patienter i flere år, arbejdsgivere skal behandle oplysninger om deres medarbejdere med henblik på betaling af arbejdsmarkedsbidrag og skat, og virksomheder skal behandle oplysninger om deres kunder af skattemæssige årsager.

I forbindelse med flyselskabernes obligatoriske videregivelse af passageroplysninger til udenlandske immigrationsmyndigheder opstod der tvivl om, hvorvidt retlige forpligtelser i henhold til *udenlandsk* ret kunne udgøre et legitimt grundlag for at behandle oplysninger i medfør af EU-retten (dette spørgsmål er omhandlet i detaljer i afsnit 6.2).

Den registeransvarliges retlige forpligtelser udgør også et grundlag for legitim databehandling i henhold til **Europarådets retsorden.** Som det tidligere er påpeget, er de retlige forpligtelser for en registeransvarlig i den private sektor kun ét specifikt eksempel på andres legitime interesser, som nævnt i artikel 8, stk. 2, i EMK. Ovennævnte eksempel er derfor også relevant for Europarådets konventioner.

Den registreredes vitale interesser

I EU-retten fastsætter databeskyttelsesdirektivet i artikel 7, litra d), at behandling af personoplysninger er lovlig, hvis den "er nødvendig for at beskytte den registreredes vitale interesser". Sådanne interesser, som er tæt forbundet med den registreredes overlevelse, kan derfor være grundlaget for legitim behandling af f.eks. helbredsoplysninger eller oplysninger om savnede personer.

I Europarådets retsorden nævnes den registreredes vitale interesser ikke i artikel 8 i EMK som begrundelse for legitim begrænsning af retten til databeskyttelse. I nogle af Europarådets henstillinger, som supplerer konvention 108 på bestemte områder, nævnes den registreredes vitale interesser dog udtrykkeligt som grundlag for legitim behandling af oplysninger[131]. Den registreredes vitale interesser er tydeligvis underforstået i sættet af begrundelser for behandling af personoplysninger: Beskyttelsen af grundlæggende rettigheder må aldrig bringe den beskyttede persons vitale interesser i fare.

131 Henstilling om profilering, artikel 3, stk. 4, litra b).

Samfundsinteresser og offentlig myndighedsudøvelse

Som følge af de mange mulige måder at tilrettelægge offentlige anliggender på fastlægges det i databeskyttelsesdirektivets artikel 7, litra e), at behandling af personoplysninger er lovlig, hvis den "er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den registeransvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt"[132].

Eksempel: I sagen *Huber mod Tyskland*[133] 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 Ausländerzentralregister (det centrale udlændingeregister, AZR). Udlændingeregistret, som indeholder personoplysninger om ikketyske EU-statsborgere, som opholder sig i Tyskland i mere end tre måneder, anvendes til statistiske formål og til brug for sikkerheds-, politi- og justitsmyndighedernes efterforskning og retsforfølgelse af handlinger, der er strafbare, eller som bringer den offentlige sikkerhed i fare. Den forelæggende domstol spurgte, om behandlingen af personoplysninger i et register som AZR er forenelig med EU-retten, idet det bemærkes, at et sådant register ikke findes for tyske statsborgere.

EU-Domstolen fastslog først, at behandling af personoplysninger i henhold til direktivets artikel 7, litra e), kun er lovlig, hvis den er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse.

Domstolen udtalte navnlig: "I betragtning af hensynet til at sikre et ensartet beskyttelsesniveau i alle medlemsstater må nødvendighedsbegrebet i artikel 7, litra e), i direktiv 95/46 [...] 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"[134].

Domstolen bemærkede, at en unionsborgers ret til ophold i en medlemsstat, hvor han ikke er statsborger, ikke er ubetinget, idet den kan være undergivet de

132 Se også databeskyttelsesdirektivet, betragtning 32.

133 EU-Domstolen, C-524/06, *Huber mod Tyskland*, 16. december 2008.

134 *Ibid.*, præmis 52.

begrænsninger og betingelser, der er fastsat i traktaten og gennemførelsesbestemmelserne hertil. Hvis anvendelsen af et register som AZR til brug for 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 forvaltningen af denne lovgivning, og centraliseringen muliggør en mere effektiv forvaltning af denne lovgivning. Den nationale ret blev pålagt at efterprøve, at disse betingelser opfyldtes i den pågældende sag. Hvis ikke, kan opbevaring og behandling af navngivne personoplysninger inden for rammerne af et register som AZR til statistisk brug ikke anses for nødvendig i den forstand, hvori udtrykket er anvendt i artikel 7, litra e), i direktiv 95/46[135].

Endelig fastholdt Domstolen, for så vidt angår spørgsmålet om behandlingen af oplysninger i registret med henblik på kriminalitetsbekæmpelse, at dette mål nødvendigvis tilsigter retsforfølgning af strafbare handlinger 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. Denne bestemmelse er således "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 som fortolket af Domstolen"[136].

Offentlige myndigheders anvendelse af personoplysninger er også omfattet af artikel 8 i EMK.

Legitime interesser, der forfølges af den registeransvarlige eller en tredjemand

Den registrerede er ikke den eneste med legitime interesser. I henhold til databeskyttelsesdirektivets artikel 7, litra f), er behandling af personoplysninger lovlig, hvis den "er nødvendig, for at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse,

135 *Ibid.*, præmis 54, 58, 59 og 66-68.

136 *Ibid.*, præmis 78 og 81.

medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes [...], går forud herfor".

I følgende dom baserede EU-Domstolen udtrykkeligt sin dom på direktivets artikel 7, litra f):

Eksempel: I sagen *ASNEF og FECEMD*[137] præciserede EU-Domstolen, at nationale lovgivninger ikke kan fastsætte supplerende krav til dem, der er nævnt i databeskyttelsesdirektivets artikel 7, litra f). 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.

Domstolen bemærkede først, at direktiv 95/46 har til formål at gøre 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 højt beskyttelsesniveau inden for EU[138]. 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 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 eller fastsætte supplerende krav, som ændrer rækkevidden af et af de seks principper, der er fastsat i denne artikel"[139]. Hvad angår den nødvendige afvejning i henhold til artikel 7, litra f), i direktiv 95/46, erkendte 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".

137 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.

138 *Ibid.*, præmis 28. Se databeskyttelsesdirektivet, betragtning 8 og 10.

139 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 30 og 32.

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 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 er opført i offentligt tilgængelige kilder, og således kategorisk og generelt udelukker enhver behandling af oplysninger, som ikke er opført i sådanne kilder"[140].

Lignende formuleringer kan findes 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[141].

4.1.2. Lovlig behandling af følsomme oplysninger

Europarådets retsorden overlader det til de nationale lovgivninger at sikre hensigtsmæssig beskyttelse i forbindelse med behandlingen af følsomme data, mens **EU-retten** ved databeskyttelsesdirektivets artikel 8 fastlægger detaljerede regler for behandling af personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning og fagforeningsmæssigt tilhørsforhold samt om helbredsforhold eller seksuelle forhold. Behandling af følsomme oplysninger er principielt forbudt[142]. Der er dog opstillet en udtømmende liste over undtagelser til dette forbud, som findes i direktivets artikel 8, stk. 2 og 3. Disse undtagelser omfatter den registreredes udtrykkelige samtykke, den registreredes vitale interesser, andres legitime interesser og samfundsinteresser.

140 *Ibid.*, præmis 40, 44, 48 og 49.

141 Henstilling om profilering, artikel 3, stk. 4, litra b).

142 Databeskyttelsesdirektivet, artikel 8, stk. 1.

I modsætning til det, der er tilfældet for ikke-følsomme oplysninger, betragtes et kontraktligt forhold til den registrerede ikke som et generelt grundlag for legitim behandling af følsomme oplysninger. Hvis følsomme oplysninger skal behandles inden for rammerne af en kontrakt med den registrerede, kræver anvendelsen af sådanne oplysninger derfor registreredes særskilte udtrykkelige samtykke i tillæg til underskrivelsen af selve kontrakten. Den registreredes udtrykkelige anmodning om varer eller tjenester, som nødvendigvis vil afsløre følsomme oplysninger, bør dog anses for at være af samme betydning som et udtrykkeligt samtykke.

Eksempel: Hvis en flypassager i forbindelse med reservation af en flyvning kræver, at flyselskabet stiller en kørestol til rådighed, og bestiller koshermad, kan flyselskabet behandle disse oplysninger, selv om passageren ikke har underskrevet et ekstra samtykke, som viser, at han eller hun accepterer anvendelsen af oplysninger om sit helbred eller sin religiøse overbevisning.

Den registreredes udtrykkelige samtykke

Den første betingelse for lovlig behandling af oplysninger, uanset om de er ikke-følsomme eller følsomme oplysninger, er den registreredes samtykke. Hvis der er tale om følsomme oplysninger, skal samtykket være udtrykkeligt. Det kan dog fastsættes i den nationale lovgivning, at samtykke til anvendelsen af følsomme oplysninger ikke er et tilstrækkeligt grundlag til at tillade, at sådanne oplysninger behandles[143], f.eks. hvis behandling i særlige tilfælde indebærer usædvanlige risici for den registrerede.

I et særligt tilfælde anerkendes endda underforstået samtykke som retsgrundlag for behandling af følsomme oplysninger: I henhold til direktivets artikel 8, stk. 2, litra e), er behandling ikke forbudt, hvis den vedrører oplysninger, som klart er offentliggjort af den registrerede. I denne bestemmelse forudsættes det tydeligvis, at den registreredes offentliggørelse af sine personoplysninger skal fortolkes som et underforstået samtykke til anvendelsen af sådanne oplysninger.

Den registreredes vitale interesser

Som ved ikke-følsomme oplysninger må følsomme oplysninger behandles af hensyn til den registreredes vitale interesser[144].

143 *Ibid.*, artikel 8, stk. 2, litra a).

144 *Ibid.*, artikel 8, stk. 2, litra c).

For at behandling af følsomme oplysninger kan være lovlig på dette grundlag, skal det nødvendigvis have været umuligt at anmode om den registreredes samtykke, f.eks. fordi den registrerede var bevidstløs eller var fraværende og ikke kunne kontaktes.

Andres legitime interesser

Som ved ikke-følsomme oplysninger kan andres legitime interesser være grundlag for behandling af følsomme oplysninger. For følsomme oplysninger og i henhold til databeskyttelsesdirektivets artikel 8, stk. 2, gælder dette dog kun i følgende tilfælde:

- hvis behandlingen er nødvendig for at beskytte en anden persons vitale interesser[145] i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke

- hvis følsomme oplysninger er relevante på det arbejdsretlige område, f.eks. helbredsoplysninger i forbindelse med en særlig farlig arbejdsplads, eller oplysninger om religiøs overbevisning i forbindelse med f.eks. helligdage[146]

- hvis en stiftelse, en forening eller et andet almennyttigt organ, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, behandler oplysninger om organets medlemmer eller sponsorer eller andre berørte parter (sådanne oplysninger er følsomme, fordi de sandsynligvis afslører de pågældende personers religiøse eller politiske overbevisning)[147]

- hvis følsomme oplysninger anvendes i forbindelse med sager ved domstole eller forvaltningsmyndigheder og er nødvendige for, at et retskrav kan fastlægges, gøres gældende eller forsvares[148].

- Hvis helbredsoplysninger bruges af erhvervsudøvende i sundhedssektoren til lægelig undersøgelse og behandling, er sådan behandling i henhold til databeskyttelsesdirektivets artikel 8, stk. 3, omfattet af denne undtagelse. Som en

145 *Ibid.*

146 *Ibid.*, artikel 8, stk. 2, litra b).

147 *Ibid.*, artikel 8, stk. 2, litra d).

148 *Ibid.*, artikel 8, stk. 2, litra e).

særlig garanti anerkendes personer kun som "erhvervsudøvende i sundhedssektoren", hvis de har tavshedspligt.

Samfundsmæssige interesser

I henhold til databeskyttelsesdirektivets artikel 8, stk. 4, kan medlemsstaterne endvidere fastsætte yderligere grunde til at behandle følsomme oplysninger, såfremt:

- behandlingen af oplysninger vedrører hensynet til vigtige samfundsmæssige interesser
- undtagelsen er fastsat ved national lovgivning eller ved en afgørelse truffet af tilsynsmyndigheden
- der gives tilstrækkelige garantier i den nationale lovgivning eller tilsynsmyndighedens beslutning til effektivt at beskytte de registreredes interesser[149].

Et fremtrædende eksempel er elektroniske patientjournalsystemer, som er ved at blive indført i mange medlemsstater. 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, som er baseret på databeskyttelsesdirektivets artikel 8, stk. 3. Hvis det antages, at sådanne elektroniske patientjournalsystemer udgør en væsentlig samfundsmæssig interesse, kan de dog baseres på direktivets artikel 8, stk. 4, som kræver et udtrykkeligt retsgrundlag for deres indførelse, herunder de nødvendige garantier for, at systemet køres sikkert[150].

149 *Ibid.*, artikel 8, stk. 4.

150 Artikel 29-Gruppen (2007), arbejdsdokument vedrørende behandling af personlige sundhedsoplysninger i elektroniske patientjournaler (EPJ), WP 131, Bruxelles, den 15. februar 2007.

4.2. Regler om behandlingssikkerhed

Hovedpunkter

- Reglerne om behandlingssikkerhed pålægger den registeransvarlige og registerføreren at gennemføre passende tekniske og organisatoriske foranstaltninger med det formål at forhindre uautoriseret indgriben i databehandlinger.
- Det nødvendige niveau af datasikkerhed fastlægges på baggrund af:
  - de sikkerhedsfunktioner, der findes på markedet til en bestemt type behandling
  - omkostningerne
  - følsomheden af de oplysninger, der behandles.
- Sikker behandling af oplysninger sikres endvidere ved den generelle forpligtelse, der pålægges alle personer, registeransvarlige og registerførere, til at sikre, at oplysningerne forbliver fortrolige.

De registeransvarliges og registerførernes forpligtelse til at indføre passende foranstaltninger til forbedring af datasikkerheden er derfor fastlagt i både **Europarådets konventioner om databeskyttelse** og **EU's databeskyttelseslovgivning**.

4.2.1. Elementer af datasikkerhed

I **EU-rettens** relevante bestemmelser anføres følgende:

> *"Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling"*[151].

En lignende bestemmelse findes i **Europarådets retsorden**:

> *Relevante sikkerhedsforanstaltninger gennemføres med henblik på at beskytte elektronisk lagrede personoplysninger mod hændelig eller ubeføjet*

151 Databeskyttelsesdirektivet, artikel 17, stk. 1.

tilintetgørelse eller hændeligt tab samt mod ikke-autoriseret adgang, ændring eller udbredelse[152].

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 (Det Europæiske Agentur for Net- og Informationssikkerhed) blev oprettet for at styrke EU's, medlemsstaternes og erhvervslivets evne til at forhindre, løse og reagere på netværks- og informationssikkerhedsproblemer[153]. ENISA offentliggør regelmæssigt analyser af aktuelle sikkerhedstrusler og rådgiver om, hvordan de kan afhjælpes.

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

- 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 registeransvarliges eller registerførerens 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

152 Konvention 108, artikel 7.

153 Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed, EUT 2004 L 77.

- automatiske protokoller over adgangen til elektroniske personoplysninger og regelmæssig kontrol af disse protokoller gennemført af den interne tilsynsfunktion

- omhyggelig dokumentation af andre former for videregivelse end automatisk adgang til oplysninger med henblik på at påvise, at ulovlig dataoverførsel ikke har fundet sted.

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 intern eller ekstern audit).

Foranstaltninger vedrørende forbedring af en registeransvarligs eller registerførers sikkerhedsniveau omfatter instrumenter, som f.eks. databeskyttelsesansvarlige, sikkerhedsuddannelse af medarbejdere, regelmæssig audit, gennemtrængningstest og kvalitetsmærker.

Eksempel: I sagen *I. mod Finland*[154] 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. Menneskerettighedsdomstolen konkluderede, at artikel 8 i EMK 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.

Anmeldelse af brud på datasikkerheden

Flere europæiske lande har i deres databeskyttelseslovgivning indført et nyt instrument til håndtering af krænkelser af datasikkerheden: De forpligter udbydere af elektroniske kommunikationstjenester til at anmelde brud på datasikkerheden til

154 Menneskerettighedsdomstolen, *I. mod Finland*, nr. 20511/03, 17. juli 2008.

de sandsynlige ofre og tilsynsmyndighederne. For telekommunikationsudbydere er det obligatorisk i henhold til EU-retten[155]. Formålet med anmeldelse af brud på datasikkerheden er at undgå skade: Anmeldelse af brud på datasikkerheden og deres mulige konsekvenser minimerer risikoen for negative følger for de registrerede. I tilfælde af grov uagtsomhed kan udbyderne idømmes bøder.

Der skal på forhånd fastlægges interne procedurer for effektiv forvaltning og indberetning af brud på sikkerheden, da tidsrammen for forpligtelsen til at anmelde brud til de registrerede og/eller tilsynsmyndigheden normalt er ganske kort i henhold til den nationale lovgivning.

4.2.2. Fortrolighed

I **EU-retten** sikres sikker behandling af oplysninger endvidere ved den generelle forpligtelse, der pålægges alle personer, registeransvarlige og registerførere, til at sikre, at oplysningerne forbliver fortrolige.

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.

Databeskyttelsesdirektivets artikel 16 vedrører kun fortrolighed inden for forhold mellem registeransvarlige og registerførere. Om registeransvarlige skal holde oplysninger fortrolige og således ikke må videregive dem til tredjemand, er omhandlet i databeskyttelsesdirektivets artikel 7 og 8.

155 Se 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 2002 L 201, artikel 4, stk. 3, 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 2009 L 337.

Tavshedspligten omfatter ikke situationer, hvor en person fik kendskab til oplysninger som privatperson og ikke som arbejdsgiver eller en registeransvarlig eller registerfører. I det tilfælde finder databeskyttelsesdirektivets artikel 16 ikke anvendelse, da privatpersoners anvendelse af personoplysninger fuldstændigt er udelukket fra direktivets anvendelsesområde, hvis sådan anvendelse falder inden for grænserne af "den familiemæssige undtagelse"[156]. Den familiemæssige undtagelse er anvendelsen af personoplysninger, "som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter"[157]. Siden EU-Domstolens afgørelse i sagen *Bodil Lindqvist*[158] 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 (flere oplysninger om denne sag findes i afsnit 2.1.2, 2.2, 2.3.1 og 6.1).

I Europarådets retsorden er tavshedspligten underforstået i begrebet datasikkerhed i artikel 7 i konvention 108, som omhandler datasikkerhed.

For registerførere betyder tavshedspligten, at de kun må bruge de personoplysninger, de har fået betroet af den registeransvarlige, i overensstemmelse med den registeransvarliges instrukser. For en registeransvarligs eller registerførers medarbejdere kræver tavshedspligten, at de kun anvender personoplysninger i overensstemmelse med instrukserne fra deres kompetente overordnede.

Tavshedspligten skal medtages i enhver kontrakt mellem registeransvarlige og deres registerførere. Registeransvarlige og registerførere 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 i konvention 108.

156 Databeskyttelsesdirektivet, artikel 3, stk. 2, andet led.

157 *Ibid.*

158 EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003.

4.3. Regler om gennemsigtighed ved behandling

Hovedpunkter

- Inden den registeransvarlige påbegynder behandlingen af personoplysninger, skal vedkommende som et absolut minimum informere den registrerede om den registeransvarliges identitet og formålet med databehandlingen, medmindre den registrerede allerede har denne information.
- Hvis oplysningerne indsamles fra tredjemand, gælder oplysningspligten ikke, hvis:
  - databehandlingen er fastsat ved lov, eller
  - hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssig vanskelig.
- Inden den registeransvarlige påbegynder behandlingen af personoplysninger, skal vedkommende desuden:
  - meddele de planlagte behandlinger til tilsynsmyndigheden eller
  - få behandlingen dokumenteret internt af en uafhængig databeskyttelsesansvarlig, hvis dette er i overensstemmelse med national lovgivning.

Princippet om retfærdig behandling kræver gennemsigtighed i behandlingen. I henhold til **Europarådets retsorden** skal en person i den forbindelse kunne få oplyst eksistensen af databehandlingsregistre, deres formål og den registeransvarlige[159]. Hvordan dette sikres, overlades til den nationale lovgivning. **EU-retten** er mere specifik og sikrer gennemsigtighed for den registrerede gennem den registeransvarliges forpligtelse til at underrette den registrerede og for offentligheden gennem anmeldelse.

I henhold til begge retsordener kan der indføres undtagelser fra og begrænsninger af den registeransvarliges forpligtelse til gennemsigtighed i den nationale lovgivning, hvis en sådan begrænsning udgør en nødvendig foranstaltning for at sikre visse offentlige interesser eller for at beskytte den registreredes eller andres rettigheder og friheder, såfremt den er nødvendig i et demokratisk samfund[160]. Sådanne

159 Konvention 108, artikel 8, litra a).

160 *Ibid.*, artikel 9, stk. 2, og databeskyttelsesdirektivet, artikel 13, stk. 1

undtagelser kan f.eks. være nødvendige i forbindelse med efterforskning af kriminalitet, men kan også begrundes i andre tilfælde.

4.3.1. Oplysningspligt

I henhold til Europarådets retsorden og EU-retten har registeransvarlige for behandlinger pligt til på forhånd at underrette den registrerede om den planlagte behandling[161]. Denne forpligtelse afhænger ikke af en anmodning fra den registrerede, men skal overholdes proaktivt af den registeransvarlige, uanset om den registrerede viser interesse for informationen eller ej.

Indhold af informationerne

Informationerne skal omfatte formålet med behandlingen samt den registeransvarliges identitet og kontaktoplysninger[162]. I henhold til databeskyttelsesdirektivet skal der gives yderligere informationer, "for så vidt som disse yderligere informationer, under hensyn til de særlige omstændigheder hvorunder oplysningerne indsamles, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne". I direktivets artikel 10 og 11 beskrives bl.a. kategorierne af behandlede oplysninger og modtagerne af sådanne oplysninger, samt hvorvidt der gives ret til at få indsigt i og foretage berigtigelse af oplysningerne. Hvis oplysninger indsamles fra den registrerede, bør informationerne afklare, om det er obligatorisk eller frivilligt at besvare spørgsmålene, samt mulige følger af ikke at svare[163].

For så vidt angår **Europarådets retsorden**, kan fremlæggelsen af sådanne informationer betragtes som god praksis i forbindelse med princippet om rimelig databehandling og er i den henseende også omhandlet i Europarådets retsorden.

Princippet om rimelig behandling kræver, at informationerne er letforståelige for den registrerede. Der skal benyttes et sprog, som er hensigtsmæssigt for målgruppen. Sprogbrugen skal tilpasses den specifikke målgruppe, f.eks. voksne eller børn, den brede offentlighed eller eksperter.

Nogle registrerede ønsker kun at få oplyst, hvordan og hvorfor deres oplysninger behandles, mens andre kræver en mere detaljeret forklaring. Hvordan dette aspekt

161 Konvention 108, artikel 8, litra a), og databeskyttelsesdirektivet, artikel 10 og 11.

162 Konvention 108, artikel 8, litra a), og databeskyttelsesdirektivet, artikel 10, litra a) og b).

163 Databeskyttelsesdirektivet, artikel 10, litra c).

af rimelig behandling afvejes, er omhandlet i en udtalelse fra Artikel 29-Gruppen, som argumenterer for idéen om lagdelte meddelelser[164], som giver den registrerede mulighed for at vælge det detaljeringsniveau, han eller hun foretrækker.

Tidspunkt for meddelelse

Databeskyttelsesdirektivet indeholder lidt forskellige bestemmelser vedrørende tidspunktet for, hvornår de registrerede skal underrettes, afhængigt af om oplysninger indsamles hos den registrerede (artikel 10) eller fra tredjemand (artikel 11). Hvis oplysninger indsamles hos den registrerede, skal informationerne gives senest på tidspunktet for indsamlingen. Hvis oplysninger indsamles fra tredjemand, skal informationerne gives senest på det tidspunkt, hvor den registeransvarlige registrerer oplysningerne, eller inden oplysningerne første gang videregives til en tredjemand.

Undtagelser fra oplysningspligten

EU-retten omfatter en generel undtagelse fra pligten til at informere den registrerede, hvis den registrerede allerede er bekendt med informationerne[165]. Dette er f.eks. tilfældet, når den registrerede allerede er bekendt med, at vedkommendes oplysninger behandles til et bestemt formål af en bestemt registeransvarlig.

I henhold til direktivets artikel 11, som vedrører pligten til at informere en registreret, når oplysningerne ikke er indsamlet hos vedkommende, finder en sådan forpligtelse heller ikke anvendelse, når behandlingen foretages i statistisk øjemed eller til historiske eller videnskabelige forskningsformål, hvis:

- underretning af den registrerede viser sig umulig, eller
- er uforholdsmæssig vanskelig, eller
- registreringen eller videregivelsen af oplysningerne er udtrykkeligt fastsat ved lov[166].

164 Artikel 29-Gruppen (2004), udtalelse 10/2004 om mere harmoniserede bestemmelser om oplysningspligt, WP 100, Bruxelles, den 25. november 2004.

165 Databeskyttelsesdirektivet, artikel 10 og artikel 11, stk. 1.

166 *Ibid.*, betragtning 40 og artikel 11, stk. 2.

Kun artikel 11, stk. 2, i databeskyttelsesdirektivet fastlægger, at registrerede ikke skal underrettes om behandlinger, hvis de er fastsat ved lov. På baggrund af den generelle juridiske antagelse af, at loven er kendt for de omhandlede, kan det hævdes, at den registrerede er bekendt med informationerne, når oplysninger er indsamlet hos en registreret i medfør af direktivets artikel 10. Eftersom kendskab til loven kun er en antagelse, kræver princippet om rimelig behandling i henhold til artikel 10, at den registrerede underrettes, selv om behandlingen er fastsat ved lov, især da det ikke er specielt besværligt at underrette den registrerede, når oplysninger indsamles direkte hos vedkommende.

For så vidt angår **Europarådets retsorden**, fastlægger konvention 108 udtrykkeligt undtagelser fra konventionens artikel 8. Igen kan de undtagelser, der er fastsat ved databeskyttelsesdirektivets artikel 10 og 11, ses som eksempler på god praksis for undtagelser i medfør af artikel 9 i konvention 108.

Forskellige metoder til underretning

Den ideelle underretningsmetode er direkte henvendelse – mundtlig eller skriftlig – til hver enkelt registreret. Hvis oplysninger indsamles hos den registrerede, bør underretning ske samtidig med indsamlingen. Hvis oplysninger indsamles fra tredjemand, kan underretning også ske ved passende offentliggørelse, især i betragtning af de indlysende praktiske vanskeligheder ved at kontakte de registrerede personligt.

Registrerede kan informeres effektivt ved at indsætte de relevante informationer på den registeransvarliges websted, f.eks. en databeskyttelsespolitik for webstedet. Der er dog en betydelig del af befolkningen, som ikke bruger internettet, og en virksomheds eller offentlig myndigheds informationspolitik bør tage højde for dette.

4.3.2. Anmeldelse

Der kan ved national lov fastsættes forpligtelser for registeransvarlige til at underrette den kompetente tilsynsmyndighed om deres behandlinger, så disse kan offentliggøres. Det kan ved national lov alternativt fastsættes, at registeransvarlige kan ansætte en databeskyttelsesansvarlig med ansvar for at føre et register over den registeransvarliges behandling af personoplysninger[167]. Dette interne register skal efter anmodning stilles til rådighed for offentligheden.

167 *Ibid.*, artikel 18, stk. 2, andet led.

Eksempel: I anmeldelsen og den interne databeskyttelsesansvarliges dokumentation beskrives hovedelementerne af den pågældende behandling af personoplysninger. Det omfatter information om den registeransvarlige, formålet med behandlingen, retsgrundlaget for behandlingen, kategorierne af behandlede oplysninger og de sandsynlige tredjemandsmodtagere, samt om der planlægges grænseoverskridende dataoverførsler, og hvis det er tilfældet, hvilke.

Tilsynsmyndighedens offentliggørelse af anmeldelser skal ske gennem et særskilt register. For at opfylde dette formål skal der være nem og vederlagsfri adgang til dette register. Det samme gælder for dokumentation, der opbevares af den databeskyttelsesansvarlige hos en registeransvarlig.

Undtagelser fra pligten til at underrette den kompetente tilsynsmyndighed eller ansætte en databeskyttelsesansvarlig kan fastsættes ved national lov for de typer behandling, hvor det ikke er sandsynligt, at de registreredes rettigheder eller frihedsrettigheder krænkes, jf. databeskyttelsesdirektivets artikel 18, stk. 2[168].

4.4. Regler om fremme af overensstemmelse

Hovedpunkter

- I forlængelse af princippet om ansvarlighed nævner databeskyttelsesdirektivet en række instrumenter til fremme af overensstemmelse:
  - forudgående kontrol af planlagte behandlinger foretaget af den nationale tilsynsmyndighed
  - databeskyttelsesansvarlige, der tilfører den registeransvarlige særlig ekspertise inden for databeskyttelse
  - adfærdskodekser, som beskriver de eksisterende databeskyttelsesregler, der skal anvendes i en bestemt sektor.
- Europarådet foreslår lignende instrumenter til fremme af overensstemmelse i sin henstilling om profilering.

168 *Ibid.*, artikel 18, stk. 2, første led.

4.4.1. Forudgående kontrol

I henhold til databeskyttelsesdirektivets artikel 20 skal tilsynsmyndigheden kontrollere de behandlinger, der kan indebære særlige risici for personers rettigheder og frihedsrettigheder – i medfør af formålet med eller omstændighederne bag behandlingen – inden behandlingen påbegyndes. Det præciseres ved national lov, hvilke behandlinger der kræver forudgående kontrol. En sådan kontrol kan bevirke, at behandlinger forbydes, eller at der udstedes påbud om at ændre den foreslåede udformning af behandlingerne. Direktivets artikel 20 har til formål at sikre, at unødvendig risikabel behandling end ikke påbegyndes, idet tilsynsmyndigheden har beføjelse til at forbyde sådanne behandlinger. Denne ordning kan kun fungere, hvis behandlingen rent faktisk anmeldes til tilsynsmyndigheden. For at sikre, at registeransvarlige overholder deres anmeldelsespligt, skal tilsynsmyndigheder have tvangsbeføjelser, som f.eks. mulighed for at udstede bøder til registeransvarlige.

Eksempel: Hvis en virksomhed foretager behandlinger, der i henhold til national lovgivning er underlagt forudgående kontrol, skal virksomheden indsende dokumentation vedrørende de planlagte behandlinger til tilsynsmyndigheden. Virksomheden må først påbegynde behandlingerne, når den har modtaget et positivt svar fra tilsynsmyndigheden.

I nogle medlemsstater kan behandlinger i henhold til den nationale lovgivning påbegyndes, hvis tilsynsmyndigheden ikke har reageret inden for en bestemt tidsfrist, f.eks. tre måneder.

4.4.2. Databeskyttelsesansvarlige

I henhold til databeskyttelsesdirektivet kan det ved national lov fastsættes, at registeransvarlige må udpege en person til at fungere som databeskyttelsesansvarlig ("person med ansvar for beskyttelse af personoplysninger")[169]. En sådan person har til opgave at sikre, at det er ikke sandsynligt, at de registreredes rettigheder og frihedsrettigheder vil kunne krænkes som følge af behandlingen[170].

Eksempel: I Tyskland skal privatejede virksomheder i henhold til § 4f, stk. 1, i den tyske forbundslov om databeskyttelse (*Bundesdatenschutzgesetz*) udpege

169 *Ibid.*, artikel 18, stk. 2, andet led.

170 *Ibid.*

en intern databeskyttelsesansvarlig, hvis de permanent har ansat mindst 10 medarbejdere inden for elektronisk behandling af personoplysninger.

For at opfylde dette formål skal den pågældende medarbejder have en vis uafhængighed i den registeransvarliges organisation, som det udtrykkeligt påpeges i direktivet. Stærke ansættelsesrettigheder, der beskytter mod eventualiteter, som f.eks. uberettiget afskedigelse, er også nødvendige, for at denne person kan udfylde sin rolle effektivt.

For at fremme overensstemmelsen med den nationale databeskyttelseslov er begrebet "interne databeskyttelsesansvarlige" også omhandlet i nogle af Europarådets henstillinger[171].

4.4.3. Adfærdskodekser

For at fremme overensstemmelsen kan industrien og andre sektorer udarbejde detaljerede regler for deres typiske behandlingsaktiviteter med det formål at kodificere bedste praksis. De førende medlemmer af sektoren vil tilstræbe at finde løsninger, der er praktiske, og som dermed sandsynligvis vil blive fulgt. Medlemsstaterne – og Kommissionen – opfordres derfor til at udarbejde adfærdskodekser, der afhængigt af de særlige forhold i de forskellige sektorer kan bidrage til en korrekt anvendelse af de nationale bestemmelser, som medlemsstaterne vedtager i medfør af direktivet[172].

For at sikre, at disse adfærdskodekser overholder de nationale bestemmelser, der er vedtaget i medfør af databeskyttelsesdirektivet, skal medlemsstaterne fastlægge en procedure for evaluering af kodekserne. Denne procedure kræver inddragelse af den nationale tilsynsmyndighed, branchesammenslutninger og andre organer, som repræsenterer andre kategorier af registeransvarlige[173].

Udkast til EF-kodeks og forslag til ændring eller forlængelse af eksisterende EF-kodekser kan forelægges Artikel 29-Gruppen til evaluering. Kommissionen kan tilse, at de kodekser, som gruppen har godkendt, offentliggøres på passende vis[174].

171 Se eksempelvis henstilling om profilering, artikel 8, stk. 3.

172 Databeskyttelsesdirektivet, artikel 27, stk. 1.

173 *Ibid.*, artikel 27, stk. 2.

174 *Ibid.*, artikel 27, stk. 3.

Eksempel: FEDMA (Federation of European Direct and Interactive Marketing) udarbejdede en europæisk adfærdskodeks for brugen af personoplysninger med henblik på markedsføring. Kodeksen blev forelagt Artikel 29-Gruppen. Et bilag vedrørende elektroniske markedsføringsmeddelelser blev tilføjet kodeksen i 2010[175].

175 Artikel 29-Gruppen (2010), udtalelse 4/2010 om FEDMA's adfærdskodeks for brugen af personoplysninger med henblik på markedsføring, WP 174, Bruxelles, den 13. juli 2010.

5

Den registreredes rettigheder og håndhævelsen heraf

EU	Omhandlede emner	Europarådet
Ret til indsigt		
Databeskyttelsesdirektivet, artikel 12 EU-Domstolen, C-553/07, *College van burgemeester en wethouders van Rotterdam mod M.E.E. Rijkeboer*, 7. maj 2009	**Ret til indsigt i egne oplysninger**	Konvention 108, artikel 8, litra b)
	Ret til berigtigelse, sletning eller blokering	Konvention 108, artikel 8, litra c) Menneskerettighedsdomstolen, *Cemalettin Canli mod Tyrkiet*, nr. 22427/04, 18. november 2008 Menneskerettighedsdomstolen, *Segerstedt-Wiberg m.fl. mod Sverige*, nr. 62332/00, 6. juni 2006 Menneskerettighedsdomstolen, *Ciubotaru mod Moldova*, nr. 27138/04, 27. april 2010
Ret til indsigelse		
Databeskyttelsesdirektivet, artikel 14, stk. 1, litra a)	**Ret til indsigelse i medfør af den registreredes særlige situation**	Henstilling om profilering, artikel 5, stk. 3

EU	Omhandlede emner	Europarådet
Databeskyttelsesdirektivet, artikel 14, stk. 1, litra b)	**Ret til indsigelse mod yderligere behandling af oplysninger med henblik på markedsføring**	Henstilling om markedsføring, artikel 4, stk. 1
Databeskyttelsesdirektivet, artikel 15	**Ret til indsigelse mod afgørelser, der alene er truffet på grundlag af elektronisk databehandling**	Henstilling om profilering, artikel 5, stk. 5
Uafhængigt tilsyn		
Chartret, artikel 8, stk. 3 Databeskyttelsesdirektivet, artikel 28 EU-institutioner, afdeling V Databeskyttelseslovgivning EU-Domstolen, C-518/07, *Europa-Kommissionen mod Tyskland*, 9. marts 2010 EU-Domstolen, C-614/10, *Europa-Kommissionen mod Østrig*, 16. oktober 2012 EU-Domstolen, C-288/12, *Europa-Kommissionen mod Ungarn*, 8. april 2014	**Nationale tilsynsmyndigheder**	Konvention 108, tillægsprotokol, artikel 1
Retsmidler og sanktioner		
Databeskyttelsesdirektivet, artikel 12	**Anmodning til den registeransvarlige**	Konvention 108, artikel 8, litra b)
Databeskyttelsesdirektivet, artikel 28, stk. 4 Forordningen om databeskyttelse inden for EU-institutionerne, artikel 32, stk. 2	**Klager indgivet til en tilsynsmyndighed**	Konvention 108, tillægsprotokol, artikel 1, stk. 2, litra b)
Chartret, artikel 47	**Domstolene (generelt)**	EMK, artikel 13
Databeskyttelsesdirektivet, artikel 28, stk. 3	**Nationale domstole**	Konvention 108, tillægsprotokol, artikel 1, stk. 4
TEUF, artikel 263, stk. 4 Forordningen om databeskyttelse inden for EU-institutionerne, artikel 32, stk. 1 TEUF, artikel 267	**EU-Domstolen**	

EU	Omhandlede emner	Europarådet
	Menneskerettigheds-domstolen	EMK, artikel 34
Retsmidler og sanktioner		
Chartret, artikel 47 Databeskyttelsesdirektivet, artikel 22 og 23 EU-Domstolen, C-14/83, *Sabine von Colson og Elisabeth Kamann mod Land Nordrhein-Westfalen*, 10. april 1984 EU-Domstolen, C-152/84, *M.H. Marshall mod Southampton and South-West Hampshire Area Health Authority*, 26. februar 1986	For overtrædelser af den nationale databeskyttelseslovgivning	EMK, artikel 13 (kun for Europarådets medlemsstater) Konvention 108, artikel 10 Menneskerettighedsdomstolen, *K.U. mod Finland*, nr. 2872/02, 2. december 2008 Menneskerettighedsdomstolen, *Biriuk mod Litauen*, nr. 23373/03, 25. november 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*, 29. juni 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 henhold til den europæiske databeskyttelseslovgivning skal den registrerede i den nationale lovgivning tillægges beføjelser til at beskytte sine oplysninger. Uafhængige tilsynsmyndigheder skal oprettes ved lov med det formål at hjælpe de registrerede med at udøve deres rettigheder og føre tilsyn med behandlingen af personoplysninger. Retten til effektive retsmidler som garanteret ved den europæiske menneskerettighedskonvention og chartret kræver desuden, at alle personer har adgang til retsmidler.

5.1. Registreredes rettigheder

Hovedpunkter

- Alle har i medfør af den nationale lovgivning ret til at anmode en registeransvarlig om information om, hvorvidt den registeransvarlige behandler vedkommendes oplysninger.

- Registrerede har i medfør af national lovgivning ret til at:
  - få aktindsigt i deres egne oplysninger fra enhver registeransvarlig, der behandler disse oplysninger
  - få deres oplysninger berigtiget (eller eventuelt blokeret) af den registeransvarlige, som behandler deres oplysninger, hvis oplysningerne er urigtige
  - få deres oplysninger slettet (eller eventuelt blokeret) af den registeransvarlige, hvis vedkommende behandler deres oplysninger ulovligt.
- Registrerede har endvidere ret til at gøre indsigelse til den registeransvarlige mod:
  - edb-behandlede afgørelser (truffet ud fra personoplysninger, der alene er behandlet ved hjælp af elektroniske hjælpemidler)
  - behandlingen af deres oplysninger, hvis den fører til uforholdsmæssige resultater
  - anvendelsen af deres oplysninger med henblik på markedsføring.

5.1.1. Ret til indsigt

I EU-retten indeholder databeskyttelsesdirektivets artikel 12 elementerne af de registreredes ret til indsigt, herunder retten til hos den registeransvarlige "at få oplyst, om der behandles personoplysninger om den pågældende selv, samt mindst formålene med behandlingen, hvilken type oplysninger det drejer sig om, og modtagerne eller kategorierne af modtagere af oplysningerne" og "at få oplysninger, som ikke er blevet behandlet i overensstemmelse med dette direktiv, berigtiget, slettet eller blokeret, navnlig hvis de er ufuldstændige eller urigtige".

Europarådets retsorden omfatter de samme rettigheder, som også skal være fastsat ved national lovgivning (artikel 8 i konvention 108). I flere henstillinger fra Europarådet anvendes udtrykket "indsigt" (access), og de forskellige aspekter af retten til indsigt er beskrevet og foreslået gennemført i national lovgivning på samme måde som beskrevet i afsnittet ovenfor.

I henhold til artikel 9 i konvention 108 og databeskyttelsesdirektivets artikel 13 kan registeransvarliges forpligtelse til at imødekomme en registrerets anmodning om indsigt begrænses, hvis en sådan begrænsning er nødvendig af hensyn til andres retlige interesser, der går forud herfor. Sådanne retlige interesser kan omfatte samfundsmæssige interesser, som f.eks. statens sikkerhed, den offentlige sikkerhed og retsforfølgning i straffesager, og private interesser, der er vigtigere end hensynet til beskyttelse af personoplysninger. Enhver undtagelse eller begrænsning skal være

nødvendig i et demokratisk samfund og skal stå i forhold til det forfulgte formål. I særlige tilfælde, f.eks. som følge af medicinske indikationer, kan beskyttelsen af den registrerede kræve, at gennemsigtigheden begrænses. Dette vedrører især begrænsning af alle registreredes ret til indsigt.

Når oplysninger udelukkende behandles med statistisk eller videnskabelig forskning for øje, tillader databeskyttelsesdirektivet, at der ved national lov fastsættes begrænsninger for retten til indsigt, men der skal dog gives tilstrækkelige retsgarantier. Det skal navnlig sikres, at der ikke træffes foranstaltninger eller afgørelser vedrørende bestemte personer, og at der "klart ikke er nogen risiko for, at den registreredes ret til privatlivets fred krænkes"[176]. Lignende bestemmelser findes i artikel 9, stk. 3, i konvention 108.

Ret til indsigt i egne oplysninger

I Europarådets retsorden anerkendes retten til indsigt i egne oplysninger udtrykkeligt ved artikel 8 i konvention 108. Menneskerettighedsdomstolen har gentagne gange bekræftet, at personer har ret til indsigt i egne oplysninger, som andre er i besiddelse af eller anvender, og at denne ret udledes af retten til respekt for privatlivet[177]. I sagen *Leander*[178] konkluderede Menneskerettighedsdomstolen, at retten til indsigt i egne personoplysninger, som var lagret af de offentlige myndigheder, dog kunne begrænses under visse omstændigheder.

I EU-retten anerkendes retten til indsigt i egne oplysninger udtrykkeligt ved databeskyttelsesdirektivets artikel 12 og som en grundlæggende rettighed i chartrets artikel 8, stk. 2.

I henhold til direktivets artikel 12, litra a), skal medlemsstaterne sikre enhver registreret ret til indsigt i deres personoplysninger og til information. Enhver registreret har navnlig ret til hos den registeransvarlige at få oplyst, om der behandles personoplysninger om den pågældende selv, og få meddelt information om mindst følgende:

176 Databeskyttelsesdirektivet, artikel 13, stk. 2.

177 Menneskerettighedsdomstolen, *Gaskin mod Det Forenede Kongerige*, nr. 10454/83, 7. juli 1989, Menneskerettighedsdomstolen, *Odièvre mod Frankrig* [GC], nr. 42326/98, 13. februar 2003, Menneskerettighedsdomstolen, *K.H. m.fl. mod Slovakiet*, nr. 32881/04, 28. april 2009, Menneskerettighedsdomstolen, *Godelli mod Italien*, nr. 33783/09, 25. september 2012.

178 Menneskerettighedsdomstolen, *Leander mod Sverige*, nr. 9248/81, 11. juli 1985.

- formålene med behandlingen
- hvilken type personoplysninger der er tale om
- hvilke oplysninger der er omfattet af behandlingerne
- modtagerne eller kategorierne af modtagere af oplysningerne
- tilgængelig information om, hvorfra disse oplysninger stammer
- hvilken logik der ligger bag edb-behandlingen af oplysningerne, hvis der er tale om edb-behandlede afgørelser.

Den nationale lovgivning kan fastsætte, hvilke informationer den registeransvarlige skal meddele, f.eks. henvisning til retsgrundlaget for behandlingen af personoplysninger.

Eksempel: Hvis man får indsigt i sine egne personoplysninger, kan man afgøre, om de er rigtige. Det er derfor en absolut nødvendighed, at den registrerede informeres om de kategorier af oplysninger, der behandles, og om indholdet af disse oplysninger. Det er således ikke tilstrækkeligt, at en registeransvarlig blot oplyser den registrerede, at man behandler vedkommendes navn, adresse, fødselsdato og interesseområde. Den registeransvarlige skal også oplyse den registrerede, at man behandler "navnet: N.N.; adressen: 1040 Wien, Schwarzenbergplatz 11, Østrig; fødselsdatoen: 10.10.1974; og interesseområdet (ifølge den registreredes angivelse): klassisk musik". Det sidste element indeholder desuden information om datakilden.

Information til den registrerede om de oplysninger, der behandles, og om tilgængelig information om deres kilde skal meddeles på en forståelig måde, dvs. at den registeransvarlige muligvis i yderligere detaljer skal forklare den registrerede, hvad der behandles. Det er f.eks. sædvanligvis ikke tilstrækkeligt blot at angive tekniske forkortelser eller medicinske udtryk som svar på en anmodning om indsigt, selv om kun sådanne forkortelser eller udtryk lagres.

Information om kilden til de oplysninger, der behandles af den registeransvarlige, skal meddeles som svar på en anmodning om indsigt, for så vidt som denne information er tilgængelig. Denne bestemmelse skal læses i lyset af principperne

om rimelighed og ansvarlighed samt muligheden for den registrerede til at forstå i hvilkne sammenhængoplysningerne behandles. En registeransvarlig må ikke tilintetgøre information om datakilden for at undgå at videregive den, og han må heller ikke ignorere de sædvanlige og anerkendte behov for dokumentation på sit aktivitetsområde. Den registeransvarliges forpligtelser med hensyn til retten til indsigt kan normalt ikke opfyldes ved at undlade at føre dokumentation over kilderne til de behandlede oplysninger.

Hvis der udføres elektroniske evalueringer, skal den generelle logik bag evalueringen forklares, herunder de kriterier, der er anvendt ved evaluering af den registrerede.

Direktivet fastlægger ikke, om retten til indsigt i oplysninger vedrører fortiden, og i så fald, hvilken periode i fortiden. Som det understreges i EU-Domstolens retspraksis, kan retten til indsigt i egne oplysninger i den henseende ikke begrænses unødigt af tidsfrister. Registrerede skal desuden have en rimelig mulighed for at få information om tidligere behandling af oplysninger.

Eksempel: I sagen *Rijkeboer*[179] blev EU-Domstolen anmodet om at afgøre, om en persons ret til indsigt i information om modtagerne eller kategorierne af modtagere af oplysninger og om indholdet af de videregivne oplysninger i medfør af direktivets artikel 12, litra a), kan begrænses til et år forud for indgivelsen af anmodningen.

For at afgøre, om en sådan tidsfrist er berettiget i henhold til direktivets artikel 12, litra a), besluttede Domstolen at fortolke den pågældende artikel i lyset af direktivets formål. Domstolen tilkendegav først, at retten til indsigt er nødvendig, for at den registrerede kan udøve sine rettigheder til at medvirke til, at oplysninger berigtiges, slettes eller blokeres af den registeransvarlige (artikel 12, litra b)), og at den registeransvarlige underretter tredjemand om sådanne berigtigelser, slettelser eller blokeringer (artikel 12, litra c)). Denne ret til indsigt er også nødvendig for, at den registrerede kan udøve sin ret efter direktivets artikel 14 til at gøre indsigelse mod behandling af vedkommendes personoplysninger eller sin ret til efter direktivets artikel 22 og 23 at iværksætte retsmidler, såfremt han har lidt skade.

179 EU-Domstolen, C-553/07, *College van burgemeester en wethouders van Rotterdam mod M. E. E. Rijkeboer*, 7. maj 2009.

For at sikre den effektive virkning af de bestemmelser, der er nævnt ovenfor, konstaterede 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".

Retten til berigtigelse, sletning og blokering af oplysninger

"[E]nhver skal have ret til indsigt i de oplysninger om sig selv, som gøres til genstand for behandling, så den pågældende kan forvisse sig om oplysningernes rigtighed og behandlingens lovlighed"[180]. I overensstemmelse med disse principper skal registrerede i den nationale lovgivning sikres ret til hos den registeransvarlige at få oplysninger, som ikke er blevet behandlet i overensstemmelse med direktivet, berigtiget, slettet eller blokeret, navnlig hvis de er ufuldstændige eller urigtige[181].

Eksempel: I sagen *Cemalettin Canli mod Tyrkiet*[182] vurderede Menneskerettighedsdomstolen, at artikel 8 i EMK 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 sagsøger optrådte som medlem af to illegale organisationer. Sagsøgerens anmodning om at få udleveret rapporten og politiets fortegnelser blev ikke imødekommet. Menneskerettighedsdomstolen fastslog, at informationen i politirapporten var inden for rammerne af artikel 8 i EMK, 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 loven. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

180 Databeskyttelsesdirektivet, betragtning 41.

181 *Ibid.*, artikel 12, litra b).

182 Menneskerettighedsdomstolen, *Cemalettin Canli mod Tyrkiet*, nr. 22427/04, 18. november 2008, præmis 33, 42 og 43, Menneskerettighedsdomstolen, *Dalea mod Frankrig*, nr. 964/07, 2. februar 2010.

Eksempel: I sagen *Segerstedt-Wiberg m.fl. mod Sverige*[183] havde sagsøgerne været tilknyttet visse liberale og kommunistiske politiske partier. De havde mistanke om, at oplysninger om dem var blevet registreret i sikkerhedspolitiets fortegnelser. Menneskerettighedsdomstolen fandt det godtgjort, at den anfægtede lagring af oplysninger var hjemlet i loven og forfulgte et legitimt formål. For nogle af sagsøgerne fandt Menneskerettighedsdomstolen, at den fortsatte opbevaring af oplysningerne var et uforholdsmæssigt indgreb i deres privatliv. For så vidt angår sagsøgeren Schmid, opbevarede myndighederne f.eks. oplysninger om, at han i 1969 angiveligt havde været fortaler for voldelig modstand mod politikontrol under demonstrationer. Menneskerettighedsdomstolen fandt, at disse oplysninger ikke vedrørte en relevant national sikkerhedsmæssig interesse, især på grund af deres historiske karakter. Menneskerettighedsdomstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt, for så vidt angik fire af de fem sagsøgere.

I nogle tilfælde er det tilstrækkeligt, at den registrerede blot anmoder om berigtigelse af f.eks. stavningen af et navn eller ændring af en adresse eller et telefonnummer. Hvis sådanne anmodninger vedrører juridiske spørgsmål, som f.eks. den registreredes juridiske identitet, eller den korrekte bopæl med henblik på forkyndelse af juridiske dokumenter, er anmodninger om berigtigelse muligvis ikke tilstrækkelige, og den registeransvarlige kan være berettiget til at anmode om bevis for den påståede fejl. Sådanne krav må ikke medføre en urimelig bevisbyrde for den registrerede, således at den registrerede forhindres i at få sine oplysninger berigtiget. Menneskerettighedsdomstolen har konstateret, at artikel 8 i EMK er blevet overtrådt i flere sager, hvor sagsøgeren ikke kunne anfægte rigtigheden af information i hemmelige arkiver[184].

Eksempel: I sagen *Ciubotaru mod Moldova*[185] kunne sagsøgeren ikke ændre registreringen af sin etniske oprindelse i officielle fortegnelser fra moldover til rumæner, fordi han angiveligt ikke kunne underbygge sin anmodning. Menneskerettighedsdomstolen fandt det acceptabelt, at stater kræver objektivt bevis ved registrering af en persons etniske identitet. Når et sådant krav alene var

183 Menneskerettighedsdomstolen, *Segerstedt-Wiberg m.fl. mod Sverige*, nr. 62332/00, 6. juni 2006, præmis 89 og 90. Se også eksempelvis Menneskerettighedsdomstolen, *M.K. mod Frankrig*, nr. 19522/09, 18. april 2013.

184 Menneskerettighedsdomstolen, *Rotaru mod Rumænien*, nr. 28341/95, 4. maj 2000.

185 Menneskerettighedsdomstolen, *Ciubotaru mod Moldova*, nr. 27138/04, 27. april 2010, præmis 51 og 59.

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 den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Under en civil retssag eller klagesag for en offentlig myndighed, der har til formål at afgøre, om oplysninger er rigtige eller ej, kan den registrerede anmode om, at der indføjes et notat i hans sagsakt om, at rigtigheden anfægtes, og at en officiel afgørelse afventes. I denne periode må den registeransvarlige ikke forelægge oplysningerne som bestemte eller endelige, især ikke over for tredjemand.

En registrerets anmodning om at få oplysninger slettet er ofte baseret på en påstand om, at der ikke er et legitimt retsgrundlag for behandlingen af oplysningerne. Sådanne påstande fremsættes ofte, når samtykke er blevet trukket tilbage, eller når bestemte oplysninger ikke længere er nødvendige for at opfylde formålet med dataindsamlingen. Byrden for at bevise, at databehandlingen er legitim, bæres af den registeransvarlige, da denne er ansvarlig for legitimiteten af behandlingen. I henhold til princippet om ansvarlighed skal den registeransvarlige til enhver tid kunne godtgøre, at der er et solidt retsgrundlag for databehandlingen. Ellers skal behandlingen stoppes.

Hvis behandlingen anfægtes, fordi oplysningerne angiveligt er urigtige eller behandles ulovligt, kan den registrerede i overensstemmelse med princippet om rimelig behandling kræve, at de anfægtede oplysninger blokeres. Det betyder, at oplysningerne ikke slettes, men at den registeransvarlige skal afholde sig fra at bruge oplysningerne, mens de er blokerede. Det vil især være nødvendigt, når den fortsatte anvendelse af urigtige oplysninger eller oplysninger, der opbevares ulovligt, kan skade den registrerede. Der bør ved national lov fastsættes flere detaljer om,

hvornår der kan opstå en forpligtelse til at blokere oplysninger, og hvordan denne skal opfyldes.

Den registrerede har ret til at kræve, at den registeransvarlige underretter tredjemand, til hvem personoplysninger er videregivet, om enhver berigtigelse, sletning eller blokering. Da videregivelsen af oplysninger til tredjemand bør være dokumenteret af den registeransvarlige, bør det være muligt at identificere modtagerne af oplysningerne og anmode om sletning. Hvis oplysningerne i mellemtiden er blevet offentliggjort, f.eks. på internettet, kan det være umuligt at få slettet alle forekomster, fordi alle modtagere ikke kan findes. I henhold til databeskyttelsesdirektivet er det obligatorisk at kontakte modtagere af oplysninger med henblik på berigtigelse, sletning eller blokering af oplysninger, "medmindre underretning viser sig umulig eller er uforholdsmæssig vanskelig"[186].

5.1.2. Ret til indsigelse

Retten til indsigelse omfatter retten til indsigelse mod edb-behandlede individuelle afgørelser, retten til indsigelse i medfør af den registreredes særlige situation og retten til indsigelse mod yderligere anvendelse af oplysninger med henblik på markedsføring.

Retten til indsigelse mod edb-behandlede individuelle afgørelser

Edb-behandlede afgørelser er afgørelser, der er truffet ud fra personoplysninger, der alene er behandlet ved hjælp af elektroniske hjælpemidler. Hvis sådanne afgørelser med sandsynlighed vil have en betydelig indvirkning på privatlivet for de omhandlede personer, fordi de eksempelvis vedrører kreditværdighed, erhvervsevne, adfærd eller pålidelighed, er der behov for særlig beskyttelse for at undgå uhensigtsmæssige følger. I henhold til databeskyttelsesdirektivet må edb-behandlede afgørelser ikke afgøre spørgsmål, der er vigtige for personer, og en person skal have mulighed for at kontrollere den edb-behandlede afgørelse[187].

Eksempel: Et vigtigt eksempel på en edb-behandlet afgørelse er credit scoring. For hurtigt at afgøre en potentiel kundes kreditværdighed indsamles visse oplysninger, som f.eks. erhverv og civilstand, hos den potentielle kunde og kombineres med oplysninger om den pågældende fra andre kilder, såsom

186 Databeskyttelsesdirektivet, artikel 12, litra c), sidste halvdel af punktum.

187 *Ibid.*, artikel 15, stk. 1.

kreditinformationssystemer. Disse oplysninger indsættes automatisk i en scoringalgoritme, der beregner en samlet værdi, som repræsenterer den potentielle kundes kreditværdighed. Virksomhedsmedarbejderen kan således på få sekunder afgøre, om den registrerede kan accepteres som kunde eller ej.

I henhold til direktivet skal medlemsstaterne dog fastsætte bestemmelser om, at en person kan undergives en edb-behandlet individuel afgørelse, når den registreredes interesser ikke trues, fordi afgørelsen var til fordel for den registrerede, eller beskyttes på anden måde[188]. Retten til indsigelse mod edb-behandlede afgørelser findes også i **Europarådets retsorden**, som det fremgår af henstillingen om profilering[189].

Retten til indsigelse i medfør af den registreredes særlige situation

Registrerede har ingen generel ret til at gøre indsigelse mod behandlingen af deres oplysninger[190]. Ved databeskyttelsesdirektivets artikel 14, litra a), indrømmes den registrerede dog ret til at gøre indsigelse i tilfælde af vægtige legitime grunde, der vedrører den pågældendes særlige situation. En lignende ret anerkendes i Europarådets henstilling om profilering[191]. Sådanne bestemmelser har til formål at sikre en hensigtsmæssig balance mellem den registreredes ret til databeskyttelse og andres legitime ret til at behandle den registreredes oplysninger.

Eksempel: En bank opbevarer oplysninger om kunder, der misligholder deres lån, i syv år. En kunde, hvis oplysninger er lagret i denne database, ansøger om et nyt lån. Databasen kontrolleres, kundens finansielle situation vurderes, og kunden får afslag på det nye lån. Kunden kan dog gøre indsigelse mod behandlingen af de personoplysninger, der er registreret i databasen, og anmode om at få dem slettet, hvis han eller hun kan bevise, at misligholdelsen udelukkende skyldtes en fejl, der var blevet rettet, straks kunden var blevet bekendt hermed.

188 *Ibid.*, artikel 15, stk. 2.

189 Henstilling om profilering, artikel 5, stk. 5.

190 Se også Menneskerettighedsdomstolen, *M.S. mod Sverige*, nr. 20837/92, 27. august 1997, hvor medicinske oplysninger blev videregivet uden samtykke eller indsigelsesmulighed, Menneskerettighedsdomstolen, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987, og Menneskerettighedsdomstolen, *Mosley mod Det Forenede Kongerige*, nr. 48009/08, 10. maj 2011.

191 Henstilling om profilering, artikel 5, stk. 3.

Hvis indsigelsen imødekommes, må den registeransvarlige ikke længere behandle de pågældende oplysninger. Behandling af den registreredes oplysninger, der foretages inden indsigelsen, er dog stadig legitim.

Retten til indsigelse mod yderligere brug af oplysninger med henblik på markedsføring

Databeskyttelsesdirektivets artikel 14, litra b), omhandler en specifik ret til at gøre indsigelsen mod anvendelsen af personoplysninger med henblik på markedsføring. En sådan ret er også fastlagt ved Europarådets henstilling om markedsføring[192]. Det er hensigten, at en sådan indsigelse rejses, inden oplysninger videregives til tredjemand med henblik på markedsføring. Den registrerede skal derfor have mulighed for at gøre indsigelse, inden oplysningerne videregives.

5.2. Uafhængigt tilsyn

Hovedpunkter

- 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 opgaver, herunder at:
  - overvåge og fremme databeskyttelse på nationalt plan
  - rådgive registrerede og registeransvarlige samt regeringen og offentligheden
  - behandle klager og bistå den registrerede i forbindelse med påståede krænkelser af databeskyttelsesrettighederne
  - føre tilsyn med registeransvarlige og registerførere
  - gribe effektivt ind ved at
    - udstede advarsler, påtaler eller endda bøder til registeransvarlige og registerførere

192 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.

- træffe afgørelser om, at oplysninger berigtiges, blokeres eller slettes
- forbyde behandling

- indbringe sagen for retten.

I henhold til databeskyttelsesdirektivet er uafhængigt tilsyn en vigtig foranstaltning til sikring af effektiv databeskyttelse. Ved direktivet indførtes der et instrument til håndhævelse af databeskyttelse, som indledningsvis ikke fandtes i konvention 108 eller OECD's retningslinjer for beskyttelse af privatlivets fred.

Uafhængigt tilsyn viste sig at være absolut nødvendigt for udviklingen af effektiv databeskyttelse, og derfor opfordrer en ny bestemmelse i OECD's reviderede retningslinjer for beskyttelse af privatlivets fred fra 2013 alle medlemslande til at etablere og opretholde myndigheder med ansvar for håndhævelse af databeskyttelse med den forvaltningsmæssige, ressourcemæssige og tekniske ekspertise, der kræves, for at de kan udøve deres beføjelser effektivt og træffe afgørelser på et objektivt, upartisk og ensartet grundlag[193].

I Europarådets retsorden har tillægsprotokollen til konvention 108 indført et krav om etablering af tilsynsmyndigheder. Dette instrument indeholder i artikel 1 det retsgrundlag for uafhængige tilsynsmyndigheder, som de kontraherende parter skal gennemføre i deres nationale lovgivninger. Artiklen beskriver disse myndigheders opgaver og beføjelser på samme måde som databeskyttelsesdirektivet. Tilsynsmyndigheder bør derfor i princippet fungere på samme måde i henhold til EU-retten og Europarådets retsorden.

I EU-retten blev tilsynsmyndighedernes kompetencer og organisation først beskrevet i databeskyttelsesdirektivets artikel 28, stk. 1. Ved forordningen om databeskyttelse inden for EU-institutionerne[194] blev Den Europæiske Tilsynsførende (EDPS) oprettet som tilsynsmyndighed for EU-organers og -institutioners behandling af personoplysninger. Ved beskrivelsen af den tilsynsførendes roller og ansvarsområder udnytter denne forordning de erfaringer, der er høstet siden databeskyttelsesdirektivets udstedelse.

193 OECD (2013), *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, præmis 19, litra c).

194 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 2001 L 8, artikel 41-48.

Databeskyttelsesmyndigheders uafhængighed er garanteret ved artikel 16, stk. 2, i TEUF og chartrets artikel 8, stk. 3. I den sidstnævnte bestemmelse betragtes en uafhængig myndigheds kontrol specifikt som et væsentligt element af den grundlæggende ret til databeskyttelse. Databeskyttelsesdirektivet kræver endvidere, at medlemsstaterne etablerer tilsynsmyndigheder, som har til opgave i fuld uafhængighed at overvåge anvendelsen af direktivet[195]. Loven vedrørende oprettelsen af en tilsynsmyndighed skal indeholde bestemmelser, der specifikt garanterer dens uafhængighed, og myndighedens specifikke organisation skal afspejle uafhængighed.

I 2010 behandlede EU-Domstolen første gang spørgsmålet om omfanget af kravet om uafhængighed for databeskyttelsesmyndigheder[196]. Følgende eksempler illustrerer EU-Domstolens tankegang.

Eksempel: I sagen *Kommissionen mod Tyskland*[197] nedlagde Europa-Kommissionen påstand over for EU-Domstolen om, at Tyskland havde foretaget en ukorrekt gennemførelse af kravet om, at tilsynsmyndighederne udøver deres funktioner "i fuld uafhængighed", og således ikke havde opfyldt landets forpligtelse i medfør af databeskyttelsesdirektivets artikel 28, stk. 1. Ifølge Kommissionen var problemet, at Tyskland havde underlagt de nationale tilsynsmyndigheder for beskyttelse af personoplysninger uden for den offentlige sektor i de forskellige delstater statsligt tilsyn.

Vurderingen af søgsmålet afhang i henhold til Domstolen af omfanget af kravet om uafhængighed i den pågældende bestemmelse og derfor af fortolkningen heraf.

Domstolen understregede, at udtrykket "i fuld uafhængighed" i direktivets artikel 28, stk. 1, skal fortolkes på grundlag af ordlyden af denne bestemmelse samt databeskyttelsesdirektivets formål og opbygning[198]. Domstolen fremhævede, at tilsynsmyndighederne er "vogter" af de rettigheder vedrørende behandling af personoplysninger, der sikres ved direktivet, og at opret-

195 Databeskyttelsesdirektivet, artikel 28, stk. 1, sidste punktum, og konvention 108, tillægsprotokol, artikel 1, stk. 3.

196 Se Den Europæiske Unions Agentur for Grundlæggende Rettigheders årsrapport for 2010, *Fundamental rights: challenges and achievements in 2010*, s. 59. Agenturet behandlede spørgsmålet mere indgående i sin rapport om databeskyttelse i EU (*Data protection in the European Union: the role of National Data Protection Authorities*), som blev offentliggjort i maj 2010.

197 EU-Domstolen, C-518/07, *Europa-Kommissionen mod Tyskland*, 9. marts 2010, præmis 27.

198 *Ibid.*, præmis 17 og 29.

telsen af en tilsynsmyndighed i hver medlemsstat har "afgørende betydning for beskyttelsen af personer i forbindelse med behandling af personoplysninger"[199]. Domstolen konkluderede, at "når tilsynsmyndighederne udøver deres funktioner, skal de handle objektivt og upartisk. De skal derfor beskyttes imod enhver form for ydre påvirkning, herunder direkte eller indirekte påvirkning fra staten eller delstaterne, og ikke blot imod påvirkning fra de kontrollerede organer"[200].

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. Som Domstolen understregede, uddyber artikel 44, stk. 2, i nævnte forordning dette uafhængighedsbegreb ved at tilføje, "at EDPS ved udøvelsen af sine pligter hverken må søge eller modtage instrukser fra andre". Dette udelukker statsligt tilsyn med en uafhængig databeskyttelsesmyndighed[201].

EU-Domstolen fastslog følgelig, at tyske databeskyttelsesinstitutioner på delstatsplan med ansvar for overvågning af behandling af personoplysninger, der foretages af ikke-offentlige organer, ikke var tilstrækkeligt uafhængige, fordi de var underlagt statsligt tilsyn.

Eksempel: I sagen *Kommissionen mod Østrig*[202] fremhævede EU-Domstolen lignende problemer vedrørende de hverv, der varetages af visse medlemmer af og medarbejdere hos den østrigske databeskyttelsesmyndighed (*Datenschutzkommission*, DSK). Domstolen konkluderede i den sag, at den østrigske lovgivning forhindrede den østrigske databeskyttelsesmyndighed i at udføre sine funktioner i fuld uafhængighed som defineret i databeskyttelsesdirektivet. Den østrigske databeskyttelsesmyndigheds uafhængighed var ikke tilstrækkeligt sikret, fordi forbundskansleren stiller personale til rådighed for databeskyttelsesmyndigheden, fører tilsyn med den og har til enhver tid ret til at blive informeret om dens arbejde.

Eksempel: I sagen Kommissionen mod Ungarn[203] fremhævede EU-Domstolen at: "forudsætningen [...] for at sikre, at hver tilsynsmyndighed er i stand til at

199 *Ibid.*, præmis 23.

200 *Ibid.*, præmis 25.

201 *Ibid.*, præmis 27.

202 EU-Domstolen, C-614/10, *Europa-Kommissionen mod Østrig*, 16. oktober 2012, præmis 59 og 63.

203 EU-Domstolen, *Europa-Kommissionen mod Ungarn*, C-288/12, 8. april 2014, præmis 50 og 67.

udføre de opgaver, der pålægges det i fuld uafhængighed, indebærer en forpligtelse for den pågældende medlemsstat til at tillade denne myndighed at gøre dette i sin fulde embedsperiode." EU-Kommissionen anførte endvidere at, "ved at stoppe tilsynsmyndigheden for beskyttelse af personoplysningers virke inden udløbet af embedsperioden, har Ungarn undladt at opfylde sine forpligtelser i henhold til Direktiv 95/46/EC [...]".

Tilsynsmyndigheder har i henhold til national lovgivning[204] bl.a. beføjelse og kompetence til at:

- rådgive registeransvarlige og registrerede om alle forhold vedrørende databeskyttelse
- undersøge behandlinger og gribe ind efter behov
- rette advarsler eller påtaler til registeransvarlige
- beordre berigtigelse, blokering, sletning eller tilintetgørelse af oplysninger
- midlertidigt eller definitivt forbyde en behandling
- indbringe sagen for retten.

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 registeransvarlig opbevarer relevante informationer.

Der er betydelige forskelle mellem de nationale retsområder, hvad angår procedurer og retskraften af en tilsynsmyndigheds resultater. De varierer fra ombudsmandslignende henstillinger til afgørelser med omgående retskraft. Når effektiviteten af de retsmidler, der findes inden for et retsområde, analyseres, skal de pågældende retsmidler derfor vurderes inden for deres sammenhæng.

204 Databeskyttelsesdirektivet, artikel 28. Se også konvention 108, tillægsprotokol, artikel 1.

5.3. Retsmidler og sanktioner

Hovedpunkter

- I henhold til konvention 108 og databeskyttelsesdirektivet skal der ved national lov fastsættes passende retsmidler og sanktioner mod krænkelser af retten til databeskyttelse.
  - Retten til et effektivt retsmiddel kræver i medfør af EU-retten, at der ved national lov fastsættes retsmidler mod krænkelser af databeskyttelsesrettigheder, uanset muligheden for at indbringe klager for en tilsynsmyndighed.
  - Der skal ved national lov fastsættes sanktioner, som er effektive, ækvivalente, står i et rimeligt forhold til overtrædelsen og har afskrækkende virkning.
- Inden en sag indbringes for domstolene, skal den forelægges en registeransvarlig. Om det også er obligatorisk at forelægge sagen for en tilsynsmyndighed, inden den indbringes for en domstol, fastsættes ved national lovgivning.
- Registrerede kan som en sidste udvej og på visse betingelser indbringe overtrædelser af databeskyttelseslovgivningen for Menneskerettighedsdomstolen.
- Registrerede kan desuden indbringe sager for EU-Domstolen, men kun i meget begrænset omfang.

Rettigheder i medfør af databeskyttelseslovgivningen kan kun udøves af den person, hvis rettigheder berøres, dvs. den person, som er eller hævder at være den registrerede. Sådanne personer kan ved udøvelsen af deres rettigheder repræsenteres af personer, der opfylder de nødvendige krav i henhold til den nationale lovgivning. Mindreårige skal repræsenteres af deres forældre eller værge. Over for tilsynsmyndighederne kan en person også repræsenteres af sammenslutninger, hvis lovlige formål er at fremme databeskyttelsesrettigheder.

5.3.1. Anmodninger til den registeransvarlige

De rettigheder, der er nævnt i afsnit 3.2, skal først udøves over for den registeransvarlige. Henvendelse til den nationale tilsynsmyndighed eller en domstol hjælper ikke, da myndigheden kun kan oplyse, at vedkommende først skal henvende sig til den registeransvarlige, og domstolen ville erklære et søgsmål for ugyldigt. De formelle krav til en juridisk relevant anmodning til en registeransvarlig, især om den skal fremsættes skriftligt, bør fastsættes ved national lov.

Den enhed, der rettes henvendelse til som registeransvarlig, skal reagere, også selv om vedkommende ikke er den registeransvarlige. Et svar skal under alle omstændigheder gives til den registrerede inden for den tidsfrist, der er fastsat ved national lovgivning, også selv om det kun angiver, at vedkommende ikke behandler nogen oplysninger om den person, der har fremsendt anmodningen. I overensstemmelse med bestemmelserne i databeskyttelsesdirektivets artikel 12, litra a), og artikel 8, litra b), i konvention 108 skal en sådan anmodning imødekommes "uden større ventetid". Der bør ved national lov derfor fastsættes en svarperiode, som er tilstrækkeligt kort, men som giver den registeransvarlige mulighed for at behandle anmodningen korrekt.

Inden anmodningen besvares, skal den enhed, der er rettet henvendelse til som registeransvarlig, kontrollere anmoderens identitet med henblik på at afgøre, om vedkommende faktisk er den, han eller hun påstår at være, og således undgå en alvorlig overtrædelse af tavshedspligten. Hvis kravene vedrørende kontrol af identitet ikke specifikt er omhandlet i den nationale lovgivning, fastlægges de af den registeransvarlige. Princippet om rimelig behandling kræver dog, at den registeransvarlige ikke pålægges alt for byrdefulde krav i forbindelse med bekræftelsen af identiteten (og autenticiteten af anmodningen som omhandlet i afsnit 2.1.1).

Hvorvidt registeransvarlige kan kræve, at anmoderen betaler et gebyr for besvarelsen af anmodninger, skal afgøres i den nationale lovgivning: I henhold til direktivets artikel 12, litra a), og artikel 8, litra b), i konvention 108 skal anmodninger om indsigt besvares "uden større [...] udgifter". I mange europæiske lande skal anmodninger i henhold til databeskyttelseslovgivningen besvares vederlagsfrit, hvis denne besvarelse ikke kræver en uforholdsmæssig og usædvanlig indsats. Til gengæld beskytter den nationale lovgivning normalt registeransvarlige mod misbrug af retten til at få besvaret anmodninger.

Hvis den person, den institution eller det organ, der er rettet henvendelse til som registeransvarlig, ikke afviser at være den registeransvarlige, skal denne enhed inden for den frist, der er fastsat ved national lovgivning:

- acceptere anmodningen og meddele anmoderen, hvordan anmodningen er blevet imødekommet, eller

- meddele anmoderen, hvorfor vedkommendes anmodning ikke imødekommes.

5.3.2. Klager indgivet til tilsynsmyndigheden

Hvis en person, som har indgivet en anmodning om indsigt eller har gjort indsigelse til en registeransvarlig, ikke modtager et svar, som er rettidigt og tilfredsstillende, kan den pågældende henvende sig til den nationale databeskyttelsesmyndighed med krav om assistance. Mens klagesagen behandles af tilsynsmyndigheden, skal det afklares, om den person, den institution eller det organ, anmoderen henvendte sig til, rent faktisk var forpligtet til at reagere på anmodningen, og om reaktionen var korrekt og tilstrækkelig. Den pågældende person skal underrettes af tilsynsmyndigheden om resultatet af klagesagen[205]. De retlige virkninger af resultatet af klagesagen ved de nationale tilsynsmyndigheder afhænger af den nationale lovgivning, dvs. om myndighedens afgørelser har retskraft og således kan håndhæves af myndighederne, eller om sagen skal indbringes for en domstol, hvis den registeransvarlige ikke følger tilsynsmyndighedens afgørelser (udtalelse, advarsel osv.).

Hvis de databeskyttelsesrettigheder, der er garanteret ved artikel 16 i TEUF, angiveligt krænkes af EU-institutioner eller -organer, kan den registrerede indgive en klage til EDPS[206], den uafhængige tilsynsførende for databeskyttelse i henhold til forordningen om databeskyttelse inden for EU-institutionerne, som fastlægger den tilsynsførendes pligter og beføjelser. Undlader den tilsynsførende at svare inden udløbet af fristen på seks måneder, er dette at sidestille med en afgørelse om afvisning af klagen.

Afgørelser truffet af en national tilsynsmyndighed skal kunne appelleres til domstolene. Dette gælder for både den registrerede og den registeransvarlige, som har været part i klagesagen ved en tilsynsmyndighed.

Eksempel: Det Forenede Kongeriges datatilsynsmyndighed (Information Commissioner) udstedte den 24. juli 2013 en afgørelse, der pålagde politiet i Hertfordshire at stoppe brugen af et system til sporing af nummerplader, som efter myndighedens vurdering var ulovligt. Data indsamlet med kamera blev lagret hos det lokale politi og i en central database. Fotos af nummerplader blev opbevaret i to år, og fotos af biler blev opbevaret i 90 dage. Myndigheden afgjorde, at en så omfattende brug af kameraer og andre former for overvågning ikke stod i forhold til det problem, man søgte at løse.

205 Databeskyttelsesdirektivet, artikel 28, stk. 4.

206 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 2001 L 8.

5.3.3. Klage indbragt for en domstol

Hvis den person, der har fremsat en anmodning til en registeransvarlig i medfør af databeskyttelseslovgivningen, ikke er tilfreds med den registeransvarliges svar, skal denne person have ret til at indbringe en klage for en national domstol[207].

Om det er obligatorisk først at forelægge sagen for en tilsynsmyndighed, inden den indbringes for en domstol, fastsættes ved national lovgivning. I de fleste tilfælde vil det dog være mest fordelagtigt for personer, der udøver deres databeskyttelsesrettigheder, først at forelægge sagen for tilsynsmyndigheden, da klagesager med krav om deres assistance bør være ubureaukratiske og vederlagsfrie. Den ekspertise, der dokumenteres i tilsynsmyndighedens afgørelse (udtalelse, advarsel osv.), kan også hjælpe den registrerede med at udøve sine rettigheder ved domstolene.

I henhold til Europarådets retsorden kan krænkelser af databeskyttelsesrettigheder, der angiveligt er begået på nationalt plan af en kontraherende part i den europæiske menneskerettighedskonvention, og som samtidig udgør en overtrædelse af artikel 8 i den europæiske menneskerettighedskonvention, desuden indbringes for Menneskerettighedsdomstolen, når alle de tilgængelige nationale retsmidler er udtømte. For at en påstand om overtrædelse af artikel 8 i EMK kan indbringes for Menneskerettighedsdomstolen, skal andre antagelighedskriterier (artikel 34-37 i EMK) også opfyldes[208].

Selv om anmodninger til Menneskerettighedsdomstolen kun kan rettes til kontraherende parter, kan de indirekte vedrøre private parters handlinger eller manglende handling, for så vidt som en kontraherende part ikke har opfyldt sine positive forpligtelser i medfør af den europæiske menneskerettighedskonvention og ikke har ydet tilstrækkelig beskyttelse mod krænkelser af databeskyttelsesrettigheder i sin nationale lovgivning.

Eksempel: I sagen *K.U. mod Finland*[209] 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 med henvisning til

207 Databeskyttelsesdirektivet, artikel 22.

208 Den europæiske menneskerettighedskonvention, artikel 34-37, findes på: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 Menneskerettighedsdomstolen, *K.U. mod Finland*, nr. 2872/02, 2. december 2009.

vedkommendes 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. Menneskerettighedsdomstolen fastslog, at stater ikke kun havde pligt til at afstå fra 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 den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Eksempel: I sagen *Köpke mod Tyskland*[210] havde sagsøgeren været under mistanke for tyveri på sin arbejdsplads og havde derfor været udsat for skjult videoovervågning. Menneskerettighedsdomstolen konkluderede, at der ikke var 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 Menneskerettighedsdomstolen finder, at en stat har krænket rettigheder, der er beskyttet af den europæiske menneskerettighedskonvention, er den pågældende stat forpligtet til at fuldbyrde Menneskerettighedsdomstolens dom. 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 lignende krænkelser, enten i form af lovændring, ændring af retspraksis eller andre foranstaltninger.

Hvis Menneskerettighedsdomstolen afsiger dom om en overtrædelse af den europæiske menneskerettighedskonvention, kan den i henhold til konventionens artikel 41 pålægge staten at betale passende erstatning til sagsøgeren.

210 Menneskerettighedsdomstolen, *Köpke mod Tyskland* (dec.), nr. 420/07, 5. oktober 2010.

I EU-retten[211] kan ofre for overtrædelser af den nationale databeskyttelseslovgivning, som gennemfører EU's databeskyttelseslovgivning, i nogle tilfælde indbringe deres sager for EU-Domstolen. En registrerets påstand om krænkelse af vedkommendes databeskyttelsesrettigheder kan indbringes for EU-Domstolen under to scenarier.

I det første scenario skal den registrerede være direkte offer for en administrativ eller regelfastsættende EU-retsakt, som krænker en persons ret til databeskyttelse. I artikel 263, stk. 4, i TEUF, fastsættes følgende:

> *"Enhver fysisk eller juridisk person kan [...] indbringe klage med henblik på prøvelse af retsakter, der er rettet til vedkommende, eller som berører denne umiddelbart og individuelt, samt af regelfastsættende retsakter, der berører vedkommende umiddelbart, og som ikke omfatter gennemførelsesforanstaltninger."*

Ofre for et EU-organs ulovlige behandling af deres personoplysninger kan således klage direkte til Retten under EU-Domstolen, som har kompetence til at afgøre sager vedrørende forordningen om databeskyttelse inden for EU-institutionerne En person, hvis retlige situation berøres direkte af en EU-retlig bestemmelse, kan også klage direkte til EU-Domstolen.

Det andet scenario vedrører EU-Domstolens kompetence til at træffe præjudicielle afgørelser i medfør af artikel 267 i TEUF.

Under den nationale sagsbehandling kan registrerede anmode den nationale domstol om at anmode EU-Domstolen om afklaring af fortolkningen af EU-traktaterne og om fortolkningen og gyldigheden af handlinger fra EU-institutioner, -organer, -kontorer eller -agenturer. Sådanne afklaringer kaldes præjudicielle afgørelser. Det er ikke et direkte retsmiddel for klageren, men det giver de nationale domstole mulighed for at sikre, at de anvender den korrekte fortolkning af EU-retten.

Hvis en part i sagen for de nationale domstole anmoder om, at et spørgsmål forelægges EU-Domstolen, har kun nationale domstole i sidste instans, hvis afgørelser ikke kan appelleres, pligt til at imødekomme dette.

---

211 EU (2007), Lissabontraktaten om ændring af traktaten om Den Europæiske Union og traktaten om oprettelse af Det Europæiske Fællesskab, underskrevet i Lissabon den 13. december 2007, EUT 2007 C 306. Se også de konsoliderede udgaver af traktaten om Den Europæiske Union (TEU) og traktaten om Den Europæiske Unions funktionsmåde (TEUF), EUT 2012 C 326.

Eksempel: I sagen *Kärntner Landesregierung m.fl.*[212] har den østrigske forfatningsdomstol forelagt spørgsmål for EU-Domstolen vedrørende gyldigheden af artikel 3-9 i direktiv 2006/24/EF (*datalagringsdirektivet*) i lyset af chartrets artikel 7, 9 og 11, og om visse bestemmelser i den østrigske forbundslov om telekommunikation, som gennemfører datalagringsdirektivet, var forenelige med aspekter af databeskyttelsesdirektivet og forordningen om databeskyttelse inden for EU-institutionerne.

Michael Seitlinger, en af sagsøgerne i hovedsagen ved forfatningsdomstolen, har påstået, at han anvender telefonen, internettet og e-mail til både arbejdsformål og private formål. De oplysninger, han sender og modtager, passerer 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 fremfører, at denne indsamling og lagring af hans personoplysninger på ingen måde er teknisk nødvendig for at få informationerne fra A til B på 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 af alle disse ekstra oplysninger var den østrigske telekommunikationslov fra 2003.

Michael Seitlinger anlagde derfor sag mod den østrigske forfatningsdomstol med påstand om, at de lovfæstede forpligtelser, der var pålagt hans telekommunikationsudbyder, krænkede hans grundlæggende rettigheder sikret ved artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder.

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.

EU-Domstolen skal principielt besvare de spørgsmål, den forelægges. Den kan ikke afvise at træffe en præjudiciel afgørelse med den begrundelse, at svaret ikke vil være relevant eller aktuelt, for så vidt angår hovedsagen. Den kan dog afvise at træffe afgørelse, hvis spørgsmålet ikke er inden for dens kompetenceområde.

212 EU-Domstolen, Forenede sager C-293/12 og C-594/12, *Digital Rights Ireland og Seitling og andre*, 8. april 2014

Hvis databeskyttelsesrettigheder, som er garanteret ved artikel 16 i TEUF, angiveligt krænkes af en EU-institution eller et EU-organ under behandlingen af personoplysninger, kan den registrerede indbringe sagen for Retten (artikel 32, stk. 1 og 4, i forordningen om databeskyttelse inden for EU-institutionerne). Det samme gælder for Den Europæiske Tilsynsførendes afgørelser vedrørende sådanne krænkelser (artikel 32, stk. 3, i forordningen om databeskyttelse inden for EU-institutionerne).

Retten har kompetence til at træffe afgørelse i sager vedrørende forordningen om databeskyttelse inden for EU-institutionerne. Hvis en person som ansat ved en EU-institution eller et EU-organ ønsker adgang til et retsmiddel, skal denne person dog klage til EU-Personaleretten.

Eksempel: Sagen *Europa-Kommissionen mod The Bavarian Lager Co. Ltd*[213] illustrerer de retsmidler, der er til rådighed mod EU-institutioners eller -organers handlinger eller afgørelser med betydning for databeskyttelse.

Bavarian Lager anmodede 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[214]. Med henvisning til artikel 32 i forordningen om databeskyttelse inden for EU-institutionerne indbragte Bavarian Lager denne beslutning for EU-Domstolen, nærmere Retten i Første Instans (forgængeren for Retten). I sin afgørelse i sag T-194/04, *Bavarian Lager mod Europa-Kommissionen*, 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 Kommissionens afvisning af anmodningen om indsigt.

5.3.4. Sanktioner

I Europarådets retsorden fastsætter artikel 10 i konvention 108, at hver part skal indføre passende sanktioner og retsmidler for overtrædelser af bestemmelser i den nationale lovgivning, som gennemfører de grundlæggende principper om

213 EU-Domstolen, C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd*, 29. juni 2010.

214 En analyse af sagen findes i: EDPS (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling*, Bruxelles, den EDPS, på: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

databeskyttelse, der er fastsat ved konvention 108[215]. **I EU-retten** fastsætter databeskyttelsesdirektivets artikel 24, at medlemsstaterne "træffer de nødvendige foranstaltninger til at sikre, at dette direktiv gennemføres i fuldt omfang, og de fastsætter bl.a. de sanktioner, der skal finde anvendelse i tilfælde af overtrædelse af de bestemmelser, der vedtages […]".

Begge instrumenter giver medlemsstaterne brede muligheder for skøn, når de skal vælge passende sanktioner og retsmidler. Ingen af de retlige instrumenter uddyber karakteren eller typen af passende sanktioner, og de giver heller ikke eksempler på sanktioner.

Følgende gør sig dog gældende:

> *Selvom EU's medlemsstater skønsbeføjelser med hensyn til valget af de foranstaltninger, der er mest hensigtsmæssige med henblik på at sikre de rettigheder, som personer opnår i kraft af EU-retten, jf. princippet om loyalt samarbejde, der er fastlagt ved artikel 4, stk. 3, i TEU, skal minimumskravene til effektivitet, ensartethed, proportionalitet og afskrækkende virkning overholdes*[216].

EU-Domstolen har gentagne gange fastholdt, at medlemsstaterne ikke frit kan fastlægge sanktioner ved national lov.

Eksempel: I sagen *Von Colson og Kamann mod Land Nordrhein-Westfalen*[217] påpegede EU-Domstolen, at alle de medlemsstater, som et direktiv er rettet til, har pligt til i deres respektive retssystemer at træffe alle nødvendige foranstaltninger til at sikre dets fulde virkning i overensstemmelse med dets mål. Uanset at det overlades til medlemsstaterne at fastlægge de fremgangmåder og midler, der skal sikre direktivets gennemførelse, fastslog Domstolen, at denne frihed ikke påvirker den forpligtelse, de pålægges. Et effektivt retsmiddel skal navnlig sætte en person i stand til fuldt ud at forfølge og håndhæve den omhandlede ret. For at opnå denne ægte og effektive beskyttelse skal rets-

215 Menneskerettighedsdomstolen, *I. mod Finland*, nr. 20511/03, 17. juli 2008, Menneskerettighedsdomstolen, *K.U. mod Finland*, nr. 2872/02, 2. december 2008.

216 Den Europæiske Unions Agentur for Grundlæggende Rettigheder (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, 2/2012*, Wien, 1. oktober 2012, s. 27.

217 EU-Domstolen, C-14/83, *Sabine von Colson og Elisabeth Kamann mod Land Nordrhein-Westfalen*, 10. april 1983

midler udløse strafferetlige og/eller kompensatoriske procedurer, som fører til sanktioner med afskrækkende virkninger.

For så vidt angår sanktioner mod EU-institutioners eller -organers overtrædelse af EU-retten, betyder det særlige anvendelsesområde for forordningen om databeskyttelse inden for EU-institutionerne, at sanktioner alene har form af disciplinære sanktioner. I forordningens artikel 49 anføres følgende: "Der kan 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 […]".

6

Grænseoverskridende overførsel af oplysninger

EU	Omhandlede emner	Europarådet
Grænseoverskridende dataudveksling		
Databeskyttelsesdirektivet, artikel 25, stk. 1 EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003	Definition	Konvention 108, tillægsprotokol, artikel 2, stk. 1
Fri dataudveksling		
Databeskyttelsesdirektivet, artikel 1, stk. 2	Mellem EU's medlemsstater	
	Mellem kontraherende parter i konvention 108	Konvention 108, artikel 12, stk. 2
Databeskyttelsesdirektivet, artikel 25	Til tredjelande med et tilstrækkeligt beskyttelsesniveau	Konvention 108, tillægsprotokol, artikel 2, stk. 1
Databeskyttelsesdirektivet, artikel 26, stk. 1	Til tredjelande i særlige tilfælde	Konvention 108, tillægsprotokol, artikel 2, stk. 2, litra a)
Begrænset videregivelse af oplysninger til tredjelande		
Databeskyttelsesdirektivet, artikel 26, stk. 2 Databeskyttelsesdirektivet, artikel 26, stk. 4	Kontraktbestemmelser	Konvention 108, tillægsprotokol, artikel 2, stk. 2, litra b) Vejledning i udarbejdelse af kontraktbestemmelser
Databeskyttelsesdirektivet, artikel 26, stk. 2	Bindende virksomhedsregler (BCR)	
Eksempler: EU-USA PNR-aftale EU-USA SWIFT-aftale	Særlige internationale aftaler	

Databeskyttelsesdirektivet omhandler ikke kun fri overførsel af data mellem medlemsstaterne, men indeholder også bestemmelser om kravene i forbindelse med overførsel af personoplysninger til tredjelande. Europarådet anerkendte også betydningen af gennemførelsesbestemmelser for grænseoverskridende overførsel af oplysninger til tredjelande og vedtog i 2001 tillægsprotokollen til konvention 108. Denne protokol overtog de væsentligste bestemmelser om overførsel af oplysninger fra parter i konventionen og EU's medlemsstater.

6.1. Arten af grænseoverskridende overførsel af oplysninger

Hovedpunkter

- Grænseoverskridende overførsel af oplysninger er overførsel af personoplysninger til en modtager, der er underlagt udenlandsk jurisdiktion.

I artikel 2, stk. 1, i tillægsprotokollen til konvention 108 beskrives grænseoverskridende overførsel af oplysninger som overførsel af personoplysninger til en modtager, der er underlagt udenlandsk jurisdiktion. Databeskyttelsesdirektivets artikel 25, stk. 1, omhandler "overførsel til et tredjeland af personoplysninger, der gøres til genstand for behandling, eller som skal gøres til genstand for behandling efter overførsel […]". Sådan overførsel af oplysninger er kun tilladt i henhold til de regler, der er fastlagt i artikel 2 i tillægsprotokollen til konvention 108 og, for EU's medlemsstater, desuden i henhold til databeskyttelsesdirektivets artikel 25 og 26.

Eksempel: I sagen *Bodil Lindqvist*[218] fastslog EU-Domstolen, 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".

218 EU-Domstolen, C-101/01, *Bodil Lindqvist*, 6. november 2003, præmis 27, 68 og 69.

Domstolen påpegede på daværende tidspunkt, at direktivet også fastlægger specifikke regler, der tillader medlemsstaterne at overvåge overførsel af personoplysninger til tredjelande.

Når der henses dels til internettets udviklingstrin på tidspunktet for udarbejdelsen af direktivet, dels til de manglende kriterier for anvendelsen af internettet i direktivet, "kan det ikke formodes, at fællesskabslovgiver har tilsigtet, at begrebet 'overførsel til et tredjeland af personoplysninger' fremtidigt skulle omfatte en sådan situation, hvor der lægges oplysninger ud på en internetside, selv om disse således er blevet gjort tilgængelige for personer i tredjelande, der har de tekniske muligheder for at få adgang hertil".

Såfremt direktivet "blev fortolket således, at der foreligger en 'overførsel til et tredjeland af personoplysninger', hver gang personoplysninger lægges ud på en internetside, vil denne overførsel nødvendigvis være en overførsel til alle de tredjelande, hvor der findes de nødvendige tekniske muligheder for at få adgang til internettet. Den særlige ordning i [direktivet] bliver derfor nødvendigvis, med hensyn til operationer på internettet, en ordning, der generelt finder anvendelse. Konstaterer Kommissionen [...], at blot et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau, er medlemsstaterne nemlig forpligtet til at hindre, at personoplysningerne lægges ud på internettet".

Princippet om, at offentliggørelse af oplysninger alene ikke er nok til at blive betragtet som grænseoverskridende overførsel af oplysninger, gælder også for offentlige registre og massemedier, som f.eks. (elektroniske) aviser og tv. Kun kommunikation, der er rettet til specifikke modtagere, hører ind under begrebet "grænseoverskridende overførsel af oplysninger".

6.2. Fri overførsel af oplysninger mellem medlemsstater eller mellem kontraherende parter

Hovedpunkter

- overførsel af personoplysninger til en anden medlemsstat i Det Europæiske Økonomiske Samarbejdsområde eller til en anden kontraherende part i konvention 108 skal være fri af begrænsninger.

I henhold til artikel 12, stk. 2, i konvention 108 skal der **inden for Europarådets retsorden** være fri overførsel af personoplysninger mellem parterne i konventionen. National lovgivning må ikke begrænse eksporten af personoplysninger til en kontraherende part, medmindre:

- oplysningernes særlige art kræver det[219], eller
- begrænsningen er nødvendig for at undgå omgåelse af nationale bestemmelser om grænseoverskridende dataoverførsel til tredjemand[220].

I EU-retten er begrænsninger af eller forbud mod fri overførsel af oplysninger mellem medlemsstaterne af hensyn til databeskyttelse forbudt i henhold til databeskyttelsesdirektivets artikel 1, stk. 2. Området for fri overførsel af oplysninger er udvidet ved aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS)[221], som bringer Island, Liechtenstein og Norge ind 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.

Hvis det samme slovenske selskab ønsker at overføre de samme personoplysninger til moderselskabet i USA, skal den slovenske dataeksportør gennemføre de procedurer, der er fastlagt ved slovensk lov for grænseoverskridende dataoverførsel til tredjelande, medmindre moderselskabet har tilsluttet sig safe harbor-principperne, en frivillig adfærdskodeks for sikring af et tilstrækkeligt databeskyttelsesniveau (se afsnit 6.3.1).

Grænseoverskridende overførsel af oplysninger til EØS-medlemsstater til formål, der ligger uden for hensigten med det indre marked, f.eks. efterforskning af kriminalitet, er dog ikke omfattet af databeskyttelsesdirektivets bestemmelser og er derfor ikke omfattet af princippet om fri overførsel af oplysninger. Hvad angår Europarådets retsorden, er alle områder omfattet af anvendelsesområdet for konvention 108 og

219 Konvention 108, artikel 12, stk. 3, litra a).

220 *Ibid.*, artikel 12, stk. 3, litra b).

221 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 1994 L 1.

tillægsprotokollen til konvention 108, selv om de kontraherende parter kan vedtage undtagelser. Alle medlemmer af EØS er også parter i konvention 108.

6.3. Fri overførsel af oplysninger til tredjelande

Hovedpunkter

- overførsel af personoplysninger til tredjelande skal være tilladt uden begrænsninger i medfør af national databeskyttelseslovgivning, hvis:
  - det er bekræftet, at modtageren garanterer tilstrækkelig databeskyttelse, eller
  - det er nødvendigt af hensyn til den registreredes særlige interesser eller andres legitime interesser, der går forud herfor, især vigtige samfundsinteresser.
- Databeskyttelsen i et tredjeland er tilstrækkelig, hvis hovedprincipperne for databeskyttelse er blevet gennemført effektivt i landets nationale lovgivning.
- Inden for EU-retten vurderes tilstrækkeligheden af et tredjelands databeskyttelse af Europa-Kommissionen. I Europarådets retsorden overlades det til den nationale lovgivning at regulere, hvordan tilstrækkelighed vurderes.

6.3.1. Fri overførsel af oplysninger som følge af tilstrækkelig beskyttelse

I henhold til **Europarådets retsorden** kan den nationale lovgivning tillade fri overførsel af oplysninger til ikke kontraherende stater, hvis den modtagende stat eller organisation sikrer et tilstrækkeligt beskyttelsesniveau i forbindelse med den planlagte overførsel af oplysninger[222]. Den nationale lovgivning fastsætter, hvordan databeskyttelsesniveauet i et andet land vurderes, og hvem der foretager vurderingen.

I EU-retten er fri overførsel af oplysninger til tredjelande med tilstrækkelig databeskyttelse omhandlet i databeskyttelsesdirektivets artikel 25, stk. 1. Kravet om tilstrækkelighed i stedet for ækvivalens betyder, at der kan tages højde for forskellige gennemførelser af databeskyttelse. I henhold til direktivets artikel 25, stk. 6, kan Kommissionen fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. I

222 Konvention 108, tillægsprotokol, artikel 2, stk. 1.

den forbindelse rådfører den sig med Artikel 29-Gruppen, som i høj grad har bidraget til fortolkningen af artikel 25 og 26[223].

Kommissionens vurdering af tilstrækkelighed har bindende virkninger. Hvis Kommissionen offentliggør en vurdering af tilstrækkelighed i Den Europæiske Unions Tidende, er alle medlemslande af EØS og deres organer forpligtede til at følge denne afgørelse. Det betyder, at data kan overføres til dette land uden krav om kontrol- eller godkendelsesprocedurer fra de nationale myndigheders side[224].

Kommissionen kan også vurdere dele af et lands retssystem eller begrænse sig til enkelte emner. Kommissionen har f.eks. foretaget en tilstrækkelighedsvurdering udelukkende af Canadas handelsret[225]. Der er også foretaget en række tilstrækkelighedsvurderinger af overførsler baseret på aftaler mellem EU og tredjelande. Disse vurderinger vedrører udelukkende én type dataoverførsel, f.eks. flyselskabers overførsel af PNR-oplysninger til udenlandske grænsekontrolmyndigheder, når flyselskabet flyver fra EU til bestemte oversøiske destinationer (se afsnit 6.4.3). Nyere praksis for dataoverførsel baseret på særlige aftaler mellem EU og tredjelande afhjælper generelt behovet for tilstrækkelighedsvurderinger, idet det antages, at aftalen i sig selv sikrer et tilstrækkeligt databeskyttelsesniveau[226].

En af de vigtigste afgørelser om tilstrækkelighed vedrører faktisk ikke et sæt retsbestemmelser[227]. Den vedrører i stedet et sæt regler eller en adfærdskodeks, der

223 Se eksempelvis Artikel 29-Gruppen (2003), *arbejdsdokument om videregivelse af personoplysninger til tredjelande: anvendelse af databeskyttelsesdirektivets artikel 26, stk. 2, på bindende virksomhedsregler ved internationale dataoverførsler*, WP 74, Bruxelles, den 3. juni 2003, og 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, den 25. november 2005.

224 En ajourført liste over lande, hvis databeskyttelsesniveau er tilstrækkeligt, findes på webstedet for Kommissionens Generaldirektorat for Retlige Anliggender på: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 Kommissionens 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 2002 L 2.

226 Aftale mellem Amerikas Forenede Stater og Den Europæiske Union om anvendelse og overførsel af passagerlisteoplysninger til United States Department of Homeland Security (EUT 2012 L 215, s. 5-14) eller aftale 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 2010 L 8, s. 11-16.

227 Europa-Kommissionen (2000), Kommissionens beslutning 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 harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium, EFT 2000 L 215.

kaldes safe harbor-principperne til beskyttelse af privatlivets fred. Disse principper er udarbejdet i samarbejde mellem EU og US til brug for amerikanske virksomheder. Medlemskab af safe harbor opnås ved afgivelse af en frivillig erklæring til det amerikanske handelsministerium og dokumenteres på en liste, der offentliggøres af dette ministerium. Eftersom et af de vigtigste elementer af tilstrækkelighed er, at databeskyttelse gennemføres effektivt, omhandler safe harbor-ordningen også et vist omfang af statsligt tilsyn. Kun virksomheder, der er underlagt US-FTC's (Federal Trade Commission) tilsyn, kan deltage i safe harbor.

6.3.2. Fri videregivelse af oplysninger i særlige tilfælde

Inden for **Europarådets retsorden** tillader artikel 2, stk. 2, i tillægsprotokollen til konvention 108, at personoplysninger overføres til tredjelande uden tilstrækkelig databeskyttelse, hvis overførslen er tilladt i henhold til national lovgivning og er nødvendig af hensyn til:

- den registreredes specifikke interesser eller
- andres legitime interesser, navnlig vigtige samfundsinteresser, der går forud herfor.

I EU-retten indeholder databeskyttelsesdirektivets artikel 26, stk. 1, bestemmelser svarende til bestemmelserne i tillægsprotokollen til konvention 108.

I henhold til direktivet kan den registreredes interesser begrunde fri overførsel af oplysninger til et tredjeland, hvis:

- der ikke hersker tvivl om, at den registrerede har givet sit samtykke til overførslen, eller
- den registrerede indgår – eller forbereder at indgå – et kontraktligt forhold, der klart kræver, at oplysningerne overføres til en modtager i et tredjeland, eller
- der er indgået en kontrakt mellem en registeransvarlig og en tredjemand af hensyn til den registrerede, eller
- overførslen er nødvendig for at beskytte den registreredes vitale interesser

- der er tale om overførsel af oplysninger fra offentlige registre (her kan samfundsinteresser, der går forud for databeskyttelse, begrunde indsigt i information, der er lagret i offentlige registre).

Andres legitime interesser[228] kan begrunde fri grænseoverskridende overførsel af oplysninger:

- af hensyn til vigtige samfundsmæssige interesser, bortset fra forhold vedrørende national eller offentlig sikkerhed, da de ikke er omfattet af databeskyttelsesdirektivet, eller

- for at et retskrav kan fastslås, gøres gældende eller forsvares ved en domstol.

De tilfælde, der er nævnt ovenfor, skal forstås som undtagelser fra reglen om, at uhindret overførsel af oplysninger til tredjelande kræver et tilstrækkeligt databeskyttelsesniveau i modtagerlandet. Undtagelser skal altid fortolkes restriktivt. Artikel 29-Gruppen har understreget dette gentagne gange i forbindelse med databeskyttelsesdirektivets artikel 26, stk. 1, især hvis samtykke hævdes at være grundlaget for overførsel af oplysninger[229]. Artikel 29-Gruppen har konkluderet, at de generelle regler vedrørende den retlige betydning af samtykke også gælder for direktivets artikel 26, stk. 1. Hvis det inden for rammerne af f.eks. ansættelsesforhold er uklart, at det samtykke, arbejdstagerne har givet, faktisk var frivilligt, kan overførsel af oplysninger ikke ske på grundlag af direktivets artikel 26, stk. 1, litra a). I sådanne tilfælde finder artikel 26, stk. 2, som kræver, at de nationale databeskyttelsesmyndigheder udsteder en tilladelse til overførsel af oplysninger, anvendelse.

6.4. Begrænset overførsel af oplysninger til tredjelande

Hovedpunkter

- Inden eksport af data til tredjelande, som ikke garanterer et tilstrækkeligt databeskyttelsesniveau, kan den registeransvarlige være forpligtet til at forelægge den planlagte overførsel for tilsynsmyndigheden.

228 Databeskyttelsesdirektivet, artikel 26, stk. 1, litra d).

229 Se navnlig 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, den 25. november 2005.

- Den registeransvarlige, der ønsker at eksportere data, skal påvise to forhold under denne undersøgelse:
  - at der findes et retsgrundlag for overførslen af oplysninger til modtageren
  - at der er truffet foranstaltninger for at sikre tilstrækkelig beskyttelse af oplysningerne hos modtageren.
- Foranstaltninger til sikring af tilstrækkelig databeskyttelse hos modtageren kan omfatte:
  - kontraktbestemmelser mellem den dataeksporterende (registeransvarlige) og den udenlandske modtager eller
  - bindende virksomhedsregler (BCR), som normalt gælder for overførsler af oplysninger inden for multinationale koncerner.
- Overførsler af oplysninger til udenlandske myndigheder kan også være underlagt en særlig international aftale.

I henhold til databeskyttelsesdirektivet og tillægsprotokollen til konvention 108 kan der ved national lov fastsættes ordninger for grænseoverskridende overførsel af oplysninger til tredjelande, som ikke garanterer et tilstrækkeligt databeskyttelsesniveau, hvis den registeransvarlige har truffet særlige forholdsregler for at sikre tilstrækkelige garantier for databeskyttelse hos modtageren, og hvis den registeransvarlige kan dokumentere dette over for en kompetent myndighed. Dette krav nævnes kun udtrykkeligt i tillægsprotokollen til konvention 108, men det betragtes også som standardprocedure ifølge databeskyttelsesdirektivet.

6.4.1. Kontraktbestemmelser

Både **Europarådets retsorden** og **EU-retten** nævner kontraktbestemmelser mellem den dataeksporterende (registeransvarlige) og modtageren i tredjelandet som en mulig metode til at garantere et tilstrækkeligt databeskyttelsesniveau hos modtageren.

På **EU-plan** har Europa-Kommissionen med bistand fra Artikel 29-Gruppen udviklet standardkontraktbestemmelser, der er officielt certificeret ved en kommissionsafgørelse som bevis for tilstrækkelig databeskyttelse[230]. Da Kommissionens afgørelser er bindende i deres helhed for medlemsstaterne, skal de nationale myndigheder, der er ansvarlige for tilsynet med grænseoverskridende overførsler af oplysninger,

230 Databeskyttelsesdirektivet, artikel 26, stk. 4.

anerkende disse standardkontraktbestemmelser i deres procedurer[231]. Hvis den dataeksporterende (registeransvarlige) og modtageren i tredjelandet når til enighed og underskriver disse bestemmelser, bør tilsynsmyndigheden acceptere dette som dokumentation for, at der gives tilstrækkelige garantier.

Sådanne standardkontraktbestemmelser inden for EU-retten betyder ikke, at registeransvarlige ikke må udarbejde andre ad hoc-kontraktbestemmelser. De skal dog sikre samme beskyttelsesniveau som standardkontraktbestemmelserne. De vigtigste kendetegn ved standardkontraktbestemmelserne er følgende:

- Der foreligger et tredjepartsløfte, som sætter den registrerede i stand til at udøve kontraktlige rettigheder, selv om de ikke er part i kontrakten.

- Modtageren eller importøren af oplysninger accepterer at være underlagt den procedure, der er fastlagt af den nationale tilsynsmyndighed og/eller domstole for den dataeksporterende (registeransvarlige).

Der er nu to sæt standardbestemmelser for overførsler fra registeransvarlig til registeransvarlig, som den dataeksporterende (registeransvarlig) kan vælge mellem[232]. For overførsler fra registeransvarlig til registerfører findes der kun ét sæt standardkontraktbestemmelser[233].

Inden for rammerne af **Europarådets retsorden** har det rådgivende udvalg vedrørende konvention 108 udarbejdet en vejledning i udarbejdelse af kontraktbestemmelser[234].

231 TEUF, artikel 288.

232 Sæt I findes i bilaget til Kommissionens beslutning 2001/497/EF af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF, EFT 2001 L 181. Sæt II findes i bilaget til 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 2004 L 385.

233 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 2010 L 39.

234 Europarådet, rådgivende udvalg vedrørende konvention 108 (2002), *Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data*.

6.4.2. Bindende virksomhedsregler (Binding Corporate Rules BCR)

Multilaterale bindende virksomhedsregler (BCR) omfatter meget ofte flere europæiske databeskyttelsesmyndigheder samtidig[235]. For at bindende virksomhedsregler kan blive godkendt, skal udkastet til reglerne forelægges hovedmyndigheden sammen med de standardiserede ansøgningsformularer[236]. Hovedmyndigheden er anført på den standardiserede ansøgningsformular. Denne myndighed underretter derefter alle tilsynsmyndighederne i de EØS-lande, hvor koncernens selskaber er etableret, selv om det er frivilligt, om de vil deltage i evalueringen af de bindende virksomhedsregler. Selv om det ikke er bindende, bør alle de berørte databeskyttelsesmyndigheder indarbejde resultatet af evalueringen i deres formelle godkendelsesprocedurer.

6.4.3. Særlige internationale aftaler

EU har indgået særlige aftaler vedrørende to typer dataoverførsler:

PNR-oplysninger (Passenger Name Records)

PNR-oplysninger indsamles af flyselskaber under reservationen og omfatter flypassagerernes navne, adresser, kreditkortoplysninger og flysæde. Ifølge amerikansk lovgivning har flyselskaberne pligt til at stille disse oplysninger til rådighed for United States Department of Homeland Security inden flyets afgang. Det gælder for flyvninger til eller fra USA.

235 Indholdet og strukturen af passende bindende virksomhedsregler er forklaret i Artikel 29-Gruppens arbejdsdokument fra 2008 om oprettelse af en ramme for bindende virksomhedsregler (*Working document setting up a framework for the structure of Binding Corporate Rules*), WP 154, Bruxelles, den 24. juni 2008, og i Artikel 29-Gruppens arbejdsdokument fra 2008 om oprettelse af en tabel over de elementer og principper, der skal indgå i bindende virksomhedsregler fra (*Working document setting up a table with the elements and principles to be found in Binding Corporate Rules*), WP 153, Bruxelles, den 24. juni 2008.

236 Artikel 29-Gruppens *anbefaling 1/2007 om standardansøgningen om godkendelse af bindende virksomhedsregler for videregivelse af personoplysninger*, WP 133, Bruxelles, den 10. januar 2007.

Der blev i 2004 vedtaget en PNR-aftale[237], for at sikre en tilstrækkelig beskyttelse af PNR Data i henhold til bestemmelserne i direktivet 95/46/EU. Pakken indeholdte tilstrækkelig beskyttelse af behandling af personoplysninger foretaget af US Department of Homeland Security (DSH)).

Der blev efter PNR-aftalens[238] annullering af CJEU underskrevet to separate aftalte med to forskellige formål) De udgør for det første et retsgrundlag for overførsel af PNR-oplysninger til de US myndigheder, og de sikrer for det andet tilstrækkelig databeskyttelse i modtagerlandet.

Den første aftale om, hvordan oplysninger deles og forvaltes mellem landene blev underskrevet i 2012. Der var flere mangler ved denne aftale, og den blev samme år erstattet med en ny aftale, som styrker retssikkerheden[239]. Den nye aftale omfatter betydelige forbedringer. Den begrænser og præciserer de formål, oplysningerne må anvendes til, som f.eks. efterforskning af alvorlig grænseoverskridende kriminalitet og terrorisme, og etableret perioden for, hvor længe data må behandles, samt at data skal anonymiseres efter seks måneder. Hvis borgeres oplysninger misbruges, har de effektiv administrativ klageadgang og adgang til domstolsprøvelse i overensstemmelse med amerikansk lov. De har også ret til indsigt i deres egne PNR-oplysninger og til at anmode US Department of Homeland Security om berigtigelse, herunder sletning, hvis oplysningerne er urigtige.

Aftalen, som trådte i kraft den 1. juli 2012, er gyldig i syv år indtil 2019.

237 Rådets afgørelse 2004/496/EF af 17. maj 2004 om indgåelse af en aftale mellem Det Europæiske Fællesskab og Amerikas Forenede Stater om luftfartsselskabers behandling og overførsel af PNR-oplysninger til United States Department of Homeland Security, Bureau of Customs and Border Protection, EUT 2004 183, s. 83 og Kommissionens beslutning 2004/535/EF af 14. maj 2004 om tilstrækkelig beskyttelse af personoplysninger, der er indeholdt i registre over flypassagerer, og som videregives til Amerikas Forenede Staters told- og grænsekontrolmyndighed (Bureau of Customs and Border Protection), EUT 2004 L 235, s. 11–22.

238 EU-Domstolen, Forenede sager C-317/04 og C-318/04, *Europa-Parlamentet mod Rådet for Den Europæiske Union* og Kommissionen for De Europæiske Fællesskaber, 30. maj 2006, præmis 57, 58 og 59, hvori Domstolen fastslog, at både afgørelsen om tilstrækkelighed og aftalen om behandlingen af oplysninger er udelukket fra anvendelsesområdet for direktivet.

239 Rådets afgørelse 2012/472/EU af 26. april 2012 om indgåelse af aftalen mellem Amerikas Forenede Stater og Den Europæiske Union om anvendelse og overførsel af passagerlisteoplysninger til United States Department of Homeland Security (2012/472/EU), EUT 2012 L 215/4. Teksten til aftalen er knyttet som bilag til denne afgørelse, EUT 2012 L 215, s. 5-14.

I december 2011 godkendte Rådet indgåelsen af en opdateret aftale mellem EU og Australien om behandling og overførsel af PNR-oplysninger[240]. Aftalen mellem EU og Australien om PNR-oplysninger er endnu et skridt på EU-dagsordenen, som omfatter globale PNR-retningslinjer[241], oprettelse af en PNR-ordning for EU[242] og forhandling af aftaler med tredjelande[243].

Oplysninger om finansielle transaktioner

Det belgiske Society for Worldwide Interbank Financial Telecommunication (SWIFT), som er registeransvarlig for de fleste globale pengeoverførsler fra europæiske banker, driver et mindre computercentre i USA og blev anmodet om at videregive oplysninger til USA's finansministerium med henblik på efterforskning af terrorisme[244].

EU fandt, at der ikke var tilstrækkeligt retsgrundlag til at videregive disse overvejende europæiske oplysninger, som kun var tilgængelige i USA, fordi et af SWIFT's databehandlingscentre var beliggende i USA.

240 Rådets afgørelse 2012/381/EU af 13. december 2011 om indgåelse af aftalen mellem Den Europæiske Union og Australien om luftfartsselskabers behandling og overførsel af passagerliste (PNR)-oplysninger til de australske told- og grænsekontrolmyndigheder (2011/381/EU), EUT 2012 L 186/3. Teksten til aftalen er knyttet som bilag til denne afgørelse, EUT 2012 L 186, s. 4-16.

241 Se f.eks. meddelelse fra Kommissionen om den globale tilgang til overførsel af passageroplysninger (PNR) til tredjelande, KOM(2010) 492 endelig, Bruxelles, den 21. september 2010. Se også Artikel 29-Gruppen (2010), Udtalelse 7/2010 om Europa-Kommissionens meddelelse om den globale tilgang til overførsel af passageroplysninger (PNR) til tredjelande. Vedtaget den 12. november 2010. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp178_da.pdf.

242 Forslag til Europa-Parlamentets og Rådets direktiv om anvendelse af passagerlisteoplysninger til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet, KOM(2011) 32 endelig, Bruxelles, den 2. februar 2011. I april 2011 anmodede Europa-Parlamentet Den Europæiske Unions Agentur for Grundlæggende Rettigheder om en udtalelse om dette forslag og dets overensstemmelse med Den Europæiske Unions charter om grundlæggende rettigheder. Se: Den Europæiske Unions Agentur for Grundlæggende Rettigheder (2011), udtalelse 1/2011 om PNR-oplysninger, Wien, den 14. juni 2011.

243 EU forhandler i øjeblikket med Canada om en ny PNR-aftale, der skal erstatte aftalen fra 2006, som er gældende i dag.

244 Se i denne sammenhæng Artikel 29-Gruppens *udtalelse 14/2011 om databeskyttelsesspørgsmål vedrørende forebyggelse af hvidvaskning af penge og finansiering af terrorisme*, WP 186, Bruxelles, den 13. juni 2011, Artikel 29-Gruppens udtalelse 10/2006 om beskyttelse af personoplysninger om behandling af personoplysninger af Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128, Bruxelles, den 22. november 2006, afgørelse fra Belgiens databeskyttelsesmyndighed (*Commission de la protection de la vie privée*) om selskabet SWIFT scrl, 9. december 2008.

En særlig aftale mellem EU og USA, den såkaldte SWIFT-aftale, blev indgået i 2010 med henblik at tilvejebringe det nødvendige retsgrundlag og garantere tilstrækkelig databeskyttelse[245].

I henhold til denne aftale overføres finansielle data lagret af SWIFT til det amerikanske finansministerium med henblik på at forebygge, efterforske, opdage eller retsforfølge terrorisme og finansiering heraf. Det amerikanske finansministerium kan anmode om finansielle data fra SWIFT, såfremt anmodningen:

- så tydeligt som muligt identificerer de finansielle data
- klart begrunder nødvendigheden af de finansielle data
- 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.

Europol skal have en kopi af hver anmodning fra det amerikanske finansministerium og skal kontrollere, om principperne i SWIFT-aftalen overholdes[246]. 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

245 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 (2010/412/EU), EUT 2010 L 195, s. 3 og 4. Teksten til aftalen er knyttet som bilag til denne afgørelse, EUT 2010 L 195, s. 5-14.

246 Den fælles kontrolinstans for Europol har gennemført audit vedrørende Europols aktiviteter på dette område. Resultaterne heraf er tilgængelige på http://europoljsb.consilium.europa.eu/reports/inspectionreport.aspx?lang=en.

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.

Registrerede har ret til fra den kompetente EU-databeskyttelsesmyndighed at få bekræftet, at deres ret til beskyttelse af personoplysninger er blevet respekteret. Registrerede har også ret til at få data, som det amerikanske finansministerium har indsamlet i medfør af SWIFT-aftalen, berigtiget, slettet eller blokeret. Registreredes ret til indsigt er dog med forbehold af 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 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 udløbet af en etårig aftaleperiode, at den pågældende part ønsker at opsige aftalen.

7

Databeskyttelse i forbindelse med politi og retsvæsen

EU	Omhandlede emner	Europarådet
	Generelt	Konvention 108
	Politiet	Henstilling om politiets brug af personoplysninger
		Menneskerettighedsdomstolen, *B.B. mod Frankrig*, nr. 5335/06, 17. december 2009
		Menneskerettighedsdomstolen, *S. og Marper mod Det Forenede Kongerige*, nr. 30562/04 og 30566/04, 4. december 2008
		Menneskerettighedsdomstolen, *Vetter mod Frankrig*, nr. 59842/00, 31. maj 2005
	Cyberkriminalitet	Konventionen om cyberkriminalitet
Databeskyttelse i forbindelse med grænseoverskridende politisamarbejde og retligt samarbejde		
Rammeafgørelse om databeskyttelse	Generelt	Konvention 108 Henstilling om politiets brug af personoplysninger
Prümafgørelsen	Vedrørende særlige data: fingeraftryk, dna, hooliganisme osv.	Konvention 108 Henstilling om politiets brug af personoplysninger
Europol-afgørelsen Eurojust-afgørelsen Frontex-forordningen	Af særlige agenturer	Konvention 108 Henstilling om politiets brug af personoplysninger

EU	Omhandlede emner	Europarådet
Schengen II-afgørelsen VIS-forordningen Eurodac-forordningen CIS-afgørelsen	Af særlige fælles informationssystemer	Konvention 108 Henstilling om politiets brug af personoplysninger
		Menneskerettighedsdomstolen, *Dalea mod Frankrig*, nr. 964/07, 2. februar 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.

7.1. Europarådets retsorden vedrørende databeskyttelse i forbindelse med politi og retsvæsen

Hovedpunkter

- 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.

På europæisk plan dækker konvention 108 alle områder af behandling 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 retsmyndighedernes arbejde, selv om de kontraherende parter kan begrænse dens anvendelse.

Politiets og retsmyndighedernes 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 de

kontraherende en rettesnor for, hvordan de bør gennemføre principperne i konvention 108 i forbindelse med politiets behandling af personoplysninger[247].

7.1.1. Henstillingen om politiets brug af personoplysninger

Menneskerettighedsdomstolen har konsekvent fastslået, at politiets eller nationale sikkerhedsmyndigheders lagring og opbevaring af personoplysninger udgør et indgreb i artikel, stk. 1, i den europæiske menneskerettighedskonvention (EMK). Mange af Menneskerettighedsdomstolens domme vedrører berettigelsen af sådanne indgreb[248].

Eksempel: I sagen *B.B. mod Frankrig*[249] fastslog Menneskerettighedsdomstolen, at registreringen af en dømt sexforbryder i en national retsdatabase var omfattet af artikel 8 i EMK. 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 den europæiske menneskerettighedskonventions artikel 8 ikke var blevet overtrådt.

Eksempel: I sagen *S. og Marper mod Det Forenede Kongerige*[250] 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 biometriske data var tilladt, hvis en person var mistænkt for en strafbar handling, selv om den mistænkte senere blev frikendt eller løsladt. Menneskerettighedsdomstolen fastslog, at den generelle og vilkårlige opbevaring af personoplysninger, som ikke var tidsbegrænset, og hvor de registrerede kun havde begrænset mulighed for at anmode om sletning, udgjorde et uforholdsmæssigt indgreb i sagsøgernes ret til respekt for privatli-

247 Europarådet, Ministerudvalget (1987), henstilling Rec(87)15 til medlemsstaterne om politiets brug af personoplysninger, 17. september 1987.

248 Se eksempelvis Menneskerettighedsdomstolen, *Leander mod Sverige*, nr. 9248/81, 26. marts 1987, Menneskerettighedsdomstolen, *M.M. mod Det Forenede Kongerige*, nr. 24029/07, 13. november 2012, og Menneskerettighedsdomstolen, *M.K. mod Frankrig*, nr. 19522/09, 18. april 2013.

249 Menneskerettighedsdomstolen, *B.B. mod Frankrig*, nr. 5335/06, 17. december 2009.

250 Menneskerettighedsdomstolen, *S. og Marper mod Det Forenede Kongerige*, nr. 30562/04 og 30566/04, 4. december 2008, præmis 119 og 125.

vet. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Mange af Menneskerettighedsdomstolens domme vedrører endvidere berettigelsen af indgreb i retten til databeskyttelse gennem overvågning.

Eksempel: I sagen *Allan mod Det Forenede Kongerige*[251] havde myndighederne i hemmelighed optaget en indsats private samtaler med en ven i fængslets besøgsområde og med en medanklaget i en fængselscelle. Menneskerettighedsdomstolen fastslog, at brugen af lyd- og videooptagelsesudstyr i sagsøgerens celle, fængslets besøgsområde og på en medindsats 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 den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

Eksempel: I sagen *Klass m.fl. mod Tyskland*[252] påstod sagsøgerne, at flere tyske retsakter, som tillod hemmelig overvågning af post og telekommunikation, var i strid med artikel 8 i EMK, navnlig fordi den pågældende person ikke var informeret om overvågningsforanstaltningerne og ikke kunne få adgang til domstolsprøvelse, når sådanne foranstaltninger var afsluttet. Menneskerettighedsdomstolen fastslog, at en trussel om overvågning nødvendigvis greb ind i friheden til kommunikation mellem brugere af post- og telekommunikationstjenester. Den fandt dog, at der var givet tilstrækkelige garantier mod misbrug. Den tyske lovgiver fandt med rette, at sådanne foranstaltninger var nødvendige i et demokratisk samfund af hensyn til den nationale sikkerhed og for at forebygge uro eller strafbare handlinger. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 ikke 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 sådanne databaser. Europarådets henstilling om politiets brug af personoplysninger omhandler dette spørgsmål og indeholder retningslinjer for, hvordan oplysninger bør indsamles til behandling af politiet, hvordan sådanne arkiver bør opbevares, hvem der bør have adgang til disse arkiver, herunder

251 Menneskerettighedsdomstolen, *Allan mod Det Forenede Kongerige*, nr. 48539/99, 5. november 2002.

252 Menneskerettighedsdomstolen, *Klass m.fl. mod Tyskland*, nr. 5029/71, 6. september 1978.

betingelserne for videregivelse 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 er også omhandlet.

I henhold til henstillingen bør politiet ikke have 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 bekæmpe 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 elektroniske hjælpemidler bør også have et specifikt retsgrundlag.

Eksempel: I sagen *Vetter mod Frankrig*[253] havde et anonymt vidne beskyldt sagsøgeren for manddrab. Da sagsøgeren regelmæssigt besøgte en vens hjem, installerede politiet aflytningsudstyr dér med undersøgelsesdommerens tilladelse. På grundlag af de samtaler, der blev optaget, blev sagsøgeren anholdt og tiltalt for manddrab. Han påstod, at optagelsen ikke kunne lægges til grund som bevis, fordi den ikke var i overensstemmelse med loven. Menneskerettighedsdomstolen tog stilling til, om brugen af aflytningsudstyr var "i overensstemmelse med loven". Aflytning af private ejendomme er bestemt ikke omfattet af anvendelsesområdet for artikel 100 ff. i den franske straffelov, da disse bestemmelser vedrører aflytning af telefonlinjer. Straffelovens artikel 81 fastlægger ikke tilstrækkelig klart, hvorvidt og hvordan myndighederne kan udøve deres skøn, når de tillader overvågning af private samtaler. Sagsøgeren havde derfor ikke haft den minimumsbeskyttelse, som borgere har ret til i henhold til retsstatsprincippet i et demokratisk samfund. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

I henstillingen konkluderes det, at der ved lagring af personoplysninger klart skal sondres mellem: administrative data og politidata, forskellige typer registrerede,

253 Menneskerettighedsdomstolen, *Vetter mod Frankrig*, nr. 59842/00, 31. maj 2005.

som f.eks. mistænkte, dømte, ofre og vidner, og data, der betragtes som kendsgerninger, og data, der betragtes som mistanker eller spekulation.

Politidata skal være strengt begrænsede med hensyn til formål. Det har betydning for videregivelsen af politidata til tredjemand. Videregivelse af sådanne data inden for politiet bør afhænge af, om der er en legitim interesse i at udveksle de pågældende oplysninger. Videregivelsen af sådanne data til parter uden for politiet bør kun være tilladt, hvis der er en klar retlig forpligtelse eller tilladelse hertil. International videregivelse bør kun være tilladt til udenlandske politimyndigheder og bør være baseret på et særligt retsgrundlag, evt. internationale aftaler, medmindre det er nødvendigt for at forebygge alvorlige og umiddelbart forestående farer.

Politiets behandling af personoplysninger skal være underlagt uafhængigt tilsyn for at sikre overensstemmelse med den nationale databeskyttelseslovgivning. Registrerede skal have alle de rettigheder, der er anført i konvention 108. Hvis registreredes ret til indsigt er blevet begrænset i medfør af artikel 9 i konvention 108 af hensyn til politiets efterforskning, skal den registrerede have ret til i henhold til national lovgivning at klage til den nationale databeskyttelsesmyndighed eller et andet uafhængigt organ.

7.1.2. 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[254]. Denne konvention kan også tiltrædes af lande, som ikke er medlem af Europarådet, og i midten af 2013 var fire lande uden for Europarådet – Australien, Den Dominikanske Republik, Japan og USA – parter i konventionen, mens 12 andre ikkemedlemmer havde undertegnet den eller var blevet opfordret til at tiltræde den.

Konventionen om cyberkriminalitet er stadig den mest indflydelsesrige 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,

254 Europarådet, Ministerudvalget (2001), konvention om cyberkriminalitet, CETS nr. 185, Budapest, 23. november 2001 med ikrafttrædelse den 1. juli 2004.

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. 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. Den forpligter de kontraherende parter til ved gennemførelsen af konventionen at sikre tilstrækkelig beskyttelse af menneskerettigheder og frihedsrettigheder, herunder rettigheder garanteret i medfør af den europæiske menneskerettighedskonvention, som f.eks. retten til databeskyttelse[255].

7.2. EU-retten vedrørende databeskyttelse i forbindelse med politi og retsvæsen

Hovedpunkter

- På EU-plan er databeskyttelse i forbindelse med politi og retsvæsen kun omhandlet, for så vidt angår grænseoverskridende politisamarbejde og retligt samarbejde.
- Der findes særlige databeskyttelsesregler for Europol og Eurojust (Den Europæiske Enhed for Retligt Samarbejde), som er EU-organer, der medvirker til og fremmer grænseoverskridende retshåndhævelse.
- 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, VIS (visuminformationssystemet) og Eurodac, et centralt system, der indeholder fingeraftryksoplysninger om tredjelandsstatsborgere, der ansøger om asyl i en EU-medlemsstat.

Databeskyttelsesdirektivet gælder ikke på området for politi og retsvæsen. I afsnit 7.2.1 beskrives de vigtigste retlige instrumenter på dette område.

255 *Ibid.*, artikel 15, stk. 1.

7.2.1. Rammeafgørelsen om databeskyttelse

Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager (*rammeafgørelsen om databeskyttelse*[256]) har til formål at beskytte fysiske personers personoplysninger, når de behandles med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser. Kompetente myndigheder inden for politi og retsvæsen handler på medlemsstaternes eller EU's vegne. Disse myndigheder er EU-agenturer eller -organer og medlemsstaternes myndigheder[257]. Anvendelsesområdet for rammeafgørelsen er begrænset til databeskyttelse i forbindelse med det grænseoverskridende samarbejde mellem disse myndigheder og omfatter ikke national sikkerhed.

Rammeafgørelsen om databeskyttelse er i vid udstrækning baseret på de principper og definitioner, der også findes i konvention 108 og databeskyttelsesdirektivet.

Data må kun anvendes af en kompetent myndighed og kun til de formål, som de er videregivet eller stillet til rådighed til. Den modtagende medlemsstat skal overholde enhver begrænsning for udvekslingen af de pågældende oplysninger, som er fastsat ved den videregivende medlemsstats lov. Den modtagende stats anvendelse af oplysningerne til et andet formål tillades dog under visse omstændigheder. De kompetente myndigheder har specifikt pligt til at registrere og dokumentere videregivelser med henblik på at hjælpe med at afklare ansvar, der følger af klager. Videregivelse af oplysninger, der er modtaget i forbindelse med grænseoverskridende samarbejde, til tredjemand kræver samtykke fra den medlemsstat, oplysningerne stammer fra, selv om der kan gøres undtagelser i presserende sager.

De kompetente myndigheder skal træffe de nødvendige sikkerhedsforanstaltninger for at beskytte personoplysninger mod ulovlig behandling.

Hver medlemsstat udpeger en eller flere uafhængige nationale tilsynsmyndigheder, der har til opgave på dens område at yde rådgivning og påse overholdelsen af de bestemmelser, der er vedtaget i medfør af rammeafgørelsen om databeskyttelse. De skal også behandle klager, der indbringes af en person vedrørende beskyttelse

256 Rådet for Den Europæiske Union (2008), Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager (*rammeafgørelsen om databeskyttelse*), EUT 2008 L 350.

257 *Ibid.*, artikel 2, litra h).

af vedkommendes rettigheder og frihedsrettigheder i forbindelse med de kompetente myndigheders behandling af personoplysninger.

Den registrerede underrettes om behandlingen af vedkommendes personoplysninger og har ret til indsigt, berigtigelse, sletning eller blokering. Hvis udøvelsen af disse rettigheder afvises af tungtvejende grunde, skal den registrerede have ret til at indgive en klage til den kompetente nationale tilsynsmyndighed og/eller en domstol. Hvis en person lider skade som følge af overtrædelser af nationale bestemmelser, der vedtages til gennemførelse af rammeafgørelsen om databeskyttelse, er denne person berettiget til erstatning fra den registeransvarlige[258]. Registrerede har generelt ret til at indbringe krænkelser af de rettigheder, der garanteres vedkommende i henhold til national lovgivning, for en domstol[259].

Kommissionen har fremsat forslag til en reform, der består af en generel forordning om databeskyttelse[260] og et generelt databeskyttelsesdirektiv[261]. Det nye direktiv erstatter den nuværende rammeafgørelse om databeskyttelse og overfører generelle principper og regler til politisamarbejde og retligt samarbejde i kriminalsager.

7.2.2. Mere specifikke databeskyttelsesinstrumenter i forbindelse med grænseoverskridende politi- og retshåndhævelsessamarbejde

Ud over rammeafgørelsen om databeskyttelse er udvekslingen af oplysninger, som medlemsstaterne er i besiddelse af, inden for bestemte områder reguleret ved en række retlige instrumenter, som f.eks. Rådets rammeafgørelse 2009/315/RIA om tilrettelæggelsen og indholdet af udvekslinger af oplysninger fra strafferegistre mellem medlemsstaterne og Rådets afgørelse vedrørende ordninger for samarbejde

258 *Ibid.*, artikel 19.

259 *Ibid.*, artikel 20.

260 Europa-Kommissionen (2012), forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse), KOM(2012) 11 endelig, Bruxelles, den 25. januar 2012.

261 Europa-Kommissionen (2012), forslag til 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, KOM(2012) 10 endelig, Bruxelles, den 25. januar 2012.

mellem finansielle efterretningsenheder i medlemsstaterne for så vidt angår udveksling af oplysninger[262].

Grænseoverskridende samarbejde[263] mellem kompetente myndigheder involverer i stigende grad udveksling af oplysninger om immigration. Dette juridiske område hører ikke ind under politiet og straffedomstolene, men er i mange henseender relevant for politiets og retsmyndighedernes arbejde. Det samme gælder for oplysninger om varer, der importeres til eller eksporteres fra EU. Ophævelsen af grænsekontrollen ved de indre grænser i EU har øget risiko for bedrageri. Medlemsstaterne har derfor skullet intensivere samarbejdet ved f.eks. at forbedre den grænseoverskridende udveksling af informationer, så de mere effektivt kan afsløre og retsforfølge overtrædelser af de nationale og europæiske toldbestemmelser.

Prümafgørelsen

Et vigtigt eksempel på institutionaliseret grænseoverskridende samarbejde ved udveksling af oplysninger, der opbevares af medlemsstaterne, er Rådets 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[264]. Prümaftalen var en international aftale om politisamarbejde, som blev undertegnet af Østrig, Belgien, Frankrig, Tyskland, Luxembourg, Nederlandene og Spanien i 2005[265].

Prümafgørelsen har til formål at hjælpe medlemsstaterne med at forbedre informationsudvekslingen med henblik på at forebygge og bekæmpe kriminalitet på tre

262 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 2009 L 93, 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 2000 L 271.

263 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, den 7. december 2012.

264 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 2008 L 210.

265 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; findes på: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

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 og senere rammeafgørelsen om databeskyttelse. De kompetente organer for tilsynet med sådanne dataudvekslinger er de nationale databeskyttelsesmyndigheder.

7.2.3. Databeskyttelse i Europol og Eurojust

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 Rådets afgørelse om oprettelse af en europæisk politienhed (*Europol-afgørelsen*)[266]. Europol støtter medlemsstaternes indsats i bestræbelserne på at forebygge og efterforske organiseret kriminalitet, terrorisme og andre former for alvorlig kriminalitet (jf. bilaget til Europol-afgørelsen), som berører to eller flere medlemsstater.

266 Rådet for Den Europæiske Union (2009), Rådets afgørelse af 6. april 2009 om oprettelse af Den Europæiske Politienhed, EUT 2009 L 121 (Europol). Se også Kommissionens forslag til forordning, som indeholder en retlig ramme for et nyt Europol, der efterfølger og erstatter det Europol, der blev oprettet ved Rådets afgørelse 2009/371/RIA af 6. april 2009 om oprettelse af Den Europæiske Politienhed (Europol), og Det Europæiske Politiakademi, der blev oprettet ved Rådets afgørelse 2005/681/RIA af 20. september 2005 om oprettelse af Det Europæiske Politiakademi (Cepol) (COM(2013) 173 final).

For at opfylde dette formål har Europol udviklet Europols informationssystem, som tilvejebringer en platform, hvor medlemsstaterne – via Europols nationale enheder – kan udveksle strafferetlige efterretninger og oplysninger. Europols informationssystem kan bruges til at give adgang til oplysninger, som vedrører personer, som 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 Europols nationale enheder 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.

Hvis det er nødvendigt for at udføre opgaverne, kan Europol lagre, ændre og anvende oplysninger om strafbare handlinger i analyseregistre. Analyseregistre oprettes med henblik på at samle, behandle eller anvende oplysninger til brug i specifikke strafferetlige efterforskninger, som gennemføres af Europol sammen med EU's medlemsstater.

I tråd med den teknologiske udvikling blev der oprettet et europæisk center til bekæmpelse af it-kriminalitet i Europol den 1. januar 2013[267]. Dette center tjener som europæisk knudepunkt for information om it-kriminalitet. Det bidrager til at sikre hurtigere reaktion i tilfælde af kriminalitet på internettet, udvikler og indfører digital retsmedicinsk teknologi og opstiller bedste praksis inden for efterforskning af it-kriminalitet. Centret fokuserer på it-kriminalitet, 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 kritiske informations- og kommunikationssystemer i EU.

De databeskyttelsesregler, der regulerer Europols aktiviteter, er blevet styrket. I henhold til Europol-afgørelsens artikel 27 finder de principper, der er fastsat ved konvention 108 og henstillingen om politiets brug af personoplysninger vedrørende elektroniske og ikke-elektroniske oplysninger, anvendelse. Videregivelse af

267 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, den 29. juni 2012.

oplysninger mellem Europol og medlemsstaterne skal også ske i overensstemmelse med de regler, der er anført i rammeafgørelsen om databeskyttelse.

For at sikre, at den gældende databeskyttelseslovgivning overholdes, og at personers rettigheder ikke krænkes ved behandlingen af personoplysninger, kontrolleres og overvåges Europols aktiviteter af Den Fælles Kontrolinstans for Europol[268]. Enhver har ret til indsigt i de personoplysninger, som Europol opbevarer om vedkommende, og har også ret til at anmode om kontrol, berigtigelse eller sletning af disse personoplysninger. Hvis en person ikke kan acceptere Europols afgørelse vedrørende udøvelsen af disse rettigheder, kan vedkommende klage til Klageudvalget under Den Fælles Kontrolinstans.

Hvis skade påføres en person på grund af retligt eller faktisk ukorrekte oplysninger, som er lagret eller behandlet af Europol, skal den skadelidte rette sin anmodning om erstatning til den kompetente myndighed i den medlemsstat, hvor skaden er sket[269]. Europol godtgør medlemsstaten, hvis skaden skyldes Europols manglende overholdelse af dets retlige forpligtelser.

Eurojust

Eurojust, som blev oprettet i 2002, er et EU-organ med hovedkvarter i Haag, som har til formål at fremme det retlige samarbejde under efterforskning og retsforfølgning af grov kriminalitet, der berører mindst to medlemsstater[270]. Eurojust har kompetence til at:

- fremme og forbedre koordineringen og samarbejdet mellem medlemsstaternes kompetente judicielle myndigheder
- medvirke til at fuldbyrde anmodninger og afgørelser om retligt samarbejde.

268 Europol-afgørelsen, artikel 34.

269 *Ibid.*, artikel 52.

270 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 2002 L 63, 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 2003 L 44, 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 2009 L 138 (*Eurojust-afgørelserne*).

Eurojusts funktioner varetages af nationale medlemmer. Hver medlemsstat udstationerer en dommer eller anklager ved Eurojust. Disse personer er, for så vidt angår deres status, underlagt deres medlemsstaters nationale lovgivning og skal have 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[271]. I undtagelsestilfælde kan Eurojust dog også i et begrænset tidsrum behandle andre personoplysninger vedrørende omstændighederne omkring en lovovertrædelse, såfremt de er af umiddelbar betydning for og indgår i den løbende 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.

Med hensyn til databeskyttelse skal Eurojust garantere et beskyttelsesniveau, der mindst svarer til principperne i Europarådets konvention 108 med efterfølgende ændringer. Dataudveksling kræver overholdelse af specifikke regler og begrænsninger, der er indført i samarbejdsaftaler og samarbejdsordninger i overensstemmelse med Rådets afgørelser om Eurojust og Eurojusts databeskyttelsesregler[272].

Der er oprettet en uafhængig kontrolinstans under Eurojust, som har til opgave at overvåge Eurojusts behandling af personoplysninger. Personer kan klage til Den Fælles Kontrolinstans, hvis de ikke kan acceptere Eurojusts besvarelse af en anmodning om indsigt, berigtigelse, blokering eller sletning af personoplysninger. Hvis Eurojust behandler personoplysninger ulovligt, er Eurojust ansvarligt i henhold til den nationale lovgivning i den medlemsstat, hvor det har sit hovedkvarter, dvs. Nederlandene, for den skade, der påføres den registrerede.

271 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.

272 Eurojusts forretningsordens bestemmelser for behandling og beskyttelse af personoplysninger, EUT 2005 C 68/01, 19. marts 2005, s. 1.

7.2.4. 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 er der på EU-plan indført en række fælles informationssystemer, der fungerer som en platform for dataudveksling mellem kompetente nationale myndigheder og EU-myndigheder med håndhævelse af særlig lovgivning for øje, herunder immigrations- og toldlove. Nogle af disse systemer er udsprunget af multilaterale aftaler, som efterfølgende er suppleret af EU-instrumenter og -systemer, som f.eks. Schengeninformationssystemet, VIS (visuminformationssystemet), Eurodac, Eurosur og CIS (toldinformationssystemet).

Det Europæiske Agentur for den Operationelle Forvaltning af Store It-systemer (eu-LISA)[273], som blev oprettet i 2012, er ansvarligt for den langsigtede forvaltning af anden generation af Schengeninformationssystemet (SIS II), visuminformationssystemet (VIS) og Eurodac. eu-LISA's kerneopgave er at sikre, at informationssystemerne fungerer effektivt, sikkert og uafbrudt. Det er også ansvarligt for at træffe de nødvendige foranstaltninger for at garantere systemernes og dataenes sikkerhed.

Schengeninformationssystemet

I 1985 tiltrådte flere medlemsstater af de tidligere Europæiske Fællesskaber aftalen mellem regeringerne for staterne i Den Økonomiske Union Benelux, Forbundsrepublikken Tyskland og Den Franske Republik 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[274]. 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.

273 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 2011 L 286.

274 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 2000 L 239.

Som følge af yderligere landes tiltræden til Schengenaftalen blev Schengensystemet endeligt integreret i EU's retlige ramme med Amsterdamtraktaten[275]. Denne beslutning blev gennemført i 1999. Den nyeste version af Schengeninformationssystemet, "SIS II", blev sat i drift den 9. april 2013. Det betjener nu alle EU's medlemsstater samt Island, Liechtenstein, Norge og Schweiz[276]. 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 indlæst om personer og genstande. C-SIS bruges af de nationale grænsekontroller, politi, toldvæsenet samt visum- og retsmyndigheder i hele Schengenområdet. Hver medlemsstat driver en national udgave af C-SIS, "N-SIS", som løbende ajourføres, således at også C-SIS ajourføres. Efter søgning i N-SIS udsendes der en indberetning, hvis:

- personen ikke har ret til at rejse til eller opholde sig i Schengenområdet, eller
- personen eller genstanden er eftersøgt af retslige eller retshåndhævende myndigheder, eller
- personen er meldt savnet, eller
- genstande, som f.eks. pengesedler, motorkøretøjer, skydevåben og identitetspapirer, er meldt stjålet eller forsvundet.

I tilfælde af en indberetning iværksættes opfølgende aktiviteter via de nationale Schengeninformationssystemer.

SIS II har nye funktioner, herunder f.eks. mulighed for at indlæse biometriske data, såsom fingeraftryk og fotografier, nye kategorier af indberetninger, såsom stjålne både, luftfartøjer, containere eller betalingsmidler, og nye forbedrede indberetninger om personer og genstande, samt kopier af europæiske arrestordrer vedrørende personer, der begæres anholdt med henblik på overgivelse/udlevering.

275 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 1997 C 340.

276 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 2006 L 381, og Rådets afgørelse 2007/533/RIA af 12. juni 2007 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (*SIS II*), EUT 2007 L 205.

Rådets afgørelse 2007/533/RIA om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (Schengen II-afgørelsen) omfatter konvention 108: "Personoplysninger, der behandles i medfør af denne afgørelse, er beskyttet i overensstemmelse med Europarådets konvention [108]"[277]. Hvis de nationale politimyndigheders anvendelse af personoplysninger sker i overensstemmelse med Schengen II-afgørelsen, skal bestemmelserne i konvention 108 og i henstillingen om politiets brug af personoplysninger gennemføres i den nationale lovgivning.

Den kompetente nationale tilsynsmyndighed i hver medlemsstat fører tilsyn med det nationale N-SIS. Den skal navnlig kontrollere kvaliteten af de oplysninger, som medlemsstaten indlæser i C-SIS via N-SIS. Den nationale tilsynsmyndighed skal sikre, at der gennemføres en revision af databehandlingerne i det nationale N-SIS mindst hvert fjerde år. De nationale tilsynsmyndigheder og Den Europæiske Tilsynsførende samarbejder og koordinerer tilsynet med C-SIS. Af hensyn til gennemsigtigheden forelægges en fælles aktivitetsrapport for Europa-Parlamentet, Rådet og eu-LISA hvert andet år.

For så vidt angår SIS II, kan personer udøve deres ret til indsigt i enhver medlemsstat, da hver N-SIS er en nøjagtig kopi af C-SIS.

Eksempel: I sagen *Dalea mod Frankrig*[278] 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. Menneskerettighedsdomstolen fastslog, at indberetningen af sagsøgeren i Schengeninformationssystemet var 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 tilstrækkelig 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.

277 Rådet for Den Europæiske Union (2007), Rådets afgørelse 2007/533/RIA af 12. juni 2007 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet, EUT 2007 L 205, artikel 57.

278 Menneskerettighedsdomstolen, *Dalea mod Frankrig* (dec.), nr. 964/07, 2. februar 2010.

Visuminformationssystemet

Visuminformationssystemet (VIS), som også drives af eu-LISA, blev udviklet med henblik på at støtte gennemførelsen af en fælles visumpolitik i EU[279]. VIS sætter Schengenlandene i stand til at udveksle visumoplysninger gennem et system, der forbinder Schengenlandenes konsulater 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 at kontrollere, om den person, der fremlægger et visum, er dets retmæssige indehaver, og identificere personer uden identitetspapirer eller med falske identitetspapirer.

I henhold til 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) må kun oplysninger om ansøgeren, vedkommendes visa, fotografier, fingeraftryk, forbindelser til tidligere ansøgninger og ansøgningsdossierer for personer, der ledsager vedkommende, registreres i VIS[280]. Kun medlemsstaternes visummyndigheder har adgang til at indtaste, ændre eller slette data i VIS, mens visummyndigheder og myndigheder med kompetence til at foretage kontrol ved ydre grænseovergangssteder, immigrationskontrol og asylmyndigheder kan søge efter oplysninger. På visse betingelser kan nationale kompetente politimyndigheder og Europol anmode om adgang til oplysninger, der er indtastet i VIS, med det formål at forebygge, afsløre og efterforske terrorisme og strafbare handlinger[281].

279 Rådet for Den Europæiske Union (2004), Rådets beslutning af 8. juni 2004 om indførelse af visuminformationssystemet (VIS), EUT 2004 L 213; 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 2008 L 218; 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 2008 L 218.

280 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 2008 L 218.

281 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 2008 L 218.

Eurodac

Eurodacs navn refererer til dactylogrammer eller fingeraftryk. Det er et centralt system, som indeholder fingeraftryksoplysninger om tredjelandsstatsborgere, der søger om asyl i en af EU's medlemsstater[282]. Systemet har været i drift siden januar 2003, og det har til formål at hjælpe med at fastslå, hvilken medlemsstat der er ansvarlig for at undersøge en bestemt asylansøgning i medfør af Rådets forordning (EF) nr. 343/2003 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en asylansøgning, der er indgivet af en tredjelandsstatsborger i en af medlemsstaterne (*Dublin II-forordningen*)[283]. Personoplysninger i Eurodac må kun anvendes til at lette anvendelsen af Dublin II-forordningen. Enhver yderligere anvendelse ifalder sanktioner.

Eurodac består af en central enhed, der 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 af hver tredjelandsstatsborger eller statsløs person på 14 år og derover, som ansøger om asyl på deres område, eller som tilbageholdes for ulovlig passage af de ydre grænser. Medlemsstater kan også tage og overføre fingeraftryk af tredjelandsstatsborgere eller statsløse personer, som opholder sig på deres område uden tilladelse.

Fingeraftryksoplysningerne lagres i Eurodac-databasen i pseudonymiseret form. I tilfælde af et match videregives pseudonymet sammen med navnet på den første medlemsstat, der overførte fingeraftryksoplysningerne, til den anden medlemsstat. Den anden medlemsstat kontakter derefter den første medlemsstat, fordi den første medlemsstat i henhold til Dublin II-forordningen er ansvarlig for behandlingen af asylansøgningen.

Personoplysninger, som er lagret i Eurodac, og som vedrører asylansøgere, opbevares i 10 år fra den dato, hvor fingeraftrykkene blev taget, medmindre den registrerede opnår statsborgerskab i en EU-medlemsstat. I det tilfælde skal oplysningerne

282 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 Dublinkonventionen, EFT 2000 L 316; 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 Dublinkonventionen, EFT 2002 L 62 (*Eurodac-forordningerne*).

283 Rådets forordning (EF) nr. 343/2003 af 18. februar 2003 om fastsættelse af kriterier og procedurer til afgørelse af, hvilken medlemsstat der er ansvarlig for behandlingen af en asylansøgning, der er indgivet af en tredjelandsstatsborger i en af medlemsstaterne, EUT 2003 L 50 (*Dublin II-forordningen*).

slettes omgående. Oplysninger vedrørende tredjelandsstatsborgere, der tilbageholdes for ulovlig passage af ydre grænser, lagres i to år. Disse oplysninger skal slettes omgående, hvis den registrerede opnår opholdstilladelse, forlader EU's område eller opnår statsborgerskab i en medlemsstat.

Ud over alle EU's medlemsstater anvender Island, Norge, Liechtenstein og Schweiz også Eurodac på grundlag af internationale aftaler.

Eurosur

Det europæiske grænseovervågningssystem (*Eurosur*)[284] 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, EU-agenturet med ansvar for at udvikle og anvende det nye begreb "integreret grænseforvaltning"[285]. Dets generelle mål er:

- 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[286].

Det indledte sit arbejde den 2. december 2013 i alle medlemsstater med ydre grænser, og den 1. december 2014 iværksættes det i de øvrige. Forordningen gælder for overvågning af medlemsstaternes ydre land- og søgrænser samt luftgrænser.

284 Europa-Parlamentets og Rådets forordning (EU) nr. 1052/2013 af 22. oktober 2013 om oprettelse af det europæiske grænseovervågningssystem (Eurosur), EUT 2013 L 295.

285 Europa-Parlamentets og Rådets forordning (EU) nr. 1168/2011 af 25. oktober 2011 om ændring af Rådets forordning (EF) nr. 2007/2004 om oprettelse af et europæisk agentur for forvaltning af det operative samarbejde ved EU-medlemsstaternes ydre grænser (*Frontex-forordningen*), EUT 2011 L 394.

286 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, den 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, den 12. december 2011, s. 18.

Toldinformationssystemet

Et andet vigtigt fælles informationssystem, som er oprettet på EU-plan, er CIS (toldinformationssystemet)[287]. 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.

Informationerne i CIS omfatter personoplysninger med henvisning til varer, transportmidler, virksomheder, personer, varer og kontanter, der er tilbageholdt, beslaglagt eller konfiskeret. Disse informationer må udelukkende bruges med henblik på observation, optagelse af rapport eller gennemførelse af særlige inspektioner eller strategiske eller operationelle analyser vedrørende personer, der mistænkes for at have overtrådt toldbestemmelserne.

Nationale told-, skatte-, landbrugs-, sundheds- og politimyndigheder, Europol og Eurojust har adgang til CIS-oplysninger.

Behandlingen af personoplysninger skal være i overensstemmelse med de specifikke regler i Rådets forordning nr. 515/97 og CIS-konventionen.[288] og bestemmelserne i databeskyttelsesdirektivet, forordningen om databeskyttelse inden for EU-institutionerne, konvention 108 og henstillingen om politiets brug af personoplysninger. Den tilsynsførende er ansvarlig for tilsynet med overensstemmelsen af CIS med forordning (EF) nr 45/2001 og indkalder til et møde mindst en gang om året med alle nationale tilsynsmyndigheder for databeskyttelse, som er kompetente i CIS-relaterede tilsynsspørgsmål.

287 Rådet for Den Europæiske Union (1995), Rådets retsakt af 26. juli 1995 om udarbejdelse af konventionen om beskyttelse af De Europæiske Fællesskabers finansielle interesser, EFT 1995 C 316, ændret af Rådet for Den Europæiske Union (2009), Rådets 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, Rådets afgørelse 2009/917/RIA af 30. november 2009 om brug af informationsteknologi på toldområdet (*CIS-afgørelsen*), EUT 2009 L 323.

288 *Ibid.*

8

Andre specifikke europæiske databeskyttelsesregler

EU	Omhandlede emner	Europarådet
Databeskyttelsesdirektivet Direktivet om databeskyttelse inden for elektronisk kommunikation	**Elektronisk kommunikation**	Konvention 108 Henstillingen om telekommunikationstjenester
Databeskyttelsesdirektivet, artikel 8, stk. 2, litra b)	**Ansættelsesmæssige relationer**	Konvention 108 Henstilling om personoplysninger i ansættelsesforhold
		Menneskerettighedsdomstolen, *Copland mod Det Forenede Kongerige*, nr. 62617/00, 3. april 2007
Databeskyttelsesdirektivet, artikel 8, stk. 3	**Medicinske oplysninger**	Konvention 108 Henstilling om medicinske oplysninger
		Menneskerettighedsdomstolen, *Z. mod Finland*, nr. 22009/93, 25. februar 1997
Direktivet om kliniske forsøg	**Kliniske forsøg**	
Databeskyttelsesdirektivet, artikel 6, stk. 1, litra b) og e), og artikel 13, stk. 2	**Statistikker**	Konvention 108 Henstilling vedrørende statistiske oplysninger
Forordning (EF) nr. 223/2009 om europæiske statistikker EU-Domstolen, C-524/06, *Huber mod Tyskland*, 16. december 2008	**Officielle statistikker**	Konvention 108 Henstilling vedrørende statistiske oplysninger

EU	Omhandlede emner	Europarådet
Direktiv 2004/39/EF 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	Konvention 108 Henstilling 90(19) om personoplysninger, der anvendes ved betaling og andre tilknyttede handlinger Menneskerettighedsdomstolen, *Michaud mod Frankrig*, nr. 12323/11, 6. december 2012

I flere tilfælde er der på europæisk plan vedtaget særlige retlige instrumenter, som mere detaljeret anvender de generelle regler i konvention 108 eller databeskyttelsesdirektivet i særlige situationer.

8.1. 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 trafikdata, 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 yderligere 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[289]. I henhold til henstillingen bør formålene med indsamling og behandling af personoplysninger i forbindelse med telekommunikation begrænses til: tilslutning af en bruger til netværket, formidling 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 markedsføringsmeddelelser. Generelt må 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 behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (*direktivet om databeskyttelse inden for elektronisk kommunikation*) efter et første forsøg i 1997 vedtaget i 2002 og ændret i 2009 med det formål at supplere og tilpasse bestemmelserne i databeskyttelsesdirektivet specifikt til telekommunikationssektoren[290]. 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

289 Europarådet, Ministerudvalget (1995), henstilling Rec(95)4 til medlemsstaterne om beskyttelse af personoplysninger telekommunikationsområdet, herunder især telefontjenester, 7. februar 1995.

290 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 2002 L 201), 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 2009 L 337.

- de data, der er nødvendige for at etablere og opretholde kommunikationen, dvs. trafikdata, som f.eks. information om kommunikationspartnerne samt tidspunkt for og varighed af kommunikationen

- trafikdata 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 registeransvarlige, som tilbyder avancerede tjenester, som f.eks. 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, f.eks. adgang med henblik på efterforskning af kriminalitet, skal i henhold til artikel 15 i direktivet om databeskyttelse inden for elektronisk kommunikation opfylde betingelserne for begrundede indgreb som fastlagt i artikel 8, stk. 2, i den europæiske menneskerettighedskonvention og bekræftet ved chartrets artikel 8 og 52.

Ved ændringerne af direktivet om databeskyttelse inden for elektronisk kommunikation[291] i 2009 indførtes følgende:

- Begrænsningerne for udsendelse af e-mail i markedsføringsøjemed blev udvidet til at gælde for tjenester for korte meddelelser (SMS), tjenester for multimediemeddelelser (MMS) og andre lignende anvendelser. Markedsførings-e-mail er forbudt, medmindre modtageren på forhånd har givet sit udtrykkelige 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.

291 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 2009 L 337.

- Medlemsstaterne blev pålagt en forpligtelse til at sikre klageadgang i tilfælde af overtrædelse af forbuddet mod uanmodet kommunikation[292].

- Indsættelse af cookies, dvs. software, som overvåger og registrerer en computerbrugers handlinger, er ikke længere tilladt uden brugerens samtykke. Hvordan dette samtykke skal gives og indhentes for at sikre tilstrækkelig beskyttelse, fastsættes ved national lov[293].

I tilfælde af brud på datasikkerheden som følge af ubeføjet 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[294].

I henhold til datalagringsdirektivet[295] (ugyldigt siden 8. april 2014) havde telekommunikationsudbydere pligt til at bevare trafikdata tilgængelige, især med henblik på bekæmpelse af grov kriminalitet, i en periode på mindst seks måneder og højst to år, uanset om udbyderen stadig havde brug for disse data i faktureringsøjemed eller til teknisk at levere tjenesten.

EU's medlemsstater skal udpege uafhængige offentlige myndigheder, som skal føre tilsyn med de lagrede datas sikkerhed.

Lagringen af telekommunikationsdata er klart et indgreb i retten til databeskyttelse[296]. Om dette indgreb er berettiget, er blevet anfægtet i flere retssager i EU's medlemsstater[297].

---

292 Artikel 13 i direktivet som ændret.

293 Se *Ibid.*, artikel 5. Se også Artikel 29-Gruppens udtalelse fra 2012 om undtagelse for cookies (*Opinion 04/2012 on cookie consent exemption*), WP 194, Bruxelles, den 7. juni 2012.

294 Se også Artikel 29-Gruppens arbejdsdokument fra 2011 om EU's nuværende ramme for brud på persondatasikkerheden og anbefalinger vedrørende den fremtidige politiske udvikling (*Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*), WP 184, Bruxelles, 5. april 2011.

295 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 2006 L 105.

296 EDPS (2011), *udtalelse af 31. maj 2011 vedrørende evalueringsrapporten fra Kommissionen til Rådet og Europa-Parlamentet om datalagringsdirektivet (direktiv 2006/24/EF)*, 31. maj 2011.

297 Tyskland, *Bundesverfassungsgericht*, 1 BvR 256/08, 2. marts 2010, Rumænien, forfatningsdomstolen (*Curtea Constituțională a României*), nr. 1258, 8. oktober 2009, Tjekkiet, forfatningsdomstolen (*Ústavní soud České republiky*), 94/2011 Sml., 22. marts 2011.

Eksempel: I sagen *Digital Rights Irland og Seitlinger m.fl.*[298] erklærede EU-domstolen datalagringsdetektivet for ugyldigt. Ifølge Domstolen fordi, *"at dette direktiv indebærer et indgreb i disse grundlæggende rettigheder, som er meget vidtrækkende og af særligt alvorlig karakter i EU's retsorden, uden at dette indgreb er præcist afgrænset af bestemmelser, der gør det muligt at sikre, at det faktisk er begrænset til det strengt nødvendige."*

Et vigtigt spørgsmål i forbindelse med elektronisk kommunikation er offentlige myndigheders indgreb. 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 den nationale sikkerhed, den offentlige sikkerhed, statens økonomiske interesser eller bekæmpelse af strafbare handlinger eller af hensyn til beskyttelsen af den registrerede eller andres rettigheder og frihedsrettigheder.

Eksempel: I sagen *Malone mod Det Forenede Kongerige*[299] var sagsøgeren blevet anklaget for en række forseelser vedrørende uærlig håndtering af stjålne varer. I løbet af retssagen viste det sig, at en af sagsøgerens telefonsamtaler var blevet aflyttet efter kendelse udstedt af det britiske indenrigsministerium. Selv om den måde, hvorpå sagsøgerens kommunikation var blevet aflyttet på, var lovlig i henhold til den nationale lovgivning, fandt Menneskerettighedsdomstolen, at der ikke var fastlagt regler vedrørende omfanget af myndighedernes skøn og den måde, hvorpå de kunne udøve dette, og at indgrebet, der var baseret på tidligere praksis, derfor ikke var i overensstemmelse med loven. Domstolen konkluderede, at den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

8.2. 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 databeskyttelsesdirektivet, for så vidt angår behandling af følsomme oplysninger.

298 EU-Domstolens forenede sager C-293/12 og C-594/12, *Digital Rights Ireland og Seitlinger m.fl.*, 8. april 2014, præmis 65.

299 Menneskerettighedsdomstolen, *Malone mod Det Forenede Kongerige*, nr. 8691/79, 2. august 1984.

- 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.

Der er ikke en specifik retlig ramme i EU, som omhandler behandling af personoplysninger i ansættelsesforhold. I databeskyttelsesdirektivet er ansættelsesmæssige forhold kun specifikt nævnt i direktivets artikel 8, stk. 2, som vedrører behandlingen af følsomme oplysninger. Europarådet udsendte i 1989 sin henstilling om personoplysninger i ansættelsesforhold, som i øjeblikket ajourføres[300].

En undersøgelse af de mest udbredte databeskyttelsesproblemer netop i forbindelse med ansættelsesforhold findes i et arbejdsdokument fra Artikel 29-Gruppen[301]. Arbejdsgruppen analyserede betydningen af samtykke som retsgrundlag for behandling af personoplysninger i ansættelsesforhold[302]. 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 der anmodes om samtykke, bør derfor overvejes nøje ved vurderingen af gyldigheden af samtykke i ansættelsesforhold.

Et udbredt databeskyttelsesproblem på mange arbejdspladser er i dag det legitime omfang af overvågningen 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. Følgende dom fra Menneskerettighedsdomstolen er især relevant i den forbindelse:

Eksempel: I sagen *Copland mod Det Forenede Kongerige*[303] blev en medarbejders brug af telefon, e-mail og internettet i hemmelighed overvåget for at kon-

300 Europarådet, Ministerudvalget (1989), henstilling Rec(89)2 til medlemsstaterne om beskyttelse af personoplysninger, der anvendes i ansættelsesforhold, 18. januar 1989. Se også undersøgelse udarbejdet af Europarådets rådgivende udvalg vedrørende konvention 108, "Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation", 9. september 2011.

301 Artikel 29-Gruppen (2001), udtalelse 8/2001 om behandling af personoplysninger i ansættelsesforhold, WP 48, Bruxelles, den 13. september 2001.

302 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, den 25. november 2005.

303 Menneskerettighedsdomstolen, *Copland mod Det Forenede Kongerige*, nr. 62617/00, 3. april 2007.

trollere, om hun i overdreven grad anvendte arbejdsgiverens udstyr til private formål. Menneskerettighedsdomstolen 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 af overvågningen af den personlige anvendelse af internettet, var således beskyttet af artikel 8 i EMK. 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 den europæiske menneskerettighedskonventions artikel 8 var blevet overtrådt.

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 ansættelsesforhold er medarbejderrepræsentanternes rolle. Sådanne repræsentanter må kun modtage medarbejderes personoplysninger, hvis de er nødvendige for, at de kan repræsentere de pågældende medarbejderes interesser.

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 kræve en helbredsundersøgelse, hvis det er nødvendigt for at afgøre, om en medarbejder er egnet til ansættelse, om kravene til forebyggende medicin er opfyldt, eller om en medarbejder kan få tildelt sociale ydelser. 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. Arbejdsgivere bør også på forhånd informere deres medarbejdere om indførelsen eller tilpasningen af elektroniske systemer til behandling af medarbejderes personoplysninger eller til overvågning af medarbejderens bevægelser eller produktivitet.

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.

8.3. Medicinske oplysninger

Hovedpunkt

- Medicinske oplysninger er følsomme oplysninger og er derfor garanteret særlig beskyttelse.

Personoplysninger vedrørende den registreredes helbred udgør følsomme oplysninger i henhold til databeskyttelsesdirektivets artikel 8, stk. 1, og artikel 6 i konvention 108. Medicinske oplysninger er til gengæld underlagt en strengere databehandlingsregler end ikke-følsomme oplysninger.

Eksempel: I sagen *Z. mod Finland*[304] 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

304 Menneskerettighedsdomstolen, *Z. mod Finland*, nr. 22009/93, 25. februar 1997, præmis 94 og 112. Se også Menneskerettighedsdomstolen, *M.S. mod Sverige*, nr. 20837/92, 27. august 1997, Menneskerettighedsdomstolen, *L.L. mod Frankrig*, nr. 7508/02, 10. oktober 2006, Menneskerettighedsdomstolen, *I. mod Finland*, nr. 20511/03, 17. juli 2008, Menneskerettighedsdomstolen, *K.H. m.fl. mod Slovakiet*, nr. 32881/04, 28. april 2009, og Menneskerettighedsdomstolen, *Szuluk mod Det Forenede Kongerige*, nr. 36936/05, 2. juni 2009.

risikoen for hiv-infektion. Den nationale domstol fastslog, at dommen i sin helhed skulle forblive fortrolig 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. Menneskerettighedsdomstolen 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 EMK.

Ifølge databeskyttelsesdirektivets artikel 8, stk. 3, er behandling af medicinske oplysninger tilladt, hvis behandlingen er nødvendig med henblik på forebyggende medicin, medicinsk diagnose, sygepleje eller patientbehandling eller forvaltning af læge- og sundhedstjenester. Behandlingen tillades dog kun, hvis den foretages af en erhvervsudøvende i sundhedssektoren, der har tavshedspligt, eller af en anden person med tilsvarende tavshedspligt[305].

I Europarådets henstilling om medicinske oplysninger fra 1997 overføres principperne i konvention 108 til databehandling på det lægelige område[306]. De foreslåede regler er i overensstemmelse med databeskyttelsesdirektivets regler, for så vidt angår de legitime formål med behandling af medicinske oplysninger, den krævede tavshedspligt for personer, der anvender medicinske oplysninger, og de registreredes ret til gennemsigtighed og indsigt, berigtigelse og sletning. Medicinske oplysninger, som behandles lovligt af erhvervsudøvende i sundhedssektoren, 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 artikel 8 i EMK[307].

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 data.

305 Se også Menneskerettighedsdomstolen, *Biriuk mod Litauen*, nr. 23373/03, 25. november 2008.

306 Europarådet, Ministerudvalget (1997), henstilling Rec(97)5 til medlemsstaterne om beskyttelse af medicinske oplysninger, 13. februar 1997.

307 Menneskerettighedsdomstolen, nr. 1585/09, *Avilkina m.fl. mod Rusland*, 6. juni 2013, præmis 53 (ikke endelig).

Videnskabelig forskning anerkendes udtrykkeligt som en grund til at opbevare data 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 2.1.3.

Der er ført intensive drøftelser på nationalt og europæisk plan om initiativer vedrørende lagring af data om en patients lægelige behandling i elektroniske patientjournaler[308]. Et særligt aspekt af landsdækkende elektroniske patientjournalsystemer er deres tilgængelighed på tværs af grænser, et emne, der især er relevant for drøftelserne af grænseoverskridende sundhedspleje i EU[309].

Et andet område, hvor man drøfter nye bestemmelser, er kliniske forsøg, dvs. forsøg med nye lægemidler på patienter i et dokumenteret forskningsmiljø – et område, hvor databeskyttelse har stor betydning. Kliniske forsøg med lægemidler til mennesker er reguleret ved Europa-Parlamentets og Rådets direktiv 2001/20/EF af 4. april 2001 om indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser om anvendelse af god klinisk praksis ved gennemførelse af kliniske forsøg med lægemidler til human brug (*direktivet om kliniske forsøg*)[310]. I december 2012 fremsatte Kommissionen forslag om en forordning til erstatning for direktivet om kliniske forsøg med henblik på at gøre forsøgsprocedurer mere ensartede og effektive[311].

308 Artikel 29-Gruppen (2007), *arbejdsdokument vedrørende behandling af personlige sundhedsoplysninger i elektroniske patientjournaler (EPJ)*, WP 131, Bruxelles, den 15. februar 2007.

309 Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser, EUT 2011 L 88.

310 Europa-Parlamentets og Rådets direktiv 2001/20/EF af 4. april 2001 om indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser om anvendelse af god klinisk praksis ved gennemførelse af kliniske forsøg med lægemidler til human brug, EFT 2001 L 121.

311 Europa-Kommissionen (2012), *forslag til Europa-Parlamentets og Rådets forordning om kliniske forsøg med humanmedicinske lægemidler og om ophævelse af direktiv 2001/20/EF*, COM(2012) 369 final, Bruxelles, den 17. juli 2012.

En række andre lovgivningsmæssige og andre initiativer vedrørende personoplysninger i sundhedssektoren behandles aktuelt på EU-plan[312].

8.4. Databehandling i statistisk øjemed

Hovedpunkter

- Oplysninger, der indsamles i statistisk øjemed, må ikke anvendes til noget andet formål.
- Oplysninger, der er indsamlet legitimt til et andet formål, må anvendes i statistisk øjemed, såfremt der ved national lov gives tilstrækkelige garantier, som opfyldes af brugerne. Til det formål bør der især sikres anonymisering og pseudonymisering inden videregivelse til tredjemand.

I databeskyttelsesdirektivet nævnes behandling i statistisk øjemed i forbindelse med mulige undtagelser fra principperne om databeskyttelse. I henhold til direktivets artikel 6, stk. 1, litra b), kan der afviges fra princippet om formålsbegrænsning, hvis der er tale om yderligere anvendelse af oplysningerne i statistisk øjemed, men de nødvendige garantier skal være sikret ved national lov. I henhold til direktivets artikel 13, stk. 2, kan retten til indsigt begrænses ved national lovgivning, såfremt oplysningerne alene anvendes i statistisk øjemed. Igen skal de nødvendige garantier være sikret ved national lov. I den sammenhæng opstiller databeskyttelsesdirektivet et specifikt krav om, at ingen af de oplysninger, der indsamles eller oprettes i forbindelse med statistisk forskning, må benyttes som grundlag for konkrete afgørelser om registrerede.

Selv om oplysninger, som lovligt er indsamlet af en registeransvarlig, må genanvendes af denne registeransvarlige til dennes egne statistiske formål – såkaldte sekundære statistikker – skal oplysningerne anonymiseres eller pseudonymiseres, afhængigt af indholdet, inden de videregives til tredjemand i statistisk øjemed, medmindre den registrerede har givet sit samtykke dertil, eller det specifikt er fastsat ved national lov. Dette følger af kravet om de fornødne garantier i databeskyttelsesdirektivets artikel 6, stk. 1, litra b).

312 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, den 27. marts 2013.

Oplysninger anvendes primært i statistisk øjemed i forbindelse med officiel statistik, der udarbejdes 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 statistiske kontorer. Tjenestemænd ved de statistiske kontorer, har særlig tavshedspligt, som nøje overholdes, da det er afgørende for borgernes tillid, som er nødvendig, hvis de statistiske kontorer skal have adgang til oplysninger.

Forordning (EF) nr. 223/2009 om europæiske statistikker indeholder vigtige regler om beskyttelse af personoplysninger i officiel statistik og er derfor også relevant for bestemmelser om officiel statistik på nationalt plan[313]. Forordningen fastholder princippet om, at der skal være et tilstrækkeligt præcist retsgrundlag for behandling af oplysninger i officiel statistik[314].

> Eksempel: I sagen *Huber mod Tyskland*[315] fandt EU-Domstolen, at en myndigheds indsamling og lagring af personoplysninger i statistisk øjemed ikke i sig selv udgjorde et tilstrækkeligt retsgrundlag til at gøre behandlingen lovlig. I henhold til den lov, der omhandlede behandling af personoplysninger, skulle kravet om nødvendighed også opfyldes, hvilket ikke var tilfældet i denne sag.

Europarådet udstedte i 1997 henstillingen vedrørende statistiske oplysninger, som omhandler udarbejdelsen af statistik i offentlige og private sektorer[316]. Ved denne henstilling introducerede Europarådet principper, der svarer til hovedreglerne i databeskyttelsesdirektivet, som er beskrevet ovenfor. Mere detaljerede regler gives i de efterfølgende udgaver.

Oplysninger, der indsamles af en registeransvarlig i statistisk øjemed, må ikke anvendes til noget andet formål, men oplysninger, der er indsamlet til andre formål,

313 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 2009 L 87.

314 Dette princip uddybes i Eurostats adfærdskodeks, der i overensstemmelse med artikel 11 i forordningen om europæiske statistikker skal give etisk vejledning i, hvordan europæiske statistikker skal udarbejdes, herunder hensigtsmæssig anvendelse af personoplysninger. Adfærdskodeksen findes på: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 EU-Domstolen, C-524/06, *Huber mod Tyskland*, 16. december 2008, se navnlig præmis 68.

316 Europarådet, Ministerudvalget (1997), henstilling Rec(97)18 til medlemsstaterne om beskyttelse af personoplysninger, der indsamles og behandles i statistisk øjemed, 30. september 1997.

må anvendes i statistisk øjemed. Henstillingen vedrørende statistiske oplysninger tillader endda, at oplysninger videregives til tredjemand, hvis det alene er i statistisk øjemed. I sådanne tilfælde skal parterne indgå skriftlig aftale om omfanget af den yderligere anvendelse i statistisk øjemed. Da dette ikke kan erstatte den registreredes samtykke, antages det, at yderligere passende garantier skal være fastsat ved national lov for at minimere risiciene for misbrug af personoplysninger, f.eks. en pligt til 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 bør også gælde personer, der er ansat til at indsamle oplysninger fra registrerede eller andre personer.

Hvis en statistisk undersøgelse, der anvender personoplysninger, ikke er omhandlet i loven, skal den registrerede give sit samtykke til anvendelsen af vedkommendes oplysninger for at gøre anvendelsen lovlig, eller den registrerede skal i det mindste have mulighed for at gøre indsigelse. Hvis oplysninger indsamles i statistisk øjemed ved at interviewe personer, skal disse personer klart oplyses om, hvorvidt videregivelse af oplysninger er påkrævet i henhold til national lov. Følsomme data bør aldrig indsamles på en sådan måde, at en person kan identificeres, medmindre det udtrykkeligt er tilladt i henhold til national lovgivning.

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. Oplysninger bør således pseudonymiseres, og krypteringsnøglen eller listen med identificerende synonymer bør lagres adskilt fra de pseudonymiserede oplysninger.

8.5. Finansielle oplysninger

Hovedpunkter

- Selv om finansielle oplysninger ikke er følsomme oplysninger som defineret i konvention 108 eller databeskyttelsesdirektivet, kræver behandlingen heraf særlige garantier for at sikre oplysningernes rigtighed og sikkerhed.
- Elektroniske betalingssystemer skal have indbygget beskyttelse, dvs. "privacy by design".
- Der opstår særlige databeskyttelsesproblemer på dette område, fordi der er behov for effektive autentifikationsmekanismer.

Eksempel: I sagen *Michaud mod Frankrig*[317] anfægtede sagsøgeren, en fransk advokat, sin pligt til i henhold til fransk lovgivning at indberette mistanke vedrørende hans klienters mulige hvidvaskning af penge. Menneskerettighedsdomstolen 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 den europæiske menneskerettighedskonvention, 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 eller strafbare handlinger. Eftersom advokater kun under meget begrænsede omstændigheder har pligt til at indberette mistanke, fandt Menneskerettighedsdomstolen, at denne forpligtelse var forholdsmæssig, og konkluderede, at artikel 8 ikke var blevet overtrådt.

Anvendelsen af den generelle ramme for databeskyttelse, der er fastsat i konvention 108, i forhold til betalinger blev udviklet af Europarådet i henstilling Rec(90)19 fra 1990[318]. Denne henstilling præciserer omfanget af lovlig indsamling og anvendelse af oplysninger i forbindelse med betalinger, især ved hjælp af betalingskort. Den foreslår endvidere de nationale lovgivere detaljerede bestemmelser vedrø-

317 Menneskerettighedsdomstolen, *Michaud mod Frankrig*, nr. 12323/11, 6. december 2012. Se også Menneskerettighedsdomstolen, *Niemietz mod Tyskland*, nr. 13710/88, 16. december 1992, præmis 29, og Menneskerettighedsdomstolen, *Halford mod Det Forenede Kongerige*, nr. 20605/92, 25. juni 1997, præmis 42.

318 Europarådet, Ministerudvalget (1990), henstilling nr. R(90)19 om beskyttelse af personoplysninger, der anvendes ved betaling og andre tilknyttede handlinger, 13. september 1990.

rende grænserne for meddelelse af betalingsoplysninger til tredjemand, tidsfrister for lagring af oplysninger, gennemsigtighed, datasikkerhed og grænseoverskridende videregivelse af oplysninger samt tilsyn og retsmidler. De foreslåede løsninger svarer til dem, der senere blev fremsat som EU's generelle ramme for databeskyttelse i databeskyttelsesdirektivet.

Der er oprettet en række retlige instrumenter for regulering af markeder for finansielle instrumenter og kreditinstitutters og investeringsselskabers virksomhed[319]. Andre retlige instrumenter medvirker til at bekæmpe insiderhandel og markedsmanipulation[320]. Følgende kritiske problemer påvirker databeskyttelse på disse områder:

- 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
- 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

319 Europa-Kommissionen (2011), *forslag til Europa-Parlamentets og Rådets direktiv om markeder for finansielle instrumenter og ophævelse af Europa-Parlamentets og Rådets direktiv 2004/39/EF*, KOM(2011) 656 endelig, Bruxelles, den 20. oktober 2011, Europa-Kommissionen (2011), *forslag til Europa-Parlamentets og Rådets forordning om markeder for finansielle instrumenter og om ændring af forordning [EMIR] om OTC-derivater, centrale modparter og transaktionsregistre*, KOM(2011) 652 endelig, Bruxelles, den 20. oktober 2011, Europa-Kommissionen (2011), *forslag til Europa-Parlamentets og Rådets direktiv om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber og om ændring af Europa-Parlamentets og Rådets direktiv 2002/87/EF om supplerende tilsyn med kreditinstitutter, forsikringsselskaber og investeringsselskaber i et finansielt konglomerat*, KOM(2011) 453 endelig, Bruxelles, den 20. juli 2011.

320 Europa-Kommissionen (2011), *forslag til Europa-Parlamentets og Rådets forordning om insiderhandel og kursmanipulation (markedsmisbrug)*, KOM(2011) 651 endelig, Bruxelles, den 20. oktober 2011, Europa-Kommissionen (2011), *forslag til Europa-Parlamentets og Rådets direktiv om strafferetlige sanktioner for insiderhandel og kursmanipulation*, KOM(2011) 654 endelig, Bruxelles, den 20. oktober 2011.

- 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[321] eller grænseoverskridende betaling via bankoverførsler, som uundgåeligt medfører videregivelse af personoplysninger[322].

321 Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 af 16. september 2009 om kreditvurderingsbureauer, EUT 2009 L 302, Europa-Kommissionen, *forslag til Europa-Parlamentets og Rådets forordning om ændring af forordning (EF) nr. 1060/2009 om kreditvurderingsbureauer*, KOM(2010) 289 endelig, Bruxelles, den 2. juni 2010.

322 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 2007 L 319.

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.

EDRi, *An introduction to data protection*, Bruxelles, findes på: www.edri.org/files/paper06_datap.pdf.

Frowein, J. og Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. og Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. og Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

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,* vol. 4, nr. 5, s. 193-220, findes på: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. og Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Kapitel 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

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.

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*, vol. 57, nr. 6, s. 1701-1777.

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*, findes på: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Kapitel 3-5

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, München, 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*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. og Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Den Europæiske Unions Agentur for Grundlæggende Rettigheder) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Den Europæiske Unions Publikationskontor.

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (konferenceudgave), Wien.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Den Europæiske Unions Publikationskontor.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, findes på: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Kapitel 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. og Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European databeskyttelseslovgivningen*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Kapitel 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Den Europæiske Unions Publikationskontor, findes på: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* ERA Forum, vol. 13, nr. 3, s. 381-395.

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*, vol. 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, findes på: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Kapitel 8

Büllesbach, A., Gijrath, S., Poullet, Y. og Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. og Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, 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*, vol. 36, nr. 5, s. 722-776.

Rosemary, J. og Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Retspraksis

Eksempler på Den Europæiske Menneskerettighedsdomstol 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
Odièvre mod Frankrig [GC], nr. 42326/98, 13. februar 2003

Afvejning af databeskyttelse i forhold til ytringsfrihed

Axel Springer AG mod Tyskland [GC], nr. 39954/08, 7. februar 2012
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

Udfordringer i forbindelse med databeskyttelse på internettet

K.U. mod Finland, nr. 2872/02, 2. december 2008

Korrespondance

Amann mod Schweiz [GC], nr. 27798/95, 16. februar 2000
Bernh Larsen Holding AS m.fl. mod Norge, nr. 24117/08, 14. marts 2013
Cemalettin Canli mod Tyrkiet, nr. 22427/04, 18. november 2008

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
McMichael mod Det Forenede Kongerige, nr. 16424/90, 24. februar 1995
M.G. mod Det Forenede Kongerige, nr. 39393/98, 24. september 2002
Rotaru mod Rumænien [GC], nr. 28341/95, 4. maj 2000
S. og Marper mod Det Forenede Kongerige, nr. 30562/04 og 30566/04, 4. december 2008
Shimovolos mod Rusland, nr. 30194/09, 21. juni 2011
Turek mod Slovakiet, nr. 57986/00, 14. februar 2006

Strafferegistre

B.B. mod Frankrig, nr. 5335/06, 17. december 2009
M.M. mod Det Forenede Kongerige, nr. 24029/07, 13. november 2012

Dna-databaser

S. og Marper mod Det Forenede Kongerige, nr. 30562/04 og 30566/04, 4. december 2008

GPS-data

Uzun mod Tyskland, nr. 35623/05, 2. september 2010

Helbredsoplysninger

Biriuk mod Litauen, nr. 23373/03, 25. november 2008
I. mod Finland, nr. 20511/03, 17. juli 2008
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
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

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
Copland mod Det Forenede Kongerige, nr. 62617/00, 3. april 2007
Cotlet mod Rumænien, nr. 38565/97, 3. juni 2003
Kruslin mod Frankrig, nr. 11801/85, 24. april 1990
Lambert mod Frankrig, nr. 23618/94, 24. august 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
Halford mod Det Forenede Kongerige, nr. 20605/92, 25. juni 1997
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

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

Segerstedt-Wiberg m.fl. mod Sverige, nr. 62332/00, 6. juni 2006

Retten til indsigelse

Leander mod Sverige, nr. 9248/81, 26. marts 1987
Mosley mod Det Forenede Kongerige, nr. 48009/08, 10. maj 2011
M.S. mod Sverige, nr. 20837/92, 27. august 1997
Rotaru mod Rumænien [GC], nr. 28341/95, 4. maj 2000

Følsomme oplysninger

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, nr. 30562/04 og 30566/04, 4. december 2008

Tilsyn og håndhævelse (forskellige aktørers rolle, herunder databeskyttelsesmyndigheder)

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 "21 Décembre 1989" m.fl. mod Rumænien, nr. 33810/07 og 18817/08, 24. maj 2011
Bykov mod Rusland [GC], nr. 4378/02, 10. marts 2009
Kennedy mod Det Forenede Kongerige, nr. 26839/05, 18. maj 2010
Klass m.fl. mod Tyskland, nr. 5029/71, 6. september 1978
Rotaru mod Rumænien [GC], nr. 28341/95, 4. maj 2000
Taylor-Sabori mod Det Forenede Kongerige, nr. 47114/99, 22. oktober 2002
Uzun mod Tyskland, nr. 35623/05, 2. september 2010
Vetter mod Frankrig, nr. 59842/00, 31. maj 2005

Videoovervågning

Köpke mod Tyskland, 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

C-73/07, *Tietosuojavaltuutettu mod Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16. december 2008
[Begrebet "i journalistisk øjemed" som defineret i databeskyttelsesdirektivets artikel 9]

Forenede sager C-92/09 og C-93/09, *Volker und Markus Schecke GbR og Hartmut Eifert mod Land Hessen*, 9. november 2010
[Proportionalitet af retlig forpligtelse til at offentliggøre personoplysninger om modtagere af støtte fra visse EU-landbrugsfonde]

C-101/01, *Bodil Lindqvist*, 6. november 2003
[Lovlighed af privatpersons offentliggørelse af oplysninger om andres privatliv på internettet]

C-131/12, *Google Spain, S.L., Google Inc. mod Agencia Española de Protección de Datos, Mario Costeja González, præjudiciel forelæggelse fra Audiencia Nacional* (Spanien) indgivet den 9. marts 2012, 25. maj 2012, verserende
[Søgemaskineudbyderes forpligtelser til efter anmodning fra den registrerede at undlade at vise personoplysninger i søgeresultater]

C-270/11, *Europa-Kommissionen mod Sverige*, 30. maj 2013
[Bøde for manglende gennemførelse af direktiv]

C-275/06, *Productores de Música de España (Promusicae) mod Telefónica de España SAU*, 29. januar 2008
[Internetudbyderes forpligtelse til at videregive identiteten af brugere af KaZaA-filudvekslingsprogrammer til en sammenslutning vedrørende beskyttelse af intellektuel ejendomsrettighed]

C-288/12, *Europa-Kommissionen mod Ungarn*, 8. april 2014
[Lovlighed af afskaffelsen af den nationale databeskyttelsesmyndighed]

C-291/12, *Michael Schwarz mod Stadt Bochum*, forslag til afgørelse fremsat af generaladvokaten, 13. juni 2013
[Overtrædelse af EU's primære lov ved forordning (EF) nr. 2252/2004 ved krav om lagring af fingeraftryk i pas]

C-360/10, *SABAM mod Netlog N.V.*, 16. februar 2012
[Sociale netværksudbyderes forpligtelse til at forhindre netværksbrugeres ulovlige anvendelse af musikværker og audiovisuelle værker]

Forenede sager C-465/00, C-138/01 og C-139/01, *Rechnungshof mod Österreichischer Rundfunk m.fl. og Neukomm und Lauermann mod Österreichischer Rundfunk*, 20. maj 2003
[Proportionalitet af retlig forpligtelse til at offentliggøre personoplysninger om løn, der gives til visse kategorier af medarbejdere ved institutioner i den offentlige sektor]

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 lov]

C-518/07, *Europa-Kommissionen mod Tyskland*, 9. marts 2010
[En national tilsynsmyndigheds uafhængighed]

C-524/06, *Huber mod Tyskland*, 16. december 2008
[Lovlighed af lagring af oplysninger om udlændinge i et statistisk register]

C-543/09, *Deutsche Telekom AG mod Tyskland*, 5. maj 2011
[Nødvendighed af fornyet samtykke]

C-553/07, *College van burgemeester en wethouders van Rotterdam mod M.E.E. Rijkeboer*, 7. maj 2009
[Den registreredes ret til indsigt]

Forenede sager C-293/12 and C-594/12, *Digital Rights Ireland og Seitling m.fl.*, 8. April 2014
[Overtrædelse af EU's primære lov ved datalagringsdirektivet]

C-614/10, *Europa-Kommissionen mod Østrig*, 16. oktober 2012
[En national tilsynsmyndigheds uafhængighed]

Retspraksis vedrørende forordningen om databeskyttelse inden for EU-institutionerne

C-28/08 P, *Europa-Kommissionen mod The Bavarian Lager Co. Ltd.*, 29. juni 2010
[Aktindsigt]

C-41/00 P, *Interporc Im- und Export GmbH mod Europa-Kommissionen*, 6. marts 2003
[Aktindsigt]

F-35/08, *Dimitrios Pachtitis mod Europa-Kommissionen og EPSO*, 15. juni 2010
[Brug af personoplysninger i forbindelse med ansættelse ved EU-institutioner]

F-46/09, *V mod Europa-Parlamentet*, 5. juli 2011
[Brug af personoplysninger i forbindelse med ansættelse ved EU-institutioner]

Liste over sager

Domstolens retspraksis

Menneskerettighedsdomstolens retspraksis

Nationale domstoles retspraksis

Den Europæiske Unions Agentur for Grundlæggende Rettigheder
Den Europæiske Menneskerettighedsdomstol – Europarådet

Håndbog om europæisk databeskyttelseslovgivning

2015 — 209 s. — 14,8 × 21 cm

ISBN 978-92-871-9949-2 (Europarådet)
ISBN 978-92-9239-495-0 (FRA)
doi:10.2811/73615

En stor mængde yderligere oplysninger om Den Europæiske Unions Agentur for Grundlæggende Rettigheder er tilgængelige på internettet via FRA's hjemmeside (http://fra.europa.eu).

Yderligere oplysninger om Den Europæiske Menneskerettighedsdomstols retspraksis findes på Domstolens hjemmeside: www.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.

10.2811/73615
TK-01-13-772-DA-C

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

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. De teknologiske fremskridt udvider mulighederne for f.eks. overvågning, opfangelse af kommunikation og lagring af data, som alt sammen skaber store udfordringer for retten til databeskyttelse. Denne håndbog har til formål at give jurister, som ikke er specialister inden for databeskyttelse, kendskab til dette juridiske område. Den giver en oversigt over EU's og Europarådets gældende retlige rammer. Den forklarer vigtig retspraksis, opsummerer vigtige afgørelser truffet af både Den Europæiske Menneskerettighedsdomstol og EU-Domstolen. Hvis der ikke findes retspraksis, vises realistiske illustrationer med hypotetiske scenarier. Målet med denne håndbog er således at sikre, at retten til databeskyttelse opretholdes med fuld kraft.

DEN EUROPÆISKE UNIONS AGENTUR FOR GRUNDLÆGGENDE RETTIGHEDER
Schwarzenbergplatz 11 – 1040 Wien – Østrig
Tlf. +43 (1) 580 30-60 – Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

EUROPARÅDET
DEN EUROPÆISKE MENNESKERETTIGHEDSDOMSTOL
67075 Strasbourg Cedex – Frankrig
Tlf. +33 (0) 3 88 41 20 00 – Fax +33 (0) 3 88 41 27 30
www.echr.coe.int – publishing@echr.coe.int

Publikationskontoret

ISBN 978-92-871-9949-2 (Europarådet)
ISBN 978-92-9239-495-0 (FRA)