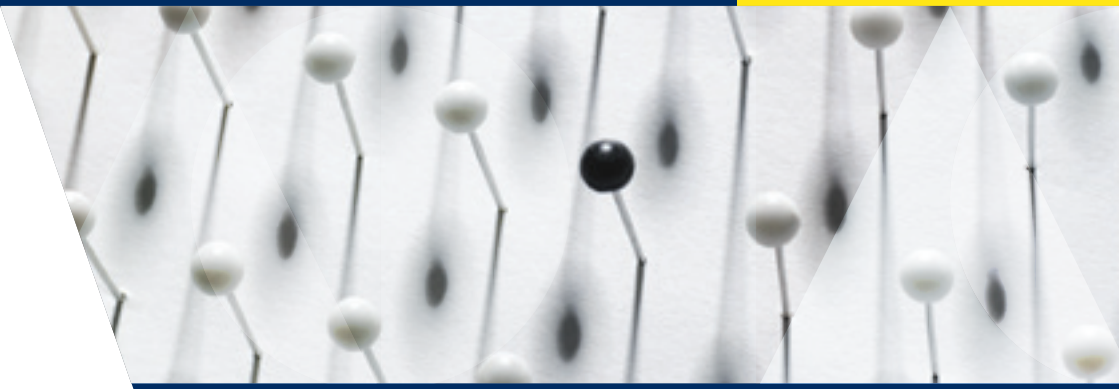
HANDBOK



Handbok om den europeiska lagstiftningen om skydd av personuppgifter

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 till handboken färdigställdes i april 2014.
Uppdateringar kommer i framtiden att finnas på FRA:s webbplats: fra.europa.eu, Europarådets webbplats: http://coe.int/dataprotection och Europadomstolens webbplats under menyn Case-Law (rättspraxis) på: http://echr.coe.int.

Europe Direct är en tjänst som hjälper dig att få svar på dina frågor om Europeiska unionen.

Gratis telefonnummer (*):

00 800 6 7 8 9 10 11

(*) Varken informationen eller samtalen kostar i regel något (men vissa operatörer, telefonkiosker och hotell kan ta betalt för samtalen).

Foto (titelsidan & insidan): © iStockphoto

En stor mängd övrig information om Europeiska unionen är tillgänglig på internet via Europa-servern (http://europa.eu).

Luxemburg: Europeiska unionens publikationsbyrå, 2015

ISBN 978-92-871-9932-4 (Europarådet)
ISBN 978-92-9239-499-8 (FRA)
doi:10.2811/73936

Printed in Belgium

Tryckt på papper som återvunnits utan användning av klor (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

Handbok om den europeiska lagstiftningen om skydd av personuppgifter

Förord

Denna handbok om den europeiska lagstiftningen om skydd av personuppgifter har utarbetats gemensamt av Europeiska unionens byrå för grundläggande rättigheter (FRA) och Europarådet tillsammans med Europadomstolens kansli. Det är den tredje i en serie av juridiska handböcker som utarbetats gemensamt av FRA och Europarådet. I mars 2011 publicerades en första handbok om lagstiftning mot diskriminering i Europa och i juni 2013 en andra om europeisk lagstiftning på området asyl, gränser och invandring.

Vi har beslutat att fortsätta vårt samarbete om ett högst aktuellt tema som påverkar oss alla, nämligen skyddet av personuppgifter. Europa har ett av de mest skyddande systemen på området, och det bygger på Europarådets konvention 108, Europeiska unionens instrument liksom rättspraxis från Europadomstolen och EU-domstolen.

Syftet med handboken är att höja medvetenheten och förbättra kunskaperna om gällande bestämmelser om skydd av personuppgifter inom Europeiska unionens och Europarådets medlemsstater, genom att fungera som en huvudsaklig referenskälla för läsaren. Den är utformad för icke specialister som är jurister, domare, nationella myndigheter för skydd av personuppgifter och andra personer som arbetar inom området.

När Lissabonfördraget trädde i kraft i december 2009 blev EU:s stadga om de grundläggande rättigheterna juridiskt bindande och därmed blev rätten till skydd av personuppgifter upphöjd till en separat grundläggande rättighet. En bättre förståelse av Europarådets konvention 108 och av EU:s instrument, vilka banat väg för skyddet av personuppgifter i Europa, liksom av rättspraxis från EU-domstolen och Europadomstolen, är avgörande för att skydda denna grundläggande rättighet.

Vi vill tacka Ludwig Boltzmann-institutet för mänskliga rättigheter för dess bidrag till utarbetandet av denna handbok. Vi vill också uttrycka vår tacksamhet till Europeiska datatillsynsmannen för återkoppling under utarbetandet. Vi tackar särskilt enheten för dataskydd vid Europeiska kommissionen under förberedelserna av handboken.

Philippe Boillat

Generaldirektör för mänskliga rättigheter och rättsstaten, Europarådet

Morten Kjaerum

Direktör vid Europeiska unionens byrå för mänskliga rättigheter

Innehåll

Förkortningar och akronymer

BCR	(Binding corporate rules) Bindande företagsregler
CETS	(Council of Europe Treaty Series) Europarådets fördragsserie
CRM	Customer relations management (hantering av kundrelationer)
C-SIS	Den centrala delen av Schengens informationssystem
EES	Europeiska ekonomiska samarbetsområdet
EFTA	Europeiska frihandelssammanslutningen
EG	Europeiska gemenskapen
ENISA	Europeiska unionens byrå för nät- och informationssäkerhet
Esma	Europeiska värdepappers- och marknadsmyndigheten
eTEN	Transeuropeiska telekommunikationsnät
EU	Europeiska unionen
eu-LISA	Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa
Europakonventionen	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EuroPriSe	Europeisk integritetsmärkning
FEU	Fördraget om Europeiska unionen, EU-fördraget
FEUF	Fördraget om Europeiska unionens funktionssätt, EUF-fördraget
FN	Förenta nationerna
FRA	Europeiska unionens byrå för grundläggande rättigheter
GPS	(Global positioning system) Satellitbaserad positionsbestämning
Konvention 108	Konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (Europarådet)
N-SIS	Nationell del av Schengens informationssystem

OECD	Organisationen för ekonomiskt samarbete och utveckling
PIN	Personligt identifieringsnummer
PNR	(Passenger name record) Passageraruppgifter
SEPA	(Single Euro Payments Area) Gemensamt eurobetalningsområde
SIS	Schengens informationssystem
Stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIS	Tullinformationssystem
VIS	Informationssystem för viseringar

Hur handboken bör användas

Handboken innehåller en översikt över lagstiftning som är tillämplig på skydd av personuppgifter inom Europeiska unionen (EU) och Europarådet.

Handboken är utformad för att bistå praktiserande jurister som inte är specialiserade på området skydd av personuppgifter. Den är avsedd för jurister, domare eller andra praktiserande liksom för dem som arbetar inom andra organ, inklusive icke-statliga organisationer, som kan ställas inför juridiska spörsmål rörande skydd av personuppgifter.

Handboken är en första referenspunkt till både EU-lagstiftningen och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) när det gäller skydd av personuppgifter. Den förklarar hur området regleras enligt EU-lagstiftningen och Europakonventionen samt Europarådets konvention om skydd av enskilda vid automatisk behandling av personuppgifter (konvention 108) och andra av Europarådets instrument. I varje kapitel finns först en tabell över tillämpliga rättsliga bestämmelser, inklusive viktig utvald rättspraxis inom de två separata europeiska rättsliga systemen. Därefter presenteras relevant lagstiftning från dessa två europeiska ordningar vartefter de är tillämpliga för ämnet. På så sätt kan läsaren se när de två rättsliga systemen överensstämmer och när de skiljer sig åt.

I tabellerna i början av respektive kapitel anges ämnet för kapitlet och tillämpliga rättsliga bestämmelser samt andra relevanta ämnen, exempelvis rättspraxis. Ordningen mellan ämnen kan skilja sig något från textens struktur inom kapitlet, om det anses bidra till en kortfattad presentation av kapitlets innehåll. Tabellerna omfattar både Europarådets och EU:s lagstiftning. Detta bör hjälpa användarna att hitta den viktiga informationen i respektive situation, särskilt om de endast omfattas av Europarådets lagstiftning.

Jurister i stater utanför EU som är medlemsstater i Europarådet och parter till Europakonventionen och konvention 108 kan få tillgång till information som är relevant för det egna landet genom att gå direkt till avsnitten om Europarådet. Jurister i EU-medlemsstater behöver använda båda sektionerna, eftersom dessa stater omfattas av båda rättsordningarna. För dem som behöver mer information om en särskild fråga finns en referensförteckning till mer specialiserat material i handbokens avsnitt ”Ytterligare läsning”.

Europarådets lagstiftning presenteras genom korta hänvisningar till utvalda mål från Europadomstolen. Dessa har valts ut från ett stort antal domar och beslut i Europadomstolen om frågor som rör skydd av personuppgifter.

EU-lagstiftning finns i lagstiftningsåtgärder som har antagits, i relevanta bestämmelser i fördragen och i Europeiska unionens stadga om de grundläggande rättigheterna, enligt tolkningen i EU-domstolens rättspraxis, (före 2009: EG-domstolen).

Den rättspraxis som beskrivs eller citeras i handboken innehåller en mängd rättspraxis från både Europadomstolen och EU-domstolen. Riktlinjerna i slutet av handboken är avsedda att bistå läsaren vid sökning av rättspraxis på nätet.

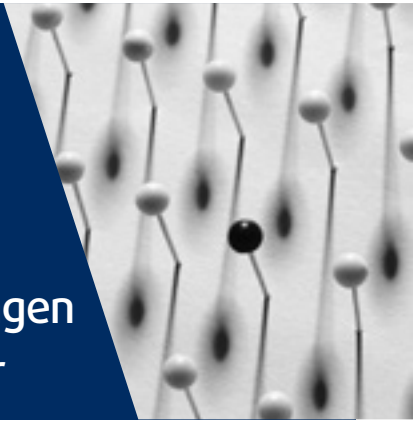
Praktiska illustrationer med hypotetiska scenarier har lagts in i textrutor med blå bakgrund för att ytterligare illustrera tillämpningen av de europeiska reglerna om skydd av personuppgifter i praktiken, särskilt när ingen specifik rättspraxis från Europadomstolen eller EU-domstolen finns i ämnet. Andra textrutor, med grå bakgrund, ger exempel från andra källor än rättspraxis, exempelvis lagstiftning.

Handboken inleds med en kort beskrivning av de två rättsliga systemens roll såsom de fastställs i Europakonventionen och EU-lagstiftningen (kapitel 1). Kapitel 2–8 omfattar följande frågor:

- terminologi om skydd av personuppgifter;
- huvudprinciper för den europeiska lagstiftningen om skydd av personuppgifter;
- bestämmelser i den europeiska lagstiftningen om skydd av personuppgifter;
- de registrerades rättigheter och dessas genomförande;
- gränsöverskridande uppgiftsflöde;
- skydd av personuppgifter inom polisiära och straffrättsliga myndigheter;
- annan specifik europeisk lagstiftning om skydd av personuppgifter.

1

Sammanhang och bakgrund för den europeiska lagstiftningen om skydd av personuppgifter



EU	Frågor som täcks	Europarådet
Rätten till skydd av personuppgifter		
Direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (nedan kallat *dataskyddsdirektivet*), EGT L 281, 23.11.1995		Europakonventionen, artikel 8 (rätt till respekt för privat- och familjeliv, hem och korrespondens). Konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (konvention 108)
Avvägning av rättigheter		
EU-domstolen, förenade målen C-92/09 och C93/09, *Volker och Markus Schecke GbR och Hartmut Eifert mot Land Hessen*, 2010	**Allmänt**	
EU-domstolen C-73/07, *Tietosuojavaltuutettu mot Satakunnan Markkinapörssi Oy och Satamedia Oy*, 2008	**Yttrandefrihet**	Europadomstolen, *Axel Springer AG mot Tyskland*, 2012 Europadomstolen, *Mosley mot Förenade kungariket*, 2011
	Frihet för konsten och vetenskapen	Europadomstolen, *Vereinigung bildender Künstler mot Österrike*, 2007
EU-domstolen, C-275/06, *Productores de Música de España (Promusicae) mot Telefónica de España SAU*, 2008	**Skydd av egendom**	
EU-domstolen, C-28/08 P, *Europeiska kommissionen mot The Bavarian Lager Co. Ltd*, 2010	**Tillgång till handlingar**	Europadomstolen, *Társaság a Szabadságjogokért mot Ungern*, 2009

1.1. Rätten till skydd av personuppgifter

Viktiga punkter

- Enligt artikel 8 i Europakonventionen utgör rätten till skydd mot insamling och användning av personuppgifter en del av rätten till respekt för privat- och familjeliv, hem och korrespondens.
- Europadomstolens konvention 108 är det första internationellt bindande instrumentet som uttryckligen tar upp skyddet av personuppgifter.
- I EU-lagstiftningen reglerades skyddet av personuppgifter första gången i dataskyddsdirektivet.
- I EU-lagstiftningen har skyddet av personuppgifter erkänts som en grundläggande rättighet.

Rätten till skydd av en enskilds privata sfär mot intrång från andra, särskilt från staten, fastställdes i ett internationellt rättsligt instrument för första gången i artikel 12 om respekten för privat- och familjeliv i FN:s allmänna förklaring om de mänskliga rättigheterna från 1948.[1] Förklaringen bidrog till utvecklingen av andra instrument för mänskliga rättigheter i Europa.

1.1.1. Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna

Europarådet bildades i efterdyningarna efter andra världskriget för att samla Europas stater och främja rättsstaten, demokrati, mänskliga rättigheter och social utveckling. Därför antogs år 1950 Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, som trädde i kraft 1953.

Staterna har en internationell skyldighet att följa konventionen. Europaparlamentets alla medlemsstater har nu införlivat eller verkställt konventionen i sin nationella lagstiftning, och förbinder sig att agera i enlighet med konventionens bestämmelser.

För att säkerställa att de avtalsslutande parterna uppfyller sina skyldigheter enligt konventionen inrättades Europadomstolen i Strasbourg i Frankrike 1959.

1 Förenta nationerna (FN), Allmän förklaring om de mänskliga rättigheterna, 10 december 1948.

Europadomstolen säkerställer att staterna uppfyller sina skyldigheter enligt konventionen genom att pröva klagomål från enskilda, grupper av enskilda, icke-statliga organisationer eller juridiska personer som anser att konventionen har överträtts. Under 2013 omfattade Europarådet 47 medlemsstater, varav 28 också var medlemmar i EU. En klagande till Europadomstolen behöver inte vara medborgare i någon av medlemsstaterna. Europadomstolen kan också granska mål mellan stater som en eller flera medlemsstater i Europarådet tagit upp mot en annan medlemsstat.

Rätten till skydd av personuppgifter ingår i rättigheterna som skyddas enligt artikel 8 i Europakonventionen, som garanterar rätten till respekt för privat- och familjeliv, hem och korrespondens och fastställer villkoren enligt vilka restriktioner för denna rätt är tillåten.[2]

I hela sin rättspraxis har Europadomstolen granskat många situationer där frågan om skydd av personuppgifter kommit upp, inte minst de som gäller avlyssning av kommunikation[3], olika former av övervakning[4] och skydd mot offentliga myndigheters lagring av personuppgifter.[5] Den har klargjort att artikel 8 i Europakonventionen inte endast innebar att staterna var skyldiga att avstå från alla åtgärder som kan innebära att rätten överträds, utan de hade under vissa omständigheter också en positiv skyldighet att aktivt säkerställa effektiv respekt för privat- och familjeliv.[6] Många av dessa fall kommer att tas upp i detalj i respektive kapitel.

1.1.2. Europarådets konvention 108

I och med framväxten av informationstekniken under 1960-talet utvecklades ett växande behov av mer detaljerade regler för att trygga enskilda och skydda deras (person)uppgifter. I mitten av 1970-talet antog Europarådets ministerkommitté olika resolutioner om skydd av personuppgifter, med hänvisning till artikel 8

2 Europarådet, Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, CETS nr 005, 1950.

3 Se exempelvis: Europadomstolen, *Malone mot Förenade kungariket*, nr 8691/79, 2 augusti 1984, Europadomstolen, *Copland mot Förenade kungariket*, nr 62617/00, 3 april 2007.

4 Se exempelvis: Europadomstolen, *Klass m.fl. mot Tyskland*, nr 5029/71, 6 september 1978, Europadomstolen, *Uzun mot Tyskland*, nr 35623/05, 2 september 2010.

5 Se exempelvis: Europadomstolen, *Leander mot Sverige*, nr 9248/81, 26 mars 1987; Europadomstolen, *S. och Marper mot Förenade kungariket*, nr 30562/04 och 30566/04, 4 december 2008.

6 Se exempelvis: Europadomstolen, *I. mot Finland*, nr 20511/03, 17 juli 2008; Europadomstolen, *K.U. mot Finland*, nr 2872/02, 2 december 2008.

i Europakonventionen.[7] År 1981 öppnades en konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (konvention 108)[8] för undertecknande. Konvention 108 var och är fortfarande det enda juridiskt bindande internationella instrumentet när det gäller skydd av personuppgifter.

Konvention 108 gäller för all databehandling som utförs av både den privata och offentliga sektorn, exempelvis databehandling som utförs av rättssystem och brottsbekämpande myndigheter. Den skyddar enskilda mot intrång, som kan ske i samband med insamling och behandling av personuppgifter, och försöker samtidigt reglera det gränsöverskridande flödet av personuppgifter. Vad gäller insamling och behandling av personuppgifter gäller principerna i konventionen framför allt rättvis och tillåten insamling och automatisk behandling av uppgifter, som lagras för angivna berättigade syften och inte för användning i syften som är oförenliga med dessa syften eller behålls längre än nödvändigt. De gäller också kvaliteten på uppgifterna. De ska framför allt vara lämpliga, relevanta och inte överdrivna (proportionerliga) samt korrekta.

Utöver att konventionen erbjuder garantier för insamling och behandling av personuppgifter förbjuds där också, i avsaknad av lämpliga rättsliga garantier, behandling av ”känsliga” uppgifter, såsom en persons etnicitet, politik, hälsa, religion, sexliv eller kriminella bakgrund.

Konventionen innehåller även enskildas rätt att veta att information lagras om honom eller henne och rätten att vid behov få den korrigerad. Restriktioner när det gäller rättigheterna i konventionen är endast möjliga när det handlar om ett överordnat intresse, såsom statens säkerhet eller försvar.

Även om konventionen medger ett fritt flöde av personuppgifter mellan de stater som är parter i konventionen, innehåller den även vissa restriktioner om dessa flöden till stater där rättsliga bestämmelser inte erbjuder motsvarande skydd.

7 Europarådet, ministerkommittén (1973), Resolution (73) 22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector (om skydd av enskildas privatliv gentemot elektroniska databanker i den privata sektorn), 26 september 1973; Europarådet, ministerkommittén (1974), Resolution (74) 29 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the public sector (om skydd av enskildas privatliv gentemot elektroniska databanker i den offentliga sektorn), 20 september 1974.

8 Europarådet, konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, Europarådet, CETS nr 108, 1981.

För att ytterligare utveckla de allmänna principerna och reglerna i konvention 108 har flera rekommendationer som inte är juridiskt bindande antagits av Europarådets ministerkommitté (se kapitel 7 och 8).

EU:s samtliga medlemsstater har ratificerat konvention 108. Under 1999 ändrades konvention 108 så att EU kunde bli en part.[9] Under 2001 antogs ytterligare ett protokoll till konvention 108, och därigenom infördes bestämmelser om gränsöverskridande flöden av uppgifter till parter som inte omfattades av konventionen, så kallade tredjeländer, och om det obligatoriska inrättandet av nationella tillsynsmyndigheter för dataskydd.[10]

Framtidsutsikter

Till följd av ett beslut att modernisera konvention 108 kunde efter ett offentligt samråd 2011 de två huvudmålsättningarna med arbetet fastställas: förstärka skyddet av privatlivet på det digitala området och stärka konventionens uppföljningsmekanism.

Även stater som inte är medlemmar i Europarådet kan ansluta sig till konvention 108, liksom icke-europeiska länder. Konventionens möjligheter som en allmän standard och dess öppna karaktär skulle kunna fungera som grund för att främja skyddet av personuppgifter på global nivå.

Hittills är 45 av de 46 avtalsparterna till konvention 108 medlemsstater i Europarådet. Uruguay, det första icke-europeiska landet blev medlem i augusti 2013 och Marocko, som av ministerkommittén har uppmanats att ansluta sig till konvention 108, håller på att formalisera anslutningen.

1.1.3. Europeiska unionens lagstiftning om skydd av personuppgifter

EU-lagstiftningen består av fördrag och sekundärlagstiftning. Fördragen, dvs. fördraget om Europeiska unionen (EU-fördraget; FEU) och fördraget om Europeiska

9 Europarådet, ändringar av konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108) som gör det möjligt för Europeiska gemenskaperna att ansluta sig, antagna av ministerkommittén, i Strasbourg, den 15 juni 1999, artikel 23.2 i konvention 108 i sin ändrade form.

10 Europarådet, Tilläggsprotokoll om tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter, CETS nr 181, 2001.

unionens funktionssätt (EUF-fördraget; FEUF), har godkänts av EU:s samtliga medlemsstater och betecknas också som ”EU:s primärlagstiftning”. EU:s förordningar, direktiv och beslut har antagits av EU:s institutioner som har fått denna befogenhet. De kallas ofta för ”EU:s sekundärlagstiftning”.

EU:s huvudsakliga rättsliga instrument om skydd av personuppgifter är Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (*dataskyddsdirektivet*).[11] Det antogs 1995, vid en tidpunkt när flera medlemsstater redan hade antagit nationell lagstiftning om skydd av personuppgifter. Fri rörlighet för varor, kapital, tjänster och personer inom den inre marknaden krävde fritt flöde av uppgifter, vilket inte kunde genomföras om inte medlemsstaterna kunde förlita sig på en enhetlig och hög nivå för skydd av personuppgifter.

Eftersom syftet med att anta dataskyddsdirektivet var att harmonisera[12] lagstiftningen om skydd av personuppgifter på nationell nivå, erbjuder direktivet en grad av precisering som är jämförbar med den (då) befintliga nationella lagstiftningen om skydd av personuppgifter. För EU-domstolen innebär direktiv 95/46 att ”skyddsnivån när det gäller enskilda personers fri- och rättigheter med avseende på behandlingen av personuppgifter måste vara likvärdig i alla medlemsstater”, att ”tillnärmningen av de nationella lagstiftningar som är tillämpliga på området inte får medföra någon inskränkning i det skydd de ger, utan ska i stället syfta till att garantera en hög skyddsnivå inom unionen” samt att ”harmoniseringen av de nämnda nationella lagstiftningarna således inte inskränker sig till en minimiharmonisering, utan leder till en i princip fullständig harmonisering”.[13] Medlemsstaterna har därför endast ett begränsat manöverutrymme när de införlivar direktivet.

Dataskyddsdirektivet är utformat för att ge underlag till principerna om rätten till privatliv som redan finns i konvention 108 och utvidga dem. Det faktum att samtliga 15 EU-medlemsstater 1995 också var avtalsparter till konvention 108 förhindrar att motstridiga regler inom dessa två rättsliga instrument antas. Dataskyddsdirektivet däremot utgår från möjligheten, enligt artikel 11 i konvention 108, att lägga till instrument för att utöka skyddet. Införandet av oberoende tillsyn som ett

11 Dataskyddsdirektivet, EGT L 281, 23 11 1995, s. 31.

12 Se exempelvis dataskyddsdirektivet, skälen 1, 4, 7 och 8.

13 EU-domstolens dom av den 24 november 2011 i de förenade målen C-468/10 och C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado*, punkterna 28–29.

instrument för att förbättra överensstämmelsen med reglerna för skydd av uppgifter visade sig framför allt vara ett viktigt bidrag till en effektivt fungerande lagstiftning om skydd av personuppgifter. (Detta inslag överfördes därför till Europarådets lagstiftning 2001, genom tilläggsprotokollet till konvention 108.)

Den territoriella tillämpningen av dataskyddsdirektivet går längre än EU:s 28 medlemsstater, och innefattar även de stater utanför EU som ingår i det europeiska ekonomiska samarbetsområdet (EES)[14], nämligen Island, Liechtenstein och Norge.

EU-domstolen i Luxemburg är behörig att pröva huruvida en medlemsstat har uppfyllt sina skyldigheter enligt dataskyddsdirektivet och lämna förhandsavgörande rörande direktivets giltighet och tolkning, i syfte att se till att det tillämpas effektivt och enhetligt i medlemsstaterna. Ett viktigt undantag från dataskyddsdirektivets tillämplighet är det så kallade hushållsundantaget, nämligen privatpersoners behandling av personuppgifter endast i privat syfte eller inom hushållet.[15] Denna behandling ses i allmänhet som en del av den privata individens frihet.

Direktivet motsvarar EU:s gällande primärrätt vid tiden för antagandet av dataskyddsdirektivet och dess huvudsakliga omfattning är begränsad till frågor som rör den inre marknaden. Utanför dess tillämpningsområde ligger i första hand frågor som rör polisiärt och straffrättsligt samarbete. Skydd av personuppgifter i dessa frågor härrör från olika rättsliga instrument, vilka beskrivs i detalj i kapitel 7.

Eftersom dataskyddsdirektivet endast kan gälla EU:s medlemsstater behövdes ytterligare ett rättsligt instrument för dataskydd när EU:s institutioner och organ behandlar personuppgifter. Förordning (EG) nr 45/2001 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (nedan kallad *dataskyddsförordningen*) uppfyller detta behov.[16]

Även inom områden som omfattas av dataskyddsdirektivet behövs ofta detaljerade bestämmelser för att nå tillräcklig tydlighet när det gäller att avväga andra berättigade intressen. Två exempel är direktiv 2002/58/EG om behandling av

14 Avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet), EGT L 1, 3.1.1994, som trädde i kraft den 1 januari 1994.

15 Dataskyddsdirektivet, artikel 3.2, andra strecksatsen.

16 Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, EGT L 8, 12.1.2001.

personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)[17] och direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (*datalagringsdirektivet*, upphävt den 8 april 2014).[18] Andra exempel kommer att diskuteras i kapitel 8. Dessa bestämmelser måste vara i linje med dataskyddsdirektivet.

Europeiska unionens stadga om de grundläggande rättigheterna

Europeiska gemenskapernas ursprungliga fördrag innehöll ingen hänvisning till mänskliga rättigheter eller skyddet av dessa. När EG-domstolen fick ta hand om påstådda överträdelser av mänskliga rättigheter inom områden som omfattas av EU-lagstiftningen utvecklades emellertid ett nytt synsätt. För att trygga skyddet av enskilda infördes grundläggande rättigheter i de så kallade allmänna principerna i europeisk lagstiftning. Enligt EU-domstolen återspeglar dessa allmänna principer innehållet i skyddet av mänskliga rättigheter som finns i nationella konstitutioner och fördrag om mänskliga rättigheter, särskilt Europakonventionen. EU-domstolen slog fast att den skulle säkerställa att EU:s lagstiftning överensstämmer med dessa principer.

Genom att erkänna att dess policyer kan ha en inverkan på mänskliga rättigheter och i en satsning på att få medborgarna att känna sig ”närmare” EU proklamerade EU år 2000 Europeiska unionens stadga om de grundläggande rättigheterna (stadgan). Stadgan innehåller alla civila, politiska, ekonomiska och sociala rättigheter för europeiska medborgare, och sammanfattar de konstitutionella traditionerna och internationella skyldigheterna som är gemensamma för medlemsstaterna. Rättigheterna som beskrivs i stadgan är uppdelade i sex avdelningar: värdighet, frihet, jämställdhet, solidaritet, medborgerliga rättigheter och rättvisa.

17 Europaparlamentets och rådets direktiv 2002/58/EC av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT 2002 L 201.

18 Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, *(datalagringsdirektivet)*, EUT 2006 L 105, upphävt den 8 april 2014.

Även om stadgan ursprungligen endast var ett politiskt dokument blev det juridiskt bindande[19] som primärrätt inom EU (se artikel 6.1 i EU-fördraget) i och med ikraftträdandet av Lissabonfördraget den 1 december 2009.[20]

EU:s primärrätt innehåller också en allmän EU-behörighet att lagstifta i dataskyddsfrågor (artikel 16 i EUF-fördraget).

Stadgan garanterar inte bara respekten för privatlivet och familjelivet (artikel 7), utan fastställer också rätten till skydd av personuppgifter (artikel 8), som uttryckligen höjer nivån på skyddet till samma nivå som en grundläggande rätt i EU-lagstiftningen. EU-institutionerna såväl som medlemsstaterna måste iaktta och garantera denna rätt, vilket även gäller för medlemsstater vid tillämpning av unionsrätten (artikel 51 i stadgan). Artikel 8 i stadgan formulerades flera år efter dataskyddsdirektivet och måste förstås som att den uttrycker den tidigare befintliga dataskyddslagstiftningen inom EU. I stadgan nämns därför inte bara uttryckligen rätten till skydd av personuppgifter i artikel 8.1 utan den hänvisar även till viktiga dataskyddsprinciper i artikel 8.2. Avslutningsvis ska enligt artikel 8.3 i stadgan en oberoende myndighet kontrollera genomförandet av dessa principer.

Framtidsutsikter

I januari 2012 föreslog Europeiska kommissionen ett reformpaket om dataskydd som innebar att de nuvarande reglerna om dataskydd behövde moderniseras mot bakgrund av den snabba teknologiska utvecklingen och globaliseringen. Reformpaketet består av ett förslag till en allmän uppgiftsskyddsförordning[21], som är avsedd att ersätta dataskyddsdirektivet liksom ett nytt allmänt uppgiftsskyddsdirektiv[22] som ska erbjuda dataskydd inom områdena polissamarbete och straffrättsligt samarbete. Vid tidpunkten för denna handboks publicering pågick diskussioner om reformpaketet.

19 EU (2012), Europeiska unionens stadga om de grundläggande rättigheterna, EUT 2012 C 326.

20 Se konsoliderade versioner av Europeiska gemenskaperna (2012), Fördraget om Europeiska unionen, EUT 2012 C 326, och Europeiska gemenskaperna (2012), Fördraget om Europeiska unionens funktionssätt, EUT 2012 C 326.

21 Europeiska kommissionen (2012), *Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning)*, COM(2012) 11 final, Bryssel, 25 januari 2012.

22 Europeiska kommissionen (2012), *Förslag till Europaparlamentets och rådets direktiv om skydd för enskilda personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter*, COM(2012) 10 final, Bryssel, 25 januari 2012.

1.2. Avvägning av rättigheter

Viktig punkt

- Rätten till uppgiftsskydd är inte en absolut rättighet, den måste vägas mot andra rättigheter.

Den grundläggande rätten till skydd av personuppgifter enligt artikel 8 i stadgan "är emellertid inte någon absolut rättighet utan måste förstås utifrån sin funktion i samhället".[23] Enligt artikel 52.1 i stadgan accepteras alltså att begränsningar kan införas när det gäller att utöva sådana rättigheter som anges i artikel 7 och 8 i stadgan, så länge dessa begränsningar medges i lagen, respekterar grunddragen i dessa rättigheter och friheter och, med beaktande av proportionalitetsprincipen, är nödvändiga och verkligen uppfyller målsättningarna av allmänt intresse som erkänns av Europeiska unionen eller behovet av att skydda andras rättigheter och friheter.[24]

I Europakonventionen säkerställs dataskydd genom artikel 8 (rätten till respekt för privat- och familjeliv) och precis som i stadgans system behöver rätten tillämpas samtidigt som omfattningen av andra konkurrerande rättigheter respekteras. I artikel 8.2 i Europakonventionen står "Offentlig myndighet får inte ingripa i denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt [...] för andra personers fri- och rättigheter".

Både Europadomstolen och EU-domstolen har därför vid upprepade tillfällen slagit fast att detta måste vägas mot andra rättigheter när artikel 8 i Europakonventionen och artikel 8 i stadgan tillämpas och tolkas.[25] Flera viktiga exempel illustrerar hur denna balans uppnås.

23 Se exempelvis EU-domstolens dom av den 9 november 2010 i de förenade målen C-92/09 och C-93/09, *Volker och Markus Schecke GbR och Hartmut Eifert mot Land Hessen*, punkt 48.

24 *Ibid.*, punkt 50.

25 Europadomstolen, *Von Hannover mot Tyskland (nr 2)* [GC], nr 40660/08 och 60641/08, 7 februari 2012, EU-domstolen, förenade målen C-468/10 och C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado*, 24 november 2011, punkt 48, EU-domstolen, C-275/06, *Productores de Música de España (Promusicae) mot Telefónica de España SAU*, 29 januari 2008, punkt 68. Se även Europarådet (2013), rättspraxis från Europadomstolen för de mänskliga rättigheterna rörande skydd av personuppgifter, DP (2013), rättspraxis, på: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

1.2.1. Yttrandefrihet

En av de rättigheter som riskerar att hamna i konflikt med rätten till skydd av personuppgifter är rätten till yttrandefrihet.

Yttrandefriheten skyddas av artikel 11 i stadgan (yttrandefrihet och informationsfrihet). Denna rätt innefattar ”åsiktsfrihet samt frihet att ta emot och sprida uppgifter och tankar utan offentlig myndighets inblandning och oberoende av territoriella gränser”. Artikel 11 motsvarar artikel 10 i Europakonventionen. Enligt artikel 52.3 i stadgan ska, i den mån som den omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen, rättigheterna ha ”samma innebörd och räckvidd som i konventionen”. De begränsningar som enligt lag får införas mot rätten som garanteras i artikel 11 i stadgan kan därför inte överskrida de som ges i artikel 10.2 i Europakonventionen, det vill säga de måste föreskrivas i lagen och de måste vara nödvändiga i ett demokratiskt samhälle ”till skydd […] för annans goda namn och rykte eller rättigheter”. Detta begrepp omfattar rätten till skydd av personuppgifter.

Relationen mellan skyddet av personuppgifter och yttrandefriheten styrs av artikel 9 i dataskyddsdirektivet, med rubriken ”Behandling av personuppgifter och yttrandefriheten”.[26] Enligt denna artikel är medlemsstaterna skyldiga att tillhandahålla ett antal undantag eller begränsningar när det gäller skyddet av personuppgifter och de anges därför, i förhållande till den grundläggande rätten till privatlivet, i kapitel II, IV och VI i direktivet. Dessa undantag får endast göras för journalistiska ändamål eller konstnärligt eller litterärt skapande, som faller inom ramen för den grundläggande rätten till yttrandefrihet, i den mån som de är nödvändiga för att förena rätten till privatlivet med reglerna för yttrandefrihet.

Exempel: I målet *Tietosuojavaltuutettu mot Satakunnan Markkinapörssi Oy och Satamedia Oy*[27], ombads EU-domstolen att tolka artikel 9 i dataskyddsdirektivet och fastställa förhållandet mellan skydd av personuppgifter och pressfriheten. Domstolen skulle undersöka Markkinapörssi och Satamedias spridning av skatteuppgifter om cirka 1,2 miljoner fysiska personer som de lagenligt erhållit från de finska skattemyndigheterna. Domstolen skulle framför allt kontrollera huruvida behandlingen av personuppgifter, som skattemyndigheterna gjorde tillgängliga, i syfte att göra det möjligt för mobiltelefonanvändare att erhålla

26 Dataskyddsdirektivet, artikel 9.

27 EU-domstolen, C-73/07, *Tietosuojavaltuutettu mot Satakunnan Markkinapörssi Oy och Satamedia Oy,* 16 december 2008, punkterna 56, 61 och 62.

skatteuppgifter rörande andra fysiska personer, måste betraktas som en verksamhet som utfördes enbart för journalistiska ändamål. Efter att ha dragit slutsatsen att Satakunnans verksamhet var ”behandling av personuppgifter” i den mening som avses i artikel 3.1 i dataskyddsdirektivet fortsatte domstolen med att tolka artikel 9 i direktivet. Domstolen noterade först behovet av rätten till yttrandefrihet i alla demokratiska samhällen och förklarade att begrepp i anslutning till denna frihet, såsom journalistik, borde tolkas brett. Den noterade sedan att i syfte att nå balans mellan de två grundläggande rättigheterna måste undantag och begränsningar i rätten till skydd av personuppgifter tillämpas i den mån som det är strikt nödvändigt. Under dessa omständigheter ansåg domstolen att sådan verksamhet som utfördes av Markkinapörssi och Satamedia rörande uppgifter från handlingar som är offentlig handling enligt nationell lagstiftning, kan klassificeras som ”journalistisk verksamhet” om syftet är att ge allmänheten information, yttranden eller idéer, oavsett vilket medium som används för att överföra dem. Domstolen beslutade också att dessa aktiviteter inte är begränsade till medieföretag och kan genomföras i vinstdrivande syfte. EU-domstolen överlät emellertid till den nationella domstolen att fastställa huruvida detta var fallet i det här särskilda målet.

Rörande förenligheten mellan rätten till skydd av personuppgifter och rätten till yttrandefrihet har Europadomstolen utfärdat flera domar som blivit milstolpar.

Exempel: I målet *Axel Springer AG mot Tyskland*[28] hävdade Europadomstolen att ett förbud som införts av en inhemsk domstol mot ägaren till en tidning som ville publicera en artikel om arrestering och fällande dom mot en välkänd skådespelare utgjorde en överträdelse av artikel 10 i Europakonventionen. Europadomstolen upprepade följande kriterier som den hade fastställt i sin rättspraxis när rätten till yttrandefrihet skulle vägas mot rätten till respekt för privatlivet:

- För det första huruvida den händelse som den publicerade artikeln gällde var av allmänt intresse: arresteringen av och den fällande domen mot en person var ett offentligt rättsligt faktum och därmed av allmänt intresse;

- För det andra huruvida den berörda personen var en offentlig person: personen i fråga var en skådespelare som var tillräckligt välkänd för att betraktas som offentlig person;

28 Europadomstolen, *Axel Springer AG mot Tyskland* [GC], nr 39954/08, 7 februari 2012, punkterna 90 och 91.

- För det tredje hur informationen erhållits och huruvida den var tillförlitlig: informationen hade kommit från den allmänna åklagarens kontor och korrektheten i informationen i båda publiceringarna var inte en tvistefråga mellan parterna.

Europadomstolen fastställde att publiceringsrestriktionerna mot företaget inte hade varit rimligt proportionerliga mot det berättigade syftet att skydda den klagandes privatliv. Domstolen drog slutsatsen att artikel 10 i Europakonventionen hade överträtts.

Exempel: I målet *Von Hannover mot Tyskland (nr 2)*[29] fann Europadomstolen ingen överträdelse av rätten till respekt för privatlivet enligt artikel 8 i Europakonventionen, när prinsessan Caroline av Monaco nekades ett åläggande mot publiceringen av ett foto av henne och hennes make under en skidsemester. Fotot åtföljdes av en artikel som bland annat redogjorde för prins Rainiers sviktande hälsa. Europadomstolen drog slutsatsen att de inhemska domstolarna noggrant hade vägt publiceringsföretagens rätt till yttrandefrihet mot den klagandes rätt till respekt för sitt privatliv. De inhemska domstolarnas karaktärisering av prins Rainiers sjukdom som en händelse i det moderna samhället kunde inte betraktas som oskälig och Europadomstolen kunde acceptera att fotografen, mot bakgrund av artikeln, åtminstone i viss mån bidrog till en debatt av allmänt intresse. Domstolen drog slutsatsen att artikel 8 i Europakonventionen inte hade överträtts.

I Europadomstolens rättspraxis är ett av de avgörande kriterierna rörande balansen mellan dessa rättigheter huruvida yttrandet i fråga bidrar till en debatt som är av allmänt intresse.

Exempel: I målet *Mosley mot Förenade kungariket*[30] publicerade en nationell veckotidning intima foton av den klagande. Han hävdade då att artikel 8 i Europakonventionen hade överträtts eftersom han inte hade haft möjlighet att ansöka om föreläggande innan fotona i fråga publicerades på grund av avsaknaden av varje krav på meddelande i förväg för tidningen vid publicering av material som kan överträda en persons rätt till privatliv. Även om spridningen

29 Europadomstolen, *Von Hannover mot Tyskland (nr 2)* [GC], nr 40660/08 och 60641/08, 7 februari 2012, punkterna 118 och 124.

30 Europadomstolen, *Mosley mot Förenade kungariket*, nr 48009/08, 10 maj 2011, punkterna 129 och 130.

av detta material i allmänhet syftade till underhållning snarare än utbildning omfattades det utan tvekan av skyddet i artikel 10 i Europakonventionen, vilket kan leda till kraven i artikel 8 i Europakonventionen när informationen var av privat och intim natur och det inte fanns något allmänintresse av publiceringen. Särskild omsorg krävdes emellertid vid granskning av restriktioner som skulle kunna fungera som en form av censur före publicering. Rörande den avkylningseffekt som kravet på en anmälan i förväg skulle kunna ge upphov till, tvivlen på dess effektivitet och det stora utrymmet för bedömning på området drog Europadomstolen slutsatsen att det inte krävdes någon juridiskt bindande anmälan i förväg enligt artikel 8. Domstolen drog därför slutsatsen att artikel 8 i Europakonventionen inte hade överträtts.

Exempel: I målet *Biriuk mot Litauen*[31] krävde den klagande skadestånd från en dagstidning eftersom den hade publicerat en artikel som hävdade att hon var hivpositiv. Informationen uppgavs ha bekräftats av läkarna vid det lokala sjukhuset. Europadomstolen ansåg inte att artikeln i fråga bidrog till någon debatt av allmänt intresse och upprepade att skyddet av personuppgifter, inte minst medicinska uppgifter, var av grundläggande betydelse för att en person skulle omfattas av rätten till respekt för privat- och familjelivet i enlighet med artikel 8 i Europakonventionen. Domstolen fäste särskild betydelse vid att medicinsk personal vid ett sjukhus, enligt rapporten i tidningen, hade lämnat information om den klagandes hivinfektion vilket uppenbart innebar ett brott mot deras tystnadsplikt som vårdpersonal. Staten hade därmed misslyckats med att garantera den klagandes rätt till respekt för privatlivet. Domstolen drog därför slutsatsen att artikel 8 i Europakonventionen hade överträtts.

1.2.2. Tillgång till handlingar

Informationsfrihet enligt artikel 11 i stadgan och artikel 10 i Europakonventionen skyddar inte enbart rätten att överföra utan även rätten att *erhålla* information. Betydelsen av statlig öppenhet för att ett demokratiskt samhälle ska fungera blir allt mer uppenbar. Under de senaste två årtiondena har därför rätten att få tillgång till handlingar som innehas av offentliga myndigheter erkänts som en viktig rättighet för alla EU-medborgare och alla fysiska eller juridiska personer som är bosatta i eller har sitt säte i en medlemsstat.

31 Europadomstolen, *Biriuk mot Litauen*, nr 23373/03, 25 november 2008.

Enligt Europarådets lagstiftning kan hänvisning ske till principerna i rekommendationen om tillgång till offentliga handlingar, som inspirerade dem som utarbetade konventionen om tillgång till offentliga handlingar (*Convention No 205 on Access to Official Documents*).[32] **Enligt EU-lagstiftningen** garanteras rätten till tillgång till handlingar av förordning (EG) nr 1049/2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (*förordningen om tillgång till handlingar*).[33] Genom artikel 42 i stadgan och artikel 15.3 i EUF-fördraget har denna rätt till tillgång utvidgats till ”tillgång till unionens institutioners, organs och byråers handlingar, oberoende av medium”. I enlighet med artikel 52.2 i stadgan utövas rätten till tillgång till handlingar också enligt de villkor och inom de begränsningar som fastställts i artikel 15.3 i EUF-fördraget. Denna rättighet kan strida mot rätten till skydd av personuppgifter om tillgång till en handling skulle innebära att andras personuppgifter avslöjas. Begäran om tillgång till handlingar eller information som innehas av offentliga myndigheter kan därför behöva vägas mot rätten till skydd av personuppgifter för personer vars uppgifter finns i de begärda handlingarna.

Exempel: I målet *Kommissionen mot Bavarian Lager*[34] fastställde EU-domstolen omfattningen av skyddet av personuppgifter i samband med tillgång till EU-institutionernas handlingar och förhållandet mellan förordning (EG) nr 1049/2001 (*förordningen om tillgång till handlingar*) och förordning (EG) nr 45/2001 (*dataskyddsförordningen*). Bavarian Lager, etablerat 1992, importerar buteljerat tyskt öl till Förenade kungariket, huvudsakligen till pubar och barer. De stötte emellertid på svårigheter eftersom den brittiska lagstiftningen faktiskt gynnade nationella produkter. Som svar på Bavarian Lagers klagomål beslutade Europeiska kommissionen att inleda ett förfarande mot Förenade kungariket för att ha underlåtit att uppfylla sina befogenheter, vilket ledde till att de ändrade de omdiskuterade bestämmelserna och anpassade dem till EU-lagstiftningen. Bavarian Lager bad då kommissionen bland annat om en kopia på protokollet från ett möte som representanter för kommissionen, de brittiska myndigheterna och *Confédération des Brasseurs du Marché Commun* (CBMC) hade deltagit i. Kommissionen gick med på att lämna ut vissa handlingar rörande mötet, men strök fem namn som återfanns i protokollet, då två personer uttryckligen

32 Europarådet, ministerkommittén (2002), Rekommendation Rec (2002)2 till medlemsstaterna om tillgång till officiella handlingar 21 februari 2002, Europarådets konvention om tillgång till officiella handlingar, CETS nr 205, 18 juni 2009. Konventionen har ännu inte trätt i kraft.

33 Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar, EGT 2001, L145.

34 EU-domstolen, C-28/08 P, *Europeiska kommissionen mot The Bavarian Lager Co. Ltd.*, 29 juni 2010, punkterna 60, 63, 76, 78 och 79.

hade invänt mot att deras identitet skulle avslöjas och kommissionen inte lyckats få kontakt med de övriga tre. Genom beslut av den 18 mars 2014 avvisade kommissionen en ny ansökan från Bavarian Lager om att få tillgång till det fullständiga protokollet från mötet, och nämnde bland annat skyddet av dessa personers privatliv, enligt garantierna i dataskyddsförordningen. Eftersom Bavarian Lager inte var nöjd med denna ståndpunkt vände sig företaget till förstainstansrätten, som upphävde kommissionens beslut genom sin dom av den 8 november 2007 (mål T194/04, *Bavarian Lager mot kommissionen*), framför allt med beaktande av att enbart angivande av namnen på personerna i fråga i förteckningen över personer som deltagit i mötet för det organ de representerade inte undergrävde privatlivet och utsatte inte dessa personers privatliv för någon fara.

Efter en uppmaning från kommissionen upphävde EU-domstolen domen i förstainstansrätten. EU-domstolen hävdade att i förordningen om tillgång till handlingar föreskrivs ”en särreglering som stärker skyddet av personer vars personuppgifter i förekommande fall kan komma att lämnas ut till allmänheten”. När någon i en begäran baserad på förordningen om tillgång till handlingar därmed försöker få tillgång till handlingar, inbegripet personuppgifter, blir enligt EU-domstolen bestämmelserna i dataskyddsförordningen tillämpliga i sin helhet. EU-domstolen drog då slutsatsen att kommissionen var i sin fulla rätt att avvisa ansökan om tillgång till det fullständiga protokollet från mötet i oktober 1996. I avsaknad av samtycke från de fem mötesdeltagarna uppfyllde kommissionen sin skyldighet till öppenhet tillräckligt genom att lämna ut en version av handlingen i fråga där namnen strukits över.

EU-domstolen anser dessutom att ”eftersom Bavarian Lager inte har lämnat någon uttrycklig och berättigad motivering och inte heller anfört något övertygande argument som visar att en överföring av dessa personuppgifter är nödvändig, har kommissionen inte kunnat göra en avvägning mellan de berörda parternas respektive intressen. Kommissionen kunde inte heller verifiera att det skulle ”saknas skäl att anta att den registrerades legitima intressen skulle kunna skadas”, såsom krävs i dataskyddsförordningen.

Enligt denna dom kräver konflikt med rätten till skydd av personuppgifter när det gäller respekten för tillgång till handlingar ett specificerat och motiverat skäl.

Rätten till tillgång till handlingar kan inte automatiskt upphäva rätten till skydd av personuppgifter.[35]

En särskild aspekt av en begäran om tillgång togs upp i följande dom från Europadomstolen.

> Exempel: I målet *Társaság a Szabadságjogokért mot Ungern*[36] hade den klagande, en icke-statlig organisation inom mänskliga rättigheter, krävt tillgång till information från författningsdomstolen om ett ännu icke avgjort ärende. Utan att samråda med den ledamot av parlamentet som hade tagit målet till domstolen vägrade domstolen att ge tillgång till begäran med motiveringen att klagomål till den kunde göras tillgängliga för externa personer endast efter godkännande från den klagande. Inhemska domstolar vidmakthöll vägran, med motiveringen att skyddet av dessa personuppgifter inte kunde åsidosättas av andra tillåtna intressen, inklusive tillgängligheten till offentlig information. Den klagande hade fungerat som en "samhällets vakthund" vars verksamhet garanterade liknande skydd som det som pressen erbjöd. I förhållande till pressfriheten hade Europadomstolen konsekvent hävdat att allmänheten hade rätt att erhålla information av allmänt intresse. Den information som den klagande sökte var "färdig och tillgänglig" och krävde inte någon insamling av uppgifter. Under dessa förhållanden hade staten en skyldighet att inte hindra flödet av information som den klagande efterfrågade. Sammanfattningsvis ansåg Europadomstolen att hinder utformade för att förhindra tillgång till information av allmänt intresse kan hindra dem som arbetar inom media eller tillhörande områden från att utföra sin nödvändiga roll som "offentlig vakthund". Domstolen drog därför slutsatsen att artikel 10 i Europakonventionen hade överträtts.

I EU-lagstiftningen är betydelsen av öppenhet noga fastställd. Öppenhetsprincipen ingår i artiklarna 1 och 10 i EU-fördraget och artikel 15.1 i EUF-fördraget.[37] Enligt skäl 2 i förordning (EG) nr 1049/2001 innebär det att medborgare kan delta närmare

35 Se emellertid de detaljerade överläggningarna i Europeiska datatillsynsmannen (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling*, Bryssel, 24 mars 2011, tillgänglig på: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 Europadomstolen, *Társaság a Szabadságjogokért mot Ungern*, nr 37374/05, 14 april 2009, se punkt 27, 36–38.

37 EU (2012), Konsoliderade versioner av Fördraget om Europeiska unionen och Fördraget om Europeiska unionens funktionssätt, EUT 2012 C 326.

i beslutsprocessen och det garanterar att administrationen åtnjuter större legitimitet och är effektivare och mer ansvarig gentemot medborgaren i ett demokratiskt system.[38]

Till följd av detta krävs det enligt rådets förordning (EG) nr 1290/2005 om finansieringen av den gemensamma jordbrukspolitiken och kommissionens förordning (EG) nr 259/2008 om tillämpningsföreskrifter för rådets förordning (EG) nr 1290/2005 att uppgifter ska offentliggöras om de stödmottagare som får stöd från Europeiska garantifonden för jordbruket (EGFJ) och Europeiska jordbruksfonden för landsbygdsutveckling (EJFLU).[39] Offentliggörandet ska bidra till offentlig kontroll av att myndigheterna använder offentliga medel på lämpligt sätt. Proportionaliteten i ett sådant offentliggörande bestreds av flera stödmottagare.

Exempel: I målet *Volker och Markus Schecke och Hartmut Eifert mot Land Hessen*[40] skulle EU-domstolen bedöma proportionaliteten i offentliggörandet, såsom EU-lagstiftningen krävde, av namnen på mottagarna av EU:s jordbruksstubventioner och de belopp de erhöll.

Domstolen noterade att rätten till uppgiftsskydd inte är absolut, hävdade att publiceringen på en webbplats av uppgifter som namngav mottagarna av två fonder för jordbruksstöd och det exakta beloppet utgör intrång i deras privatliv i allmänhet och i deras skydd av personuppgifterna i synnerhet.

Domstolen ansåg att denna konflikt med artikel 7 och 8 i stadgan tillgodosågs i lagen och uppfyllde en målsättning med allmänt intresse som erkänns av EU, nämligen bland annat förbättrad öppenhet när det gäller användningen av gemenskapsmedel. EU-domstolen hävdade emellertid att publiceringen av namnen på fysiska personer som mottar EU:s jordbruksstöd från dessa två fonder och det exakta belopp som erhållits utgjorde en oproportionerlig åtgärd och inte var motiverad med beaktande av artikel 52.1 i stadgan. Domstolen

38 EU-domstolen, C-41/00 P, *Interporc Im- und Export GmbH mot Europeiska gemenskapernas kommission*, 6 mars 2003, punkt 39, och EU-domstolen, C-28/08 P, *Europeiska kommissionen mot The Bavarian Lager Co. Ltd.*, 29 juni 2010, punkt 54.

39 Rådets förordning (EG) nr 1290/2005 av den 21 juni 2005 om finansieringen av den gemensamma jordbrukspolitiken, EUT 2005 L 209, och kommissionens förordning (EG) nr 259/2008 av den 18 mars 2008 om tillämpningsföreskrifter för rådets förordning (EG) nr 1290/2005 när det gäller offentliggörande av uppgifter om de stödmottagare som får stöd från Europeiska garantifonden för jordbruket (EGFJ) och Europeiska jordbruksfonden för landsbygdsutveckling (EJFLU), EUT 2008 L 76.

40 EU-domstolen, förenade målen C-92/09 och C-93/09, *Volker och Markus Schecke GbR och Hartmut Eifert mot Land Hessen*, 9 november 2010, punkt 47–52, 58, 66–67, 75, 86 och 92.

fastställde därför att EU-lagstiftningen om offentliggörande av information om mottagarna av jordbruksstöd delvis var ogiltig.

1.2.3. Frihet för konsten och vetenskapen

En annan rätt som bör vägas mot rätten till respekt för privatlivet och uppgiftsskydd är friheten för konsten och vetenskapen, som uttryckligen skyddas i artikel 13 i stadgan. Rätten härrör i första hand från rätten till tanke- och yttrandefrihet och den ska utövas med beaktande av artikel 1 i stadgan (människans värdighet). Europadomstolen anser att frihet för konsten och vetenskapen skyddas enligt artikel 10 i Europakonventionen.[41] Rätten som garanteras genom artikel 13 i stadgan kan också omfattas av begränsningarna som godkänns i artikel 10 i Europakonventionen.[42]

Exempel: I målet *Vereinigung bildender Künstler mot Österrike*[43] förbjöd de österrikiska domstolarna den klagande föreningen att fortsätta att ställa ut en målning som innehöll foton av huvuden som tillhörde olika offentliga personer i sexuella ställningar. En österrikisk parlamentariker, vars foto använts i målningen, vidtog rättsliga åtgärder mot den klagande föreningen, och sökte ett åläggande som skulle förbjuda föreningen att ställa ut målningen. Den inhemska domstolen utfärdade ett åläggande och accepterade hans begäran. Europadomstolen upprepade att artikel 10 i Europakonventionen var tillämplig när det gäller att sprida idéer som kränkte, chockade eller störde staten eller någon del av befolkningen. De som skapade, utförde, distribuerade eller ställde ut konstverk bidrog till utbytet av idéer och uppfattningar och staten var skyldig att inte inkräkta otillbörligt på deras yttrandefrihet. Med tanke på att målningen var ett collage och enbart använde foton av personers huvuden, och att deras kroppar var målade på ett orealistiskt och överdrivet sätt, som uppenbarligen inte syftade till att återspegla eller ens antyda verkligheten, slog Europadomstolen fast att ”målningen knappast kunde uppfattas som att den tar upp detaljer om [de avbildades] privatliv, utan snarare hänvisade till hans offentliga ställning som politiker” och att ”i denna roll måste [den avbildade] uppvisa större tolerans när det gäller kritik”. Vid bedömning av de olika intressen som stod på spel ansåg Europadomstolen att ett obegränsat förbud mot ytterligare utställning av

41 Europadomstolen, *Müller m.fl. mot Schweiz*, nr 10737/84, 24 maj 1988.

42 Förklaringar avseende stadgan om de grundläggande rättigheterna , EUT 2007 C 303.

43 *Europadomstolen Vereinigung bildender Künstler mot Österrike*, nr 68345/01, 25 januari 2007, se särskilt punkterna 26 och 34.

målningen var oproportionerlig. Domstolen drog slutsatsen att artikel 10 i Europakonventionen hade överträtts.

När det gäller vetenskap är den europeiska lagstiftningen om skydd av personuppgifter medveten om vetenskapens särskilda värde för samhället. De allmänna begränsningarna för användning av personuppgifter är därför mindre. Dataskyddsdirektivet och konvention 108 tillåter båda lagring av uppgifter för vetenskaplig forskning när de inte längre behövs för det syfte de ursprungligen samlades in för. Senare användning av personuppgifter för vetenskaplig forskning ska dessutom inte anses som ett oförenligt syfte. Nationell lagstiftning har i uppgift att utveckla mer detaljerade bestämmelser, inbegripet de nödvändiga garantierna, för att förena den vetenskapliga forskningens intressen med rätten till uppgiftsskydd (se även avsnitten 3.3.3 och 8.4).

1.2.4. Skydd av egendom

Rätten till skydd av egendom ingår i artikel 1 i det första protokollet till Europakonventionen och även i artikel 17.1 i stadgan. En viktig aspekt av rätten till egendom är skyddet av immateriell äganderätt, som uttryckligen nämns i artikel 17.2 i stadgan. Flera direktiv finns i EU:s rättsordning som syftar till att effektivt skydda immateriell egendom, särskilt copyright. Immateriell egendom omfattar inte bara litterär och konstnärlig egendom utan även patent, varumärken och tillhörande rättigheter.

Såsom EU-domstolens rättspraxis har visat måste skyddet av den grundläggande rätten till egendom vägas mot skyddet av andra grundläggande rättigheter, särskilt mot rätten till skydd av personuppgifter.[44] Det har förekommit fall där institutioner för skydd av copyright har krävt att internetleverantörer skulle lämna ut identiteten på användare av internetplattformar för fildelning. Dessa plattformar gör det ofta möjligt för internetanvändare att ladda ned musiktitlar kostnadsfritt även om dessa är skyddade av copyright.

Exempel: Målet *Promusicae mot Telefónica de España*[45] gällde den spanska internetleverantören Telefónicas vägran att till Promusicae, en icke vinstdrivande organisation av musikproducenter och utgivare av musikinspelningar och audiovisuella inspelningar, lämna ut personuppgifter för vissa personer som

44 Europadomstolen, *Ashby Donald m.fl. mot Frankrike*, nr 36769/08, 10 januari 2013.

45 EU-domstolen, C-275/06, *Productores de Música de España (Promusicae) mot Telefónica de España SAU*, 29 januari 2008, punkterna 54 och 60.

företaget levererade internettjänster till. Promusicae ville ha informationen för att kunna inleda civilmål mot de personer som påstods använda ett fildelningsprogram som gav tillgång till fonogram vars nyttjanderättigheter innehades av Promusicaes medlemmar.

Den spanska domstolen hänvisade frågan till EU-domstolen och frågade om dessa personuppgifter enligt gemenskapslagstiftningen måste lämnas ut i samband med en civilprocess för att säkerställa effektivt skydd av copyright. Domstolen hänvisade till direktiv 2000/31, 2001/29 och 2004/48, även mot bakgrund av artikel 17 och 47 i stadgan. Domstolen drog slutsatsen att dessa tre direktiv, liksom direktivet om integritet och elektronisk kommunikation (direktiv 2002/58), inte hindrar medlemsstaterna från att fastställa en skyldighet att lämna ut personuppgifter i samband med en civilprocess för att säkerställa effektivt skydd av copyright.

EU-domstolen påpekade att målet därför hade rest frågan om behovet av att förena kraven på skydd av olika grundläggande rättigheter, nämligen rätten till respekt för privatlivet med rätten till skydd av egendom och en effektiv prövning.

Domstolen drog slutsatsen att ”det ankommer på medlemsstaterna när de införlivar de ovannämnda direktiven med nationell rätt, att utgå ifrån en tolkning av direktiven som gör det möjligt att uppnå en korrekt balans mellan de olika grundläggande rättigheter som åtnjuter skydd enligt gemenskapens rättsordning. Vid genomförandet av införlivandeåtgärderna beträffande dessa direktiv, ankommer det på medlemsstaternas myndigheter och domstolar att inte bara tolka sin nationella rätt på ett sätt som står i överensstämmelse med dessa direktiv utan även att se till att de inte grundar sig på en tolkning av dem som skulle stå i strid med dessa grundläggande rättigheter eller med andra allmänna principer för gemenskapsrätten, såsom proportionalitetsprincipen.”[46]

46 *Ibid.*, punkterna 65 och 68, se även EU-domstolen, C-360/10, *SABAM mot Netlog N.V.*, 16 februari 2012.

2 Dataskyddsterminologi

EU	Frågor som täcks	Europarådet
Personuppgifter		
Dataskyddsdirektivet, artikel 2 a EU-domstolens dom av den 9 november 2010 i de förenade målen C-92/09 och C-93/09, *Volker und Markus Schecke GbR och Hartmut Eifert mot Land Hessen* EU-domstolens dom av den 29 januari 2008 i mål C-275/06, *Productores de Música de España (Promusicae) mot Telefónica de España SAU*	**Rättslig definition**	Konvention 108, artikel 2 a Europadomstolen, *Bernh Larsen Holding AS m.fl. mot Norge*, nr 24117/08, 14 mars 2013
Dataskyddsdirektivet, artikel 8.1 EU-domstolens dom av den 6 november 2003 i mål C-101/01, *Bodil Lindqvist*	**Särskilda kategorier av personuppgifter (känsliga uppgifter)**	Konvention 108, artikel 6
Dataskyddsdirektivet, artikel 6.1 e	**Anonymiserade och pseudonymiserade uppgifter**	Konvention 108, artikel 5 e Konvention 108, motivering, artikel 42
Behandling av uppgifter		
Dataskyddsdirektivet, artikel 2 b EU-domstolens dom av den 6 november 2003 i mål C-101/01, *Bodil Lindqvist*	**Definitioner**	Konvention 108, artikel 2 c

EU	Frågor som täcks	Europarådet
Användare av uppgifter		
Dataskyddsdirektivet, artikel 2 d	**Registeransvarig**	Konvention 108, artikel 2 d Rekommendation om profilering, artikel 1 g *
Dataskyddsdirektivet, artikel 2 e EU-domstolen, C-101/01, *Bodil Lindqvist*, 6 november 2003	**Registerförare**	Rekommendation om profilering, artikel 1 h
Dataskyddsdirektivet, artikel 2 g	**Mottagare**	Konvention 108, tilläggsprotokoll, artikel 2.1
Dataskyddsdirektivet, artikel 2 f	**Tredjepart**	
Samtycke		
Dataskyddsdirektivet, artikel 2 h EU-domstolen, C-543/09, *Deutsche Telekom AG mot Bundesrepublik Deutschland*, 5 maj 2011	**Definition och krav för giltigt samtycke**	Rekommendation om medicinska uppgifter, artikel 6, och olika efterföljande rekommendationer

Anmärkning: **Europarådet, ministerkommittén (2010), rekommendation Rec (2010)13 till medlemsstaterna om skydd för enskilda vid automatisk databehandling av personuppgifter i samband med profilering (rekommendation om profilering), 23 november 2010.*

2.1. Personuppgifter

Viktiga punkter

- Uppgifter anses som personuppgifter om de gäller en identifierad eller åtminstone identifierbar person, dvs. den registrerade.
- En person är identifierbar om ytterligare information kan erhållas utan orimlig ansträngning, och den möjliggör identifiering av den registrerade.
- Autentisering innebär att bevisa att en viss person innehar en viss identitet och/eller har tillstånd att utföra viss verksamhet.
- Det finns särskilda kategorier uppgifter, så kallade känsliga uppgifter, som anges i konvention 108 och i dataskyddsdirektivet, som kräver utökat skydd och därför omfattas av särskilda rättsliga regler.
- Uppgifter är anonymiserade om de inte längre innehåller några kännetecken, de är pseudonymiserade om kännetecknen är krypterade.
- I motsats till anonymiserade uppgifter är pseudonymiserade uppgifter personuppgifter.

2.1.1. Huvudsakliga aspekter av begreppet personuppgifter

Enligt EU-lagstiftningen och **Europarådets lagstiftning** definieras ”personuppgifter” som information som rör en identifierad eller identifierbar person[47], det vill säga information om en person vars identitet antingen är uppenbar eller åtminstone kan fastställas med hjälp av kompletterande information.

Om uppgifter om en sådan person behandlas kallas personen den registrerade.

En person

Rätten till skydd av personuppgifter utvecklades ur rätten till respekt för privatlivet. Begreppet privatliv rör människor. Fysiska personer är därför i första hand de som omfattas av dataskydd. Enligt yttrandet från artikel 29-gruppen är dessutom endast *levande personer* skyddade enligt den europeiska lagstiftningen om skydd av personuppgifter.[48]

Rättspraxis från Europadomstolen rörande artikel 8 i Europakonventionen visar att det kan vara svårt att fullständigt separera frågor som rör privatliv och yrkesliv.[49]

> Exempel: I målet *Amann mot Schweiz*[50] avlyssnade myndigheterna ett affärsrelaterat telefonsamtal till den klagande. Baserat på samtalet undersökte myndigheterna den klagande och fyllde i en blankett om den klagande till det nationella säkerhetsregistret. Även om avlyssningen gällde ett affärsrelaterat telefonsamtal ansåg Europadomstolen att lagringen av uppgifter om samtalet rörde den klagandes privatliv. Domstolen påpekade att begreppet ”privatliv” inte behöver tolkas restriktivt, framförallt som respekt för privatlivet omfattade rätten att etablera och utveckla relationer med andra människor. Det fanns dessutom inga principskäl till att motivera uteslutning av verksamhet av professionell eller affärsmässig natur från begreppet ”privatliv”. En sådan bred tolkning motsvarade den som anges i konvention 108. Europadomstolen fann

47 Dataskyddsdirektivet, artikel 2 a, Konvention 108, artikel 2 a.

48 Artikel 29-gruppen (2007), *Yttrande 4/2007 om begreppet personuppgifter*, WP 136, 20 juni 2007, s. 22.

49 Se exempelvis: Europadomstolen, *Rotaru mot Rumänien* [GC], nr 28341/95, 4 maj 2000, punkt 43, Europadomstolen, *Niemietz mot Tyskland*, 13710/88, 16 december 1992, punkt 29.

50 Europadomstolen, *Amann mot Schweiz* [GC], nr 27798/95, 16 februari 2000, punkt 65.

också att intrånget i den klagandes fall inte hade skett i enlighet med lagstiftningen eftersom inhemsk lag inte innehöll specifika och detaljerade uppgifter om insamling, registrering och lagring av information. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Om frågor kring yrkesliv dessutom kan bli föremål för uppgiftsskydd, förefaller det diskutabelt att endast fysiska personer skulle erbjudas skydd. Rättigheter enligt Europakonventionen garanteras inte enbart för fysiska personer utan för alla.

Det finns rättspraxis inom Europadomstolen med domar om ansökningar från juridiska personer om påstådd överträdelse av deras rätt till skydd mot användningen av deras uppgifter enligt artikel 8 i Europakonvention. Domstolen granskade emellertid målet enligt rätten till respekt för hem och korrespondens, snarare än i förhållande till privatlivet:

Exempel: Målet *Bernh Larsen Holding AS m.fl. mot Norge*[51] gällde ett klagomål från tre norska företag om ett beslut från skattemyndigheterna där man krävde att de till skatterevisorerna skulle lämna en kopia av alla uppgifter på en dataserver de tre använde gemensamt.

Europadomstolen fann att en sådan skyldighet för den klagandes företag utgjorde ett intrång i deras rätt till respekt för ”hem” och ”korrespondens” i enlighet med artikel 8 i Europakonventionen. Domstolen fann emellertid att skattemyndigheterna hade effektiva och lämpliga garantier mot missbruk: de klagande företagen hade blivit informerade i god tid, de var närvarande och kunde lämna förslag vid ingripandet på plats och materialet skulle förstöras när skatterevisionen hade genomförts. Under dessa omständigheter hade en korrekt balans uppnåtts mellan de klagande företagens rätt till respekt för ”hem” och ”korrespondens” och deras intresse av att skydda privatlivet för personer som arbetar för dem, å ena sidan, och det allmänna intresset av att säkerställa effektiv inspektion för skattebedömningssyften å andra sidan. Domstolen ansåg därför att artikel 8 i Europakonventionen inte hade överträtts.

Enligt konvention 108 gäller dataskydd huvudsakligen skydd av fysiska personer. De avtalsslutande parterna kan emellertid utvidga dataskyddet till juridiska personer, exempelvis företag och föreningar, i sin inhemska lagstiftning. **EU:s lagstiftning**

51 Europadomstolen, *Bernh Larsen Holding AS m.fl. mot Norge*, nr 24117/08, 14 mars 2013. Se emellertid även Europadomstolen, *Liberty m.fl. mot Förenade kungariket*, nr 58243/00, 1 juli 2008.

om skydd av personuppgifter omfattar i allmänhet skydd av juridiska personer när det gäller behandling av uppgifter som gäller dem. De nationella lagstiftarna är fria att besluta i frågan.[52]

> Exempel: I målet *Volker och Markus Schecke och Hartmut Eifert mot Land Hessen*[53] hänvisade EU-domstolen till offentliggörandet av personuppgifter om mottagare av jordbruksstöd och ansåg att ”juridiska personer endast kan göra gällande rätt till skydd enligt artiklarna 7 och 8 i stadgan vad avser en sådan identifiering, om angivandet av den juridiska personens firma medför att en eller flera fysiska personer identifieras. […R]ätten till respekt för privatlivet vad avser behandling av personuppgifter, vilken erkänns i artiklarna 7 och 8 i stadgan, omfattar varje uppgift som rör en fysisk person som är namngiven eller som på annat sätt kan identifieras”.[54]

En persons identifierbarhet

Enligt EU:s lagstiftning och **Europarådets lagstiftning** innehåller information uppgifter om en person:

- om en enskild person identifieras i denna information, eller
- om en enskild person, även om han eller hon inte är identifierad, beskrivs i informationen på ett sätt som gör det möjligt att ta reda på vem den registrerade är genom ytterligare undersökningar.

Båda typer av information skyddas på samma sätt enligt europeisk lagstiftning om skydd av personuppgifter. Europadomstolen har vid upprepade tillfällen slagit fast att ”personuppgifter” enligt Europakonventionen är detsamma som i konvention 108, särskilt gällande villkoret att relatera till identifierade eller identifierbara personer.[55]

52 Dataskyddsdirektivet, skäl 24.

53 EU-domstolen, förenade målen C-92/09 och C-93/09, *Volker och Markus Schecke GbR och Hartmut Eifert mot Land Hessen*, 9 november 2010, punkt 53.

54 *Ibid.,* punkt 52.

55 Se Europadomstolen, *Amann mot Schweiz* [GC], nr 27798/95, 16 februari 2000, punkt 65 et al.

De juridiska definitionerna av personuppgifter klargör inte ytterligare när en person anses som identifierad.[56] Självklart kräver identifiering beståndsdelar som beskriver en person på ett sådant sätt att han eller hon kan särskiljas från alla andra personer och kan kännas igen som en enskild person. En persons namn är ett utmärkt exempel på dessa beståndsdelar i en beskrivning. I undantagsfall kan andra kännetecken ha en liknande effekt som ett namn. För offentliga personer kan det exempelvis räcka med att hänvisa till personens ställning, såsom Europeiska kommissionens ordförande.

> Exempel: I målet *Promusicae*[57] slog EU-domstolen fast att det har ”inte bestritts att Promusicaes yrkande att namn och hemvist för vissa av de personer som använder sig av [ett visst fildelningsprogram på internet] skall företes ett yrkande om att få tillgång till personuppgifter, det vill säga upplysningar om identifierade eller identifierbara fysiska personer, enligt definitionen i artikel 2 a i direktiv 95/46 […]. Om Telefónica lämnar ut dessa uppgifter, vilka enligt Promusicae finns lagrade hos Telefónica, vilket bolaget inte har bestritt, skulle detta innebära behandling av personuppgifter i den mening som avses i artikel 2 första stycket i direktiv 2002/58, jämförd med artikel 2 b i direktiv 95/46”.

Eftersom många namn inte är unika kan fastställandet av en persons identitet behöva ytterligare kännetecken för att säkerställa att en person inte sammanblandas med någon annan. Födelsedatum och födelseplats används ofta. Personnummer har dessutom införts i vissa länder för att lättare kunna skilja mellan medborgare. Biometriska uppgifter, såsom fingeravtryck, digitala foton eller irisskanning, blir allt viktigare för att identifiera personer i den teknologiska tidsåldern.

För tillämpning av den europeiska lagstiftningen om skydd av personuppgifter krävs emellertid ingen identifiering av hög kvalitet av den registrerade – det räcker att den berörda personen kan identifieras. En person betraktas som identifierbar om en upplysning innehåller beståndsdelar för identifiering genom vilka personen kan identifieras, direkt eller indirekt.[58] Enligt skäl 26 i dataskyddsdirektivet är det avgörande huruvida det är sannolikt att rimliga hjälpmedel för identifiering är tillgängliga

56 Se även Europadomstolen, *Odièvre mot Frankrike* [GC], nr 42326/98, 13 februari 2003, och Europadomstolen, *Godelli mot Italien*, nr 33783/09, 25 september 2012.

57 EU-domstolen, C-275/06, *Productores de Música de España (Promusicae) mot Telefónica de España SAU*, 29 januari 2008, punkt 45.

58 Dataskyddsdirektivet, artikel 2 a.

och kan komma att användas av förutsebara användare av informationen. Detta innefattar tredjepartsmottagare (se avsnitt 2.3.2).

Exempel: En lokal myndighet beslutar att samla in uppgifter om bilar som kör för fort på lokalgator. De fotograferar bilarna, registrerar automatiskt tid och plats, i syfte att lämna över uppgifterna till behöriga myndigheter så att de kan bötfälla dem som överträtt hastighetsgränserna. En registrerad lämnar in ett klagomål om att den lokala myndigheten inte har någon rättslig grund enligt lagstiftningen om skydd av personuppgifter för denna typ av insamling. Den lokala myndigheten vidhåller att den inte samlar in personuppgifter. Enligt myndigheten utgör registreringsskyltar uppgifter om anonyma personer. Den lokala myndigheten har ingen juridisk befogenhet att få tillgång till det allmänna fordonsregistret för att ta reda på bilägarens eller förarens identitet.

Resonemanget överensstämmer inte med skäl 26 i dataskyddsdirektivet. Med tanke på att syftet med insamlingen av uppgifter tydligt är att identifiera och bötfälla fortkörare, är det förutsebart att man kommer att försöka identifiera fortkörarna. Även om de lokala myndigheterna inte direkt har tillgång till några identifieringsmöjligheter kommer de att vidarebefordra uppgifterna till den behöriga myndigheten, polisen, som har sådana möjligheter. I skäl 26 ingår också uttryckligen ett scenario där det är förutsebart att ytterligare mottagare av uppgifter, utöver den omedelbara användaren av uppgifterna, kan försöka identifiera den enskilda. Mot bakgrund av skäl 26 är den lokala myndighetens åtgärder likställiga med att samla in uppgifter om identifierbara personer, och det krävs därför en rättslig grund enligt lagstiftningen om skydd av personuppgifter.

Enligt Europarådets lagstiftning uppfattas identifierbarhet på ett liknande sätt. I artikel 1.2 i rekommendationen om betalningsuppgifter[59] exempelvis, anges att en person inte ska betraktas som ”identifierbar” om identifieringen kräver en orimlig mängd tid, kostnad eller arbetskraft.

Autentisering

Detta är ett förfarande genom vilket en person kan bevisa att han eller hon har en viss identitet och/eller har befogenhet att göra vissa saker, såsom att komma in på

59 Europarådet, ministerkommittén (1990), rekommendation nr R (90) 19 om skydd av personuppgifter som används vid betalningar och andra tillhörande åtgärder, 13 september 1990.

ett säkerhetsområde, eller ta ut pengar från ett bankkonto. Autentisering kan uppnås genom jämförelse av biometriska uppgifter, såsom ett foto eller fingeravtryck i ett pass, med uppgifter om den person som presenterar sig, exempelvis vid en invandringskontroll, eller genom att be om information som bör vara känd enbart av en person med en viss identitet eller tillstånd, såsom ett personligt identifieringsnummer (PIN) eller lösenord, eller genom att kräva uppvisande av ett visst kännetecken som enbart ska innehas av personen med en viss identitet eller tillstånd, såsom ett speciellt chipkort eller nyckel till ett bankfack. Utöver lösenord eller chipkort, ibland tillsammans med PIN, är elektroniska signaturer ett instrument som är särskilt avpassat för att identifiera och autentisera en person i elektronisk kommunikation.

Typ av uppgifter

All slags information kan vara personuppgifter under förutsättning att den gäller en person.

> Exempel: En överordnads bedömning av en anställds arbetsresultat, som lagras i den anställdas personliga akt, är personuppgifter om den personen, även om det endast helt eller delvis återspeglar den överordnades personliga uppfattning, exempelvis ”den anställda satsar inte på arbetet” och inte hårda fakta som ”den anställda har varit frånvarande från arbetet i fem veckor under de senaste sex månaderna”.

Personuppgifter omfattar information som rör en persons privatliv liksom information om hans eller hennes yrkesmässiga eller offentliga liv.

I *Amann*-målet[60] tolkade Europadomstolen begreppet ”personuppgifter” som att de inte var begränsade till frågor inom en enskild persons privata sfär (se avsnitt 2.1.1). Betydelsen av begreppet ”personuppgifter” är också relevant för dataskyddsdirektivet:

> Exempel: I målet *Volker och Markus Schecke och Hartmut Eifert mot Land Hessen*[61] slog EU-domstolen fast att ”[d]et saknar härvid betydelse att de uppgifter

60 Se Europadomstolen, *Amann mot Schweiz*, nr 27798/95, 16 februari 2000, punkt 65.

61 Förenade målen C-92/09 och C-93/09, *Volker und Markus Schecke GbR och Hartmut Eifert mot Land Hessen*, 9 november 2010, punkt 59.

som offentliggörs rör yrkesverksamhet [...]. Europadomstolen har i detta sammanhang, vad avser tolkningen av artikel 8 i Europakonventionen, förklarat att begreppet privatliv inte ska tolkas restriktivt och att 'det inte finns något principiellt skäl som talar emot att yrkesverksamhet ska omfattas av begreppet privatliv'."

Uppgifter rör personer även om innehållet i informationen indirekt avslöjar uppgifter om en person. I vissa fall, när det finns en nära koppling mellan ett föremål och en händelse – exempelvis en mobiltelefon, en bil, en olycka – å ena sidan, och en person – exempelvis dess ägare, användare eller offer – å andra sidan, borde information om ett föremål eller en händelse också betraktas som personuppgifter.

Exempel: I målet *Uzun mot Tyskland*[62] övervakades den klagande och en annan man via GPS-utrustning som monterats i den andra mannens bil på grund av deras misstänkta inblandning i bombattacker. I detta fall ansåg Europadomstolen att iakttagelse av den klagande via GPS var ett intrång i dennas privatliv som skyddas genom artikel 8 i Europakonventionen. GPS-övervakningen hade emellertid skett i enlighet med lagen och var dessutom proportionerlig mot det berättigade målet att undersöka flera åtalspunkter rörande försök till mord och var därför nödvändigt i ett demokratiskt samhälle. Domstolen drog slutsatsen att artikel 8 i Europakonventionen inte hade överträtts.

Form av förekomst av uppgifterna

Den form som personuppgifterna lagras eller används i är inte relevant för tillämpligheten av lagstiftningen om skydd av personuppgifter. Skriftliga eller talade meddelanden kan innehålla personuppgifter liksom bilder[63], inbegripet film[64] eller ljud[65] från övervakningskameror. Elektroniskt registrerad information, kan liksom information på papper vara personuppgifter, till och med cellprover av mänsklig vävnad kan vara personuppgifter, eftersom de registrerar personens DNA.

62 Europadomstolen, *Uzun mot Tyskland*, nr 35623/05, 2 september 2010.

63 Europadomstolen, *Von Hannover mot Tyskland*, nr 59320/00, 24 juni 2004, Europadomstolen, *Sciacca mot Italien*, nr 50774/99, 11 januari 2005.

64 Europadomstolen, *Peck mot Förenade kungariket*, nr 44647/98, 28 januari 2003, Europadomstolen, *Köpke mot Tyskland*, nr 420/07, 5 oktober 2010.

65 Dataskyddsdirektivet, skälen 16 och 17; Europadomstolen, *P.G. och J.H. mot Förenade kungariket*, nr 44787/98, 25 september 2001, punkt 59 och 60, Europadomstolen, *Wisse mot Frankrike*, nr 71611/01, 20 december 2005.

2.1.2. Särskilda kategorier av personuppgifter

Enligt EU-lagstiftningen och **Europarådets lagstiftning** finns det särskilda kategorier personuppgifter som, genom sin art kan utgöra en risk för den registrerade när de behandlas och därför behöver utökat skydd. Behandling av dessa särskilda kategorier av uppgifter (”känsliga uppgifter”) får därför tillåtas endast tillsammans med särskilda garantier.

När det gäller definitionen av känsliga uppgifter anges både i konvention 108 (artikel 6) och dataskyddsdirektivet (artikel 8) följande kategorier:

- personuppgifter som avslöjar ras eller etniskt ursprung;
- personuppgifter som avslöjar politiska åsikter eller religiösa eller andra övertygelser;
- personuppgifter som gäller hälsa eller sexualliv.

Exempel: I målet *Bodil Lindqvist*[66] slog EU-domstolen fast att ”uppgift om att en person har skadat sin fot och är deltidssjukskriven utgör en personuppgift om hälsa, i den mening som avses i artikel 8.1 i direktiv 95/46.”

I dataskyddsdirektivet anges även ”medlemskap i fackförening” som känsliga uppgifter, eftersom den informationen kan vara en stark indikator på politisk övertygelse eller anslutning.

Enligt konvention 108 anses också personuppgifter som hänför sig till att någon dömts för brott som känsliga.

I artikel 8.7 i dataskyddsdirektivet uppmanas EU:s medlemsstater att ”bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas.”

66 EU-domstolens dom av den 6 november 2003 i mål C-101/01, *Bodil Lindqvist*, punkt 51.

2.1.3. Anonymiserade och pseudonymiserade uppgifter

Enligt principen om begränsad lagring av uppgifter som ingår i dataskyddsdirektivet och i konvention 108 (och diskuteras mer i detalj i kapitel 3), måste uppgifter ”förvaras på ett sätt som förhindrar identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna samlades in eller för vilka de senare behandlades.”[67] Uppgifterna skulle behöva anonymiseras om en registeransvarig ville lagra dem efter att de blivit förlegade och inte längre tjänade sitt ursprungliga syfte.

Anonymiserade uppgifter

Uppgifter är anonymiserade om alla identifierande beståndsdelar har eliminerats från en uppsättning personuppgifter. Inga beståndsdelar får finnas kvar i informationen som genom en rimlig ansträngning skulle kunna användas för att på nytt identifiera den berörda personen/de berörda personerna.[68] När uppgifter har anonymiserats korrekt är de inte längre personuppgifter.

Om personuppgifter inte längre tjänar sitt ursprungliga syfte men ska bevaras i en personifierad form för historisk, statistisk eller vetenskaplig användning är detta enligt dataskyddsdirektivet och konvention 108 möjligt, under förutsättning att lämpliga garantier mot missbruk tillämpas.[69]

Pseudonymiserade uppgifter

Personlig information innehåller kännetecken som namn, födelsedatum, kön och adress. När personlig information pseudonymiseras ersätts kännetecknen av en pseudonym. Pseudonymisering uppnås exempelvis genom kryptering av kännetecken i personuppgifter.

Pseudonymiserade uppgifter nämns inte uttryckligen i de rättsliga definitionerna vare sig i konvention 108 eller dataskyddsdirektivet. I den förklarande rapporten till konvention 108 anges i artikel 42 emellertid att ”[k]ravet [...] rörande tidsfrister för lagring av uppgifter i sin namnförbundna form innebär inte att uppgifter efter

67 Dataskyddsdirektivet, artikel 6.1 e och konvention 108, artikel 5 e.

68 *Ibid.*, skäl 26.

69 *Ibid.*, artikel 6.1 e och konvention 108, artikel 5 e.

viss tid oåterkalleligt ska separeras från namnet på den person de är relaterade till, utan endast att det inte ska vara möjligt att enkelt koppla ihop uppgifterna och kännetecknen". Det är en effekt som kan uppnås genom att uppgifterna pseudonymiseras. För den som inte har tillgång till krypteringsnyckeln kan pseudonymiserade uppgifter med svårighet identifieras. Kopplingen till en identitet finns fortfarande i form av pseudonymen plus krypteringsnyckeln. För den som har rätt att använda krypteringsnyckeln är det enkelt att återidentifiera uppgifterna. Det krävs särskild vaksamhet för att förhindra att personer utan tillstånd använder krypteringsnycklar.

Eftersom pseudonymisering av uppgifter är ett av de viktigaste sätten att åstadkomma skydd av uppgifter i stor skala, när det inte är möjligt att helt avstå från att använda personuppgifter, måste logiken och effekten av denna åtgärd förklaras mer i detalj.

Exempel: Meningen "Charles Spencer, född den 3 april 1967, är far till fyra barn, två pojkar och två flickor" kan exempelvis pseudonymiseras enligt följande:

"C.S. 1967, är far till fyra barn, två pojkar och två flickor"; eller

"324, är far till fyra barn, två pojkar och två flickor"; eller

"YESz320l, är far till fyra barn, två pojkar och två flickor".

Användare som har tillgång till de pseudonymiserade uppgifterna har vanligtvis ingen möjlighet att identifiera "Charles Spencer, född den 3 april 1967" utifrån "324" eller "YESz320l". Pseudonymiserade uppgifter löper därför sannolikt mindre risk att missbrukas.

Det första exemplet är emellertid mindre säkert. Om meningen "C.S. 1967 är far till fyra barn, två pojkar och två flickor" används i det lilla samhälle där Charles Spencer bor, kan det vara lätt att känna igen honom. Metoden med pseudonymisering påverkar dataskyddets effektivitet.

Personuppgifter med krypterade kännetecken används i många sammanhang som ett sätt att hålla personers identitet hemlig. Detta är särskilt användbart när registeransvariga behöver se till att de hanterar samma registrerade person men inte kräver, eller inte borde ha, de registrerades verkliga identitet. Detta är exempelvis fallet när en forskare studerar en sjukdoms förlopp hos patienter, vars identitet är känd

endast av sjukhuset där de behandlas och varifrån forskaren får de pseudonymiserade fallstudierna. Pseudonymisering är därför ett viktigt inslag i raden av teknik för att förbättra respekten för privatlivet. Det kan fungera som en viktig beståndsdel vid genomförande av inbyggt integritetsskydd. Det innebär att dataskyddet är inbyggt i konstruktionen av avancerade databehandlingssystem.

2.2. Behandling av uppgifter

Viktiga punkter

- Begreppet ”behandling” hänför sig i första hand till automatisk behandling.
- Enligt EU-lagstiftningen hänför sig ”behandling” dessutom till manuell behandling i strukturerade lagringssystem.
- Enligt Europarådets lagstiftning kan betydelsen av ”behandling” utvidgas av den inhemska lagstiftningen till att även innefatta manuell hantering.

Dataskydd enligt konvention 108 och dataskyddsdirektivet är huvudsakligen inriktat på automatisk databehandling.

I **Europarådets lagstiftning** erkänns i definitionen av automatisk behandling emellertid att vissa stadier av manuell användning av personuppgifter kan krävas mellan automatiska åtgärder. På samma sätt definieras, enligt **EU:s lagstiftning**, automatisk behandling av uppgifter som ”åtgärder som vidtas med personuppgifter, helt eller delvis på automatisk väg”.[70]

Exempel: I målet *Bodil Lindqvist*[71] ansåg EU-domstolen att:

”omnämnandet av olika personer – vilka identifieras med namn eller på annat sätt, till exempel med telefonnummer eller med uppgifter om deras arbetsförhållanden och fritidsintressen – på en webbsida utgör en ’behandling av personuppgifter som helt eller delvis företas på automatisk väg’, i den mening som avses i artikel 3.1 i direktiv 95/46.”

Manuell behandling av uppgifter kräver också dataskydd.

70 Konvention 108, artikel 2 c och dataskyddsdirektivet, artikel 2 b och artikel 3.1.

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

Dataskydd **enligt EU-lagstiftningen** är inte på något sätt begränsat till automatisk databehandling. Enligt EU-lagstiftningen gäller dataskydd för behandling av personuppgifter i ett manuellt registreringssystem, det vill säga ett särskilt utformat pappersarkiv.[72] Skälet till denna utvidgning av dataskyddet är att:

- pappersarkiv kan struktureras på ett sätt som gör det enkelt och snabbt att hitta information; och

- lagring av personuppgifter i strukturerade pappersarkiv gör det enklare att kringgå restriktionerna i lagen för automatisk databehandling.[73]

Enligt Europarådets lagstiftning reglerar konvention 108 i första hand databehandling i automatiska dataarkiv.[74] Det ger emellertid också möjlighet att utvidga skyddet till manuell behandling i inhemsk lag. Många parter till konvention 108 har utnyttjat denna möjlighet och uttalat sig om detta till Europarådets generalsekreterare.[75] Utvidgning av dataskyddet enligt ett sådant uttalande måste hänföra sig till all manuell databehandling och kan inte begränsas till behandling i manuella arkivsystem.[76]

När det gäller sättet att behandla de processer som ingår är begreppet behandling omfattande **enligt både EU-lagstiftning och Europarådets lagstiftning:** ”behandling av personuppgifter […] ska avse varje åtgärd […] till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring”[77] som utförs med personuppgifter. Begreppet ”behandling” innefattar också åtgärder genom vilka uppgifterna inte längre är en registeransvarigs ansvar utan överförs till en annan registeransvarig.

Exempel: Arbetsgivare samlar in och behandlar uppgifter om sina anställda, inbegripet information rörande deras löner. Rättslig grund för att lagligt göra detta är anställningsavtalet.

72 Dataskyddsdirektivet, artikel 3.1.

73 *Ibid.*, skäl 27.

74 Konvention 108, Artikel 2 b.

75 Se deklarationerna enligt konvention 108, artikel 3.2 c.

76 Se lydelsen i konvention 108, artikel 3.2.

77 Dataskyddsdirektivet, artikel 2 b. Se även konvention 108, artikel 2 c.

Arbetsgivare måste lämna sin personals löneuppgifter till skattemyndigheterna. Denna vidarebefordran av uppgifter kommer också att innebära ”behandling” enligt betydelsen av detta begrepp i konvention 108 och i direktivet. Den rättsliga grunden för att lagligt göra detta är emellertid inte anställningsavtalet. Det måste finnas ytterligare en rättslig grund för behandlingen som leder till att löneuppgifter överförs från arbetsgivaren till skattemyndigheterna. Den rättsliga grunden ingår vanligtvis i bestämmelserna i nationell skattelagstiftning. Utan dessa bestämmelser skulle det inte vara tillåtet att överföra uppgifterna.

2.3. Användare av personuppgifter

Viktiga punkter

- Den som beslutar att bearbeta personuppgifter om andra är ”registeransvarig” enligt lagstiftningen om skydd av personuppgifter. Om flera personer fattar detta beslut gemensamt kan de vara ”gemensamt registeransvariga”.
- En ”registerförare” är en juridiskt separat enhet som behandlar personuppgifter för den registeransvarigas räkning.
- En registerförare blir en registeransvarig om han eller hon använder uppgifter i eget syfte, och inte följer den registeransvarigas instruktioner.
- Alla som mottar uppgifter från en registeransvarig är ”mottagare”.
- En ”tredje part” är en fysisk eller juridisk person som inte agerar efter instruktioner från den registeransvariga (och inte är den registrerade).
- En ”tredjepartsmottagare” är en person eller enhet som är juridiskt skild från den registrerade, men erhåller personuppgifter från den registrerade.

2.3.1. Registeransvariga och registerförare

Den viktigaste konsekvensen av att vara registeransvarig eller registerförare är det juridiska ansvaret för att uppfylla respektive skyldigheter enligt dataskyddslagen. Endast de som kan hållas ansvariga enligt tillämplig lag kan därför ta på sig dessa uppgifter. Inom den privata sektorn är det vanligtvis en fysisk eller juridisk person, inom den offentliga sektorn är det vanligtvis en myndighet. Andra enheter, såsom organ eller institutioner utan juridisk person, kan vara registeransvariga eller registerförare endast när det finns särskilda juridiska bestämmelser för detta.

Exempel: När marknadsavdelningen vid företaget Sunshine planerar att behandla uppgifter för en marknadsundersökning blir företaget, inte marknadsavdelningen, registeransvarig för denna behandling. Marknadsavdelningen kan inte vara registeransvarig eftersom den inte är en separat juridisk person.

I företagskoncerner räknas moderföretaget och respektive dotterbolag som separata registeransvariga eller registerförare eftersom de är separata juridiska enheter. Som en konsekvens av denna juridiskt separata ställning kommer överföringen av uppgifter mellan företag i en koncern att kräva en särskild rättslig grund. Det är inget privilegium att tillåta utbyte av personuppgifter som sådant mellan de separata juridiska enheterna inom företagskoncernen.

Privatpersoners roll behöver nämnas i detta sammanhang. **Enligt EU-lagstiftningen** omfattas privatpersoner, när de behandlar uppgifter om andra i en rent personlig verksamhet eller i ett hushåll, inte av reglerna i dataskyddsdirektivet och de ska inte vara registeransvariga.[78]

Rättspraxis har emellertid visat att dataskyddslagstiftningen ändå gäller när en privatperson vid användning av internet publicerar uppgifter om andra.

Exempel: EU-domstolen vidhöll i målet *Bodil Lindqvist*[79] att:

”omnämnandet av olika personer [...] på en webbsida utgör en ’behandling av personuppgifter som helt eller delvis företas på automatisk väg’, i den mening som avses i artikel 3.1 i direktiv 95/46.”[80]

Denna behandling av personuppgifter faller inte under rent personlig eller inhemsk verksamhet som ligger utanför dataskyddsdirektivets omfattning, eftersom detta undantag ”skall [...] tolkas så, att det endast avser sådan verksamhet som utgör en del av enskildas privat- eller familjeliv, vilket uppenbart inte är fallet i fråga om sådan behandling av personuppgifter som består i att de offentliggörs på internet och därmed blir åtkomliga för ett obestämt antal personer.”[81]

78 Dataskyddsdirektivet, skäl 12 och artikel 3.2, sista strecksatsen.

79 EU-domstolens dom av den 6 november 2003 i mål C-101/01, *Bodil Lindqvist*.

80 *Ibid.*, punkt 27.

81 *Ibid.*, punkt 47.

Registeransvarig

Enligt EU-lagstiftningen definieras en registeransvarig som någon som ”på egen hand eller tillsammans med andra fastställer ändamålen med och medlen för behandlingen av personuppgifter”.[82] I en registeransvarigs beslut fastställs varför och hur uppgifterna ska behandlas. **I Europarådets lagstiftning** anges i definitionen av ”registeransvarig” dessutom att denna beslutar om vilka kategorier av personuppgifter som ska lagras.[83]

I konvention 108 hänvisas i definitionen av en registeransvarig till ytterligare aspekter av registeransvaret som kräver övervägande. Definitionen hänvisar till frågan om vem som har tillåtelse att behandla vissa uppgifter för vissa syften. När påstådd olaglig behandling äger rum och den ansvariga registeransvariga måste hittas, blir det emellertid den person eller enhet, som t.ex. ett företag eller en myndighet, som beslutar att uppgifterna ska behandlas oberoende av om det var juridiskt berättigat att göra det eller inte[84] som anses vara den registeransvariga. En begäran om radering måste därför alltid lämnas till den ”faktiska” registeransvariga.

Gemensamt registeransvar

Definitionen av ”registeransvarig” i dataskyddsdirektivet innebär att det också kan finnas flera juridiskt separata enheter som tillsammans eller gemensamt med andra fungerar som registeransvarig. Det innebär att de beslutar tillsammans att behandla uppgifter för ett gemensamt syfte.[85] Detta är emellertid juridiskt möjligt endast när en särskild rättslig grund gör det möjligt att behandla uppgifterna gemensamt för ett gemensamt syfte.

Exempel: En databas som flera kreditinstitutioner driver gemensamt om sina försumliga kunder är ett vanligt exempel på gemensamt registeransvar. När någon ansöker om en kreditlimit från en bank som är en av de gemensamma registeransvariga kontrollerar bankerna databasen för att kunna fatta informerade beslut om den klagandes kreditvärdighet.

82 Dataskyddsdirektivet, artikel 2 d.

83 Konvention 108, Artikel 2 d.

84 Se även artikel 29-gruppen (2010), *Yttrande 1/2010 om begreppen registeransvarig och registerförare*, WP 169, Bryssel, 16 februari 2010, s. 15.

85 Dataskyddsdirektivet, artikel 2 d.

I bestämmelserna fastställs inte uttryckligen huruvida gemensamt registeransvar kräver att det delade syftet ska vara detsamma för var och en av de registeransvariga eller huruvida det är tillräckligt om deras syften endast delvis överlappar varandra. Ingen relevant rättspraxis är emellertid ännu tillgänglig på europeisk nivå och det finns inte heller någon klarhet kring konsekvenserna när det gäller ansvar. Artikel 29-gruppen förespråkar en bredare tolkning av begreppet gemensamt registeransvar i syfte att möjliggöra viss flexibilitet för att sörja för den ökande komplexiteten i verkligheten när det gäller gängse databehandling.[86] Ett mål som innefattar Society for Worldwide Interbank Financial Telecommunication (SWIFT) illustrerar arbetsgruppens ståndpunkt.

Exempel: I det så kallade SWIFT-målet anlitade europeiska bankinstitutioner SWIFT, ursprungligen som registerförare, för att överföra uppgifter under banktransaktioner. SWIFT lämnade ut dessa uppgifter om banktransaktioner, lagrade i dataservicecentrum i Förenta staterna, till det amerikanska finansdepartementet utan att uttryckligen blivit ombedd att göra det av de europeiska bankinstitutioner som anlitat SWIFT. När artikel 29-gruppen utvärderade lagligheten i situationen kom den till slutsatsen att europeiska bankinstitutioner som anlitar SWIFT, liksom SWIFT själv, måste betraktas som gemensamt registeransvariga inför europeiska kunder när det gäller utlämning av deras uppgifter till de amerikanska myndigheterna.[87] Genom att besluta om att lämna ut uppgifterna hade SWIFT – utan tillåtelse – intagit rollen som registeransvarig, och bankinstitutionerna hade uppenbarligen svikit sin skyldighet att övervaka registerföraren och kunde därför inte helt fritas från ansvaret som registeransvariga. Situationen resulterar i gemensamt registeransvar.

Registerförare

En ”registerförare” definieras **enligt EU-lagstiftningen** som någon som behandlar personuppgifter för en registeransvarigs räkning.[88] Den verksamhet som anförtros en registerförare kan vara begränsad till en mycket specifik uppgift eller ett mycket specifikt sammanhang eller kan vara relativt allmän och omfattande.

86 Artikel 29-gruppen (2010), *Yttrande 1/2010 om begreppen registeransvarig och registerförare*, WP 169, Bryssel, 16 februari 2010, s. 19.

87 Artikel 29-gruppen (2006), *Yttrande 10/2006 om behandling av personuppgifter hos SWIFT (Society for Worldwide Interbank Financial Telecommunication),* WP 128, Bryssel, 22 november 2006.

88 Dataskyddsdirektivet, artikel 2 e.

I Europarådets lagstiftning är betydelsen av en registerförare densamma som i EU-lagstiftningen.

Utöver att registerförare behandlar uppgifter för andra, är de också registeransvariga i egen rätt i förhållande till den behandling de utför för egna syften, t.ex. administrationen av sina egna anställda, försäljning och konton.

Exempel: Företaget Everready är specialiserat på databehandling för administration av uppgifter om personal för andra företag. I den funktionen är Everready registerförare.

När Everready behandlar uppgifterna om sina egna anställda är företaget emellertid registeransvarig för databehandlingsåtgärderna i syfte att uppfylla sina skyldigheter som arbetsgivare.

Relationen mellan registeransvarig och registerförare

Som vi har sett definieras den registeransvariga som den person som fastställer syften och medel för behandling.

Exempel: Direktören för företaget Sunshine beslutar att företaget Moonlight, som är specialiserat inom marknadsanalys, ska genomföra en marknadsanalys av Sunshines kunduppgifter. Även om uppgiften att fastställa sättet att behandla uppgifterna därigenom delegeras till Moonlight, är Sunshine fortfarande registeransvarig och Moonlight är endast registerförare eftersom Moonlight, enligt avtalet, kan använda kunduppgifterna från Sunshine endast i de syften som Sunshine fastställer.

Om befogenheten att fastställa sätten att behandla uppgifterna delegeras till en registerförare, måste den registeransvariga ändå kunna ingripa i registerförarens beslut när det gäller möjligheterna till behandling. Det övergripande ansvaret ligger fortfarande hos den registeransvariga som måste övervaka registerförarna för att se till att deras beslut överensstämmer med dataskyddslagen. Ett avtal som förbjuder den registeransvariga att hindra registerförarens beslut skulle därför sannolikt tolkas som att det leder till ett gemensamt registeransvar, där båda parter delar det juridiska ansvaret som registeransvarig.

Om en registerförare dessutom inte skulle rätta sig efter begränsningarna för uppgifter såsom de föreskrivs av den registeransvariga, måste registerföraren bli registeransvarig minst i den mån som den registeransvariga överträder sina instruktioner. Detta gör högst sannolikt registerföraren till en registeransvarig som agerar utan tillstånd. Den ursprungliga registeransvariga kommer å sin sida att tvingas förklara hur det var möjligt för registerföraren att överträda sitt uppdrag. Artikel 29-gruppen tenderar definitivt att förutsätta gemensamt registeransvar i dessa fall, eftersom detta leder till det bästa skyddet av de registrerades intressen.[89] En viktig konsekvens av gemensamt registeransvar bör vara solidariskt ansvar för skador, som erbjuder de registrerade större möjligheter till prövning.

Det kan också finnas frågor om ansvarsfördelningen när en registeransvarig är ett litet företag och registerföraren ett stort bolag som har möjlighet att diktera villkoren för sina tjänster. Under dessa förhållanden vidhåller artikel 29-gruppen emellertid att ansvarsstandarden inte bör sänkas på grund av ekonomisk obalans och att förståelsen av begreppet registeransvarig måste bibehållas.[90]

För tydlighetens och öppenhetens skull bör detaljerna i förhållandet mellan en registeransvarig och en registerförare registreras i ett skriftligt kontrakt.[91] Om inget sådant avtal finns är det en överträdelse av den registeransvarigas skyldighet att tillhandahålla skriftlig dokumentation om ömsesidigt ansvar och kan leda till sanktioner.[92]

Registerförare kan vilja delegera vissa uppgifter till ytterligare underregisterförare. Detta är juridiskt tillåtet och kommer att i detalj bero på de avtalsmässiga bestämmelserna mellan den registeransvariga och registerföraren, inbegripet huruvida den registeransvarigas tillstånd krävs i varje enskilt fall eller om det räcker att enbart informera.

89 Artikel 29-gruppen (2010), *Yttrande 1/2010 om begreppen registeransvarig och registerförare* WP 169, Bryssel, 16 februari 2010, s. 25; och artikel 29-gruppen (2006), *Yttrande 10/2006 om behandling av personuppgifter hos SWIFT (Society for Worldwide Interbank Financial Telecommunication)*, WP 128, Bryssel, 22 november 2006.

90 Artikel 29-gruppen (2010), *Yttrande 1/2010 om begreppen registeransvarig och registerförare*, WP 169, Bryssel, 16 februari 2010, s. 26.

91 Dataskyddsdirektivet, artikel 17.3 och 17.4.

92 Artikel 29-gruppen (2010), *Yttrande 1/2010 om begreppen registeransvarig och registerförare*, WP 169, Bryssel, 16 februari 2010, s. 27.

Enligt Europarådets lagstiftning är tolkningen av begreppen registeransvarig och registerförare enligt förklaringen ovan fullt tillämplig, vilket framgår av rekommendationerna som har utarbetats i enlighet konvention 108.[93]

2.3.2. Mottagare och tredjeparter

Skillnaden mellan dessa två kategorier personer eller enheter som infördes genom dataskyddsdirektivet ligger huvudsakligen i deras förhållande till den registeransvariga och, därmed i deras tillåtelse att få tillgång till personuppgifter som innehas av den registeransvariga.

En ”tredje part” är någon som är juridiskt skild från den registeransvariga. Att lämna ut uppgifter till en tredje part kommer därför alltid att kräva en särskild rättslig grund. Enligt artikel 2 f i dataskyddsdirektivet är en tredje part ”den fysiska eller juridiska person, den myndighet, den institution eller det andra organ än den registrerade, den registeransvarige, registerföraren och de personer som under den registeransvariges eller registerförarens direkta ansvar har befogenhet att behandla uppgifterna”. Det innebär att personer som arbetar för en organisation som är juridiskt skild från den registeransvariga – även om den tillhör samma koncern eller företag – kommer att vara (eller tillhöra) ”tredje part”. Å andra sidan skulle en banks filialer som behandlar kunders konton under direkt överinseende av sina huvudkontor inte betraktas som ”tredje parter”.[94]

”Mottagare” är ett bredare begrepp än ”tredje part”. I den mening som avses i artikel 2 g i dataskyddsdirektivet är en mottagare ”den fysiska eller juridiska person, den myndighet, den institution eller det andra organ till vilket uppgifterna utlämnas, vare sig det är en tredje man eller inte”. Mottagaren kan antingen vara en person som inte är registeransvarig eller registerförare – det skulle då vara en tredje part – eller någon hos den registeransvariga eller registerföraren, såsom en anställd eller en annan avdelning inom samma företag eller myndighet.

Distinktionen mellan mottagare och tredje parter är viktig endast på grund av villkoren för tillåten spridning av uppgifter. De anställda hos en registeransvarig eller registerförare kan utan ytterligare rättsliga krav vara mottagare av personuppgifter om de är involverade i behandlingsförfarandet hos den registeransvariga eller

93 Se exempelvis rekommendationen om profilering, artikel 1.

94 Artikel 29-gruppen (2010), *Yttrande 1/2010 om begreppen registeransvarig och registerförare*, WP 169, Bryssel, 16 februari 2010, s. 31.

registerföraren. Å andra sidan får en tredje part, som lagligen är skild från den registeransvariga eller registerföraren, inte använda personuppgifter som behandlas av den registeransvariga om det inte föreligger specifika rättsliga grunder i ett specifikt fall. Tredjepartsmottagare av uppgifter behöver därför alltid en rättslig grund för att få ta emot personuppgifter.

Exempel: En registerförares anställda, som använder personuppgifter inom de befogenheter som arbetsgivaren anförtrott honom eller henne, är mottagare av uppgifter, men inte en tredje part, eftersom han eller hon använder uppgifterna i registerförarens namn och enligt dennas instruktioner.

Om emellertid samma anställda beslutar att använda uppgifterna, som han eller hon kan få tillgång till som anställd hos registerföraren, för sina egna syften och säljer dem till ett annat företag, har den anställda agerat som en tredje part. Han eller hon följer inte längre registerförarens (arbetsgivarens) order. Som tredje part skulle den anställda behöva en rättslig grund för att förvärva och sälja uppgifterna. I detta exempel har den anställda definitivt inte en sådan rättslig grund och dessa åtgärder är därför olagliga.

2.4. Samtycke

Viktiga punkter

- Samtycke som en rättslig grund för att behandla personuppgifter måste vara fritt, informerat och specifikt.
- Samtycket måste ha lämnats otvetydigt. Samtycke kan antingen lämnas uttryckligen eller underförstått genom att den registrerade agerar på ett sätt som inte lämnar några tvivel om att han eller hon godkänner att uppgifterna behandlas.
- Behandling av känsliga uppgifter på grundval av samtycke kräver uttryckligt samtycke.
- Samtycket kan när som helst dras tillbaka.

Samtycke innebär ”varje fritt lämnad specifik och informerad indikation om den registrerades önskemål”.[95] Det är i många fall den rättsliga grunden för berättigad behandling av uppgifter (se avsnitt 4.1).

95 Dataskyddsdirektivet, artikel 2 h.

2.4.1. Beståndsdelar i ett giltigt samtycke

I **EU-lagstiftningen** anges tre beståndsdelar som krävs för att ett samtycke ska vara giltigt, vilket syftar till att garantera att de registrerade verkligen avsåg att godkänna att uppgifter fick användas:

- den registrerade får inte ha varit under press vid samtycket;
- den registrerade måste ha blivit vederbörligen informerad om syftet och konsekvenserna av samtycket; och
- samtyckets omfattning måste vara rimligt konkret.

Endast om alla dess krav är uppfyllda kommer samtycket att vara giltigt i den mening som avses i dataskyddsdirektivet.

Konvention 108 innehåller ingen definition av samtycke. Detta återfinns i den inhemska lagstiftningen. **Enligt Europarådets lagstiftning** motsvarar beståndsdelarna i ett giltigt samtycke de som förklarats tidigare, eftersom de härrör ur rekommendationerna som har utvecklats enligt konvention 108.[96] Kraven för samtycke är desamma för en giltig avsiktsförklaring enligt europeisk civilrätt.

Ytterligare krav enligt civilrätten för giltigt samtycke, såsom rättskapacitet, gäller naturligt också mot bakgrund av uppgiftsskyddet, eftersom dessa krav är grundläggande juridiska förutsättningar. Ogiltigt samtycke från personer som inte har rättskapacitet innebär att det saknas en rättslig grund för att behandla uppgifter om dessa personer.

Samtycke kan lämnas antingen uttryckligen eller[97] underförstått. Det förra medför ingen tvekan om den registrerades avsikt och kan antingen ske muntligt eller skriftligt medan den senare är en slutsats på grund av omständigheterna. Varje samtycke måste lämnas på ett otvetydigt sätt.[98] Det innebär att det inte ska finnas några rimliga tvivel om att den registrerade ville lämna sitt medgivande för att tillåta behandling av hans eller hennes uppgifter. Att dra slutsatsen om samtycke endast på grund av inaktivitet innebär exempelvis inte att lämna otvetydigt samtycke. Om

96 Se exempelvis konvention 108, statistiska rekommendationer om uppgifter, punkt 6.

97 Dataskyddsdirektivet, artikel 8.2.

98 *Ibid.*, Artikel 7 a och artikel 26.1.

de uppgifter som ska behandlas är känsliga, är uttryckligt samtycke obligatoriskt och måste vara otvetydigt.

Frivilligt samtycke

Förekomsten av frivilligt samtycke är giltigt endast ”om den registrerade kan utöva ett verkligt val och det inte finns någon risk för besvikelse, hotelser, tvång eller betydande negativa konsekvenser om han eller hon inte ger sitt samtycke”.[99]

Exempel: På många flygplatser måste passagerarna passera en kroppsskanner för att komma in på boardingområdet.[100] Under förutsättning att passagerarnas uppgifter behandlas under skanningen måste behandlingen överensstämma med en av de rättsliga grunderna enligt artikel 7 i dataskyddsdirektivet (se avsnitt 4.1.1). Att passera en kroppsskanner presenteras ibland för passagerarna som en möjlighet vilket innebär att deras samtycke skulle kunna motivera behandlingen. Passagerarna kan emellertid vara rädda för att deras vägran att passera kroppsskannern kan skapa misstänksamhet, eller leda till ytterligare kontroller, såsom kroppsvisitering. Många passagerare samtycker till att skannas eftersom de genom att göra det undviker potentiella problem eller förseningar. Ett sådant samtycke är sannolikt inte tillräckligt frivilligt.

En sund laglig grund kan därför endast återfinnas i en handling från lagstiftaren, baserat på artikel 7 e i dataskyddsdirektivet, som innebär en skyldighet för passagerarna att samarbeta på grund av ett överordnat allmänt intresse. En sådan lagstiftning kan fortfarande erbjuda ett val mellan skanning och manuell kontroll, men endast som en del av ytterligare åtgärder för gränskontroll som krävs under särskilda omständigheter. Detta är vad Europeiska kommissionen angav i två förordningar om säkerhetsskanning 2011.[101]

99 Se även artikel 29-gruppen (2011), *Yttrande 15/2011 om begreppet samtycke*, WP 187, Bryssel, 13 juli 2011, s. 12.

100 Exemplet kommer från *Ibid.*, s. 15.

101 Kommissionens förordning (EU) nr 1141/2011 av den 10 november 2011 om ändring av förordning (EG) nr 272/2009 om komplettering av gemensamma grundläggande standarder för skydd av civil luftfart beträffande användningen av säkerhetsskannrar vid flygplatser inom EU, EUT 2011 L 293, och kommissionens genomförandeförordning (EU) nr 1147/2011 av den 11 november 2011 om ändring av förordning (EU) nr 185/2010 om genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd beträffande användningen av säkerhetsskannrar vid EU:s flygplatser, EUT 2011 L 294.

Frivilligt samtycke kan också hotas av underordnade situationer när det föreligger en betydande ekonomisk eller annan obalans mellan den registeransvariga som säkerställer samtycke och den registrerade som ger sitt samtycke.[102]

Exempel: Ett stort företag planerar att skapa ett register som innehåller namnen på alla anställda, deras funktion i företaget och deras företagsadress, enbart för att förbättra den interna kommunikationen i företaget. Personalchefen föreslår att man ska lägga till ett foto på varje anställd i registret så att det exempelvis blir enklare att känna igen kolleger vid möten. Personalrepresentanter kräver att detta endast ska ske om den enskilda medarbetaren ger sitt samtycke.

I en sådan situation ska medarbetarens samtycke vara den rättsliga grunden för att behandla fotografierna i registret eftersom det är uppenbart att ett foto som publiceras i registret inte har några negativa konsekvenser i sig, och det är dessutom sannolikt att medarbetaren inte kommer att möta negativa effekter från arbetsgivaren om han eller hon inte vill ha sitt foto i registret.

Detta innebär emellertid inte att samtycke inte kan vara giltigt i sammanhang då det skulle få negativa konsekvenser om någon inte vill ge sitt samtycke. Om det faktum att man inte samtycker till att få ett kundkort i en stormarknad endast leder till att man inte får prisavdrag för vissa varor, är samtycke fortfarande en giltig rättslig grund för att behandla personuppgifter för de kunder som samtyckte till att få ett sådant kort. Det föreligger inget underordnat förhållande mellan företaget och kunden, och konsekvenserna om man inte ger sitt samtycke är inte tillräckligt allvarliga för den registrerade för att förhindra ett fritt val.

Å andra sidan: så snart tillräckligt viktiga varor eller tjänster kan erhållas endast och exklusivt om vissa personuppgifter lämnas till tredje part, kan den registrerades samtycke till att hans eller hennes uppgifter lämnas ut vanligtvis inte anses som ett frivilligt beslut och är därför inte giltigt enligt dataskyddslagen.

Exempel: Godkännande från ett flygbolags passagerare om överföring av passageraruppgifter (så kallade PNR-uppgifter), det vill säga uppgifter om deras identitet, matvanor eller hälsoproblem till invandrarmyndigheterna i ett visst

102 Se även artikel 29-gruppen (2001), *Yttrande 8/2001 om behandling av personuppgifter i anställningsförhållanden*, WP 48, Bryssel, 13 september 2001; och artikel 29-gruppen (2005), *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, WP 114, Bryssel, 25 november 2005.

land kan inte anses som ett giltigt samtycke enligt dataskyddslagstiftningen, eftersom passagerarna inte har något val om de vill besöka landet i fråga. Om dessa uppgifter ska överföras lagenligt krävs en annan rättslig grund än samtycke – sannolikt en särskild lag.

Informerat samtycke

Den registrerade måste ha tillräckligt med information innan han eller hon fattar sitt beslut. Huruvida informationen är tillräcklig kan endast beslutas från fall till fall. Vanligtvis omfattar informerat samtycke en exakt och lättförståelig beskrivning av det ämne som kräver samtycke och dessutom en redogörelse för konsekvenserna av att ge sitt samtycke eller ej. Det språk som används för att informera bör anpassas till de förutsebara mottagarna av informationen.

Informationen måste också vara lättillgänglig för den registrerade. Informationens tillgänglighet och synlighet är viktiga beståndsdelar. I en digital miljö kan informationsmeddelanden på flera nivåer vara en bra lösning, eftersom den registrerade, utöver en kortfattad version av informationen, också kan få tillgång till en mer omfattande version.

Specifikt samtycke

För att vara giltigt måste samtycket också vara specifikt. Detta går hand i hand med kvaliteten på den information som lämnas om syftet med samtycket. I detta sammanhang är en genomsnittlig registrerads rimliga förväntningar relevanta. Den registrerade måste återigen ombes att ge sitt samtycke om behandlingsförfaranden ska läggas till eller ändras på ett sätt som rimligen inte kan förutses när det inledande samtycket gavs.

Exempel: I målet *Deutsche Telekom AG*[103] tog EU-domstolen upp frågan om huruvida en telekomleverantör som behövde lämna personuppgifter om prenumeranter enligt artikel 12 i *direktivet om privatliv och elektronisk*

103 EU-domstolen, C-543/09, *Deutsche Telekom AG mot Bundesrepublik Deutschland*, 5 maj 2011, se särskilt punkterna 53 och 54.

kommunikation[104] behövde ett förnyat samtycke från de registrerade, eftersom mottagarna inte ursprungligen namngavs när samtycket gavs.

EU-domstolen ansåg att enligt den artikeln krävdes inte förnyat samtycke innan uppgifterna lämnades ut eftersom de registrerade enligt denna bestämmelse hade möjlighet att samtycka till endast syftet med behandlingen, som är publicering av deras uppgifter, och de kunde inte välja mellan olika register där uppgifterna skulle kunna offentliggöras.

Domstolen underströk att "det följer av en kontextuell och systematisk tolkning av artikel 12 i direktivet om integritet och elektronisk kommunikation att samtycket enligt andra punkten i nämnda artikel avser ändamålet med offentliggörandet av personuppgifter i en allmän abonnentförteckning och inte vem som i det enskilda fallet tillhandahåller abonnentförteckningen".[105] Det är dessutom "själva offentliggörandet av personuppgifter i en abonnentförteckning med ett särskilt ändamål som kan visa sig vara till förfång för en abonnent"[106] och inte vem som ligger bakom offentliggörandet.

2.4.2. Rätten att när som helst dra tillbaka samtycke

I dataskyddsdirektivet nämns ingen generell rätt att när som helst dra tillbaka ett samtycke. Det antas emellertid allmänt att en sådan rätt finns och att det måste vara möjligt för den registrerade att utöva den när han eller hon vill. Det bör inte finnas några krav på att ge en anledning till tillbakadragandet och ingen risk för negativa konsekvenser utöver att eventuella förmåner, som kan ha varit följden av den tidigare godkända användningen av uppgifterna, kan komma att avslutas.

Exempel: En kund samtycker till att erhålla reklamutskick per e-post till en adress som han eller hon lämnar till en registeransvarig. Om kunden skulle dra tillbaka sitt samtycke måste den registeransvariga omedelbart sluta med reklamutskicken. Inga straff såsom avgifter får förekomma.

104 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT 2002 L 201.

105 EU-domstolen, C-543/09, *Deutsche Telekom AG mot Bundesrepublik Deutschland*, 5 maj 2011; se särskilt punkt 61

106 *Ibid.*, se särskilt punkt 62.

Om kunden fick 5 % rabatt på kostnaden för ett hotellrum i utbyte mot att samtycka till att hans eller hennes epostadress används för reklamutskick ska inte ett senare tillbakadragande av samtycket leda till att dessa rabatter ska betalas tillbaka.

3

Huvudprinciper i den europeiska lagstiftningen om skydd av personuppgifter

EU	Frågor som täcks	Europarådet
Dataskyddsdirektivet, Artikel 6.1 a och 6.1 b EU-domstolen, C-524/06, *Huber mot Bundesrepublik Deutschland*, 16 december 2008 EU-domstolen, förenade målen C-92/09 och C93/09, *Volker och Markus Schecke GbR och Hartmut Eifert mot Land Hessen*, 9 november 2010	**Principen om tillåten behandling**	Konvention 108, artikel 5 a och 5 b Europadomstolen, *Rotaru mot Rumänien* [GC], nr 28341/95, 4 maj 2000 Europadomstolen, *Taylor-Sabori mot Förenade kungariket*, nr 47114/99, 22 oktober 2002 Europadomstolen, *Peck mot Förenade kungariket*, nr 44647/98, 28 januari 2003 Europadomstolen, *Khelili mot Schweiz*, nr 16188/07, 18 oktober 2011 Europadomstolen, *Leander mot Sverige*, nr 9248/81, 26 mars 1987
Dataskyddsdirektivet, artikel 6.1 b	**Principen om specifikation och begränsning av syftet**	Konvention 108, Artikel 5 b
	Principerna om uppgiftskvalitet:	
Dataskyddsdirektivet, artikel 6.1 c	**Uppgifternas relevans**	Konvention 108, Artikel 5 c

EU	Frågor som täcks	Europarådet
Dataskyddsdirektivet, artikel 6.1 d	Uppgifternas riktighet	Konvention 108, Artikel 5 d
Dataskyddsdirektivet, artikel 6.1 e	Begränsad lagring av uppgifter	Konvention 108, Artikel 5 e
Dataskyddsdirektivet, artikel 6.1 e	Undantag för vetenskaplig forskning och statistik	Konvention 108, Artikel 9.3
Dataskyddsdirektivet, artikel 6.1 a	Principen om rättvis behandling	Konvention 108, Artikel 5 a Europadomstolen, *Haralambie mot Rumänien*, nr 21737/03, 27 oktober 2009 Europadomstolen, *K.H. m.fl. mot Slovakien*, nr 32881/04, 28 april 2009
Dataskyddsdirektivet, artikel 6.2	Principen om ansvarighet	

Principerna i artikel 5 i konvention 108 innehåller det viktigaste i den europeiska dataskyddslagstiftningen. De återfinns även i artikel 6 i dataskyddsdirektivet som utgångspunkt för mer detaljerade bestämmelser i de senare artiklarna i direktivet. All senare dataskyddslagstiftning inom Europarådet eller på EU-nivå måste uppfylla dessa principer och de måste beaktas vid tolkning av lagstiftningen. Eventuella undantag från och restriktioner kring dessa huvudprinciper måste ske på nationell nivå.[107] De måste åstadkommas genom lagstiftning, ha ett berättigat syfte och vara nödvändiga i ett demokratiskt samhälle. Samtliga tre villkor måste uppfyllas.

3.1. Principen om tillåten behandling

Viktiga punkter

- För att förstå principen om tillåten behandling måste man hänvisa till villkoren för lagliga begränsningar av rätten till uppgiftsskydd mot bakgrund av artikel 52.1 i stadgan och kraven på berättigat ingripande enligt artikel 8.2 i Europakonventionen.

107 Konvention 108, artikel 9 2, dataskyddsdirektivet, artikel 13 och artikel 9.2.

- Behandling av personuppgifter är tillåtet endast om den:
  - sker i enlighet med lagen; och
  - har ett berättigat syfte; och
  - är nödvändig i ett demokratiskt samhälle för att uppnå det berättigade syftet.

I EU-lagstiftningen och Europarådets lagstiftning är principen om behandling på ett korrekt och lagligt sätt den första princip som nämns. Den uttrycks i nästan exakt samma termer i artikel 5 i konvention 108 och i artikel 6 i dataskyddsdirektivet.

Ingen av dessa bestämmelser innehåller någon definition av vad som utgör ”tillåten behandling”. För att förstå denna juridiska term är det nödvändigt att hänvisa till berättigat ingripande enligt Europakonventionen såsom den tolkas i Europadomstolens rättspraxis och villkoren för tillåtna begränsningar enligt artikel 52 i stadgan.

3.1.1. Kraven på berättigat ingripande enligt Europakonventionen

Behandling av personuppgifter kan utgöra ett ingripande i rätten till respekt för den registrerades privatliv. Rätten till respekt för privatlivet är emellertid inte en absolut rättighet utan måste vägas mot och förenas med andra berättigade intressen, vare sig det handlar om andra personer (privata intressen) eller samhället som helhet (offentligt intresse).

Statligt ingripande är motiverat i följande fall.

I enlighet med lagen

Enligt Europadomstolens rättspraxis är ingripande förenligt med lagen om det baseras på en bestämmelse i inhemsk lag som har viss beskaffenhet. Lagen måste vara ”tillgänglig för de berörda personerna och förutsebar när det gäller dess effekter”.[108] En regel är förutsebar ”om den formuleras med tillräcklig precision för att göra det möjligt för alla enskilda – vid behov tillsammans med lämpliga råd – att reglera sitt

108 Europadomstolen, *Amann mot Schweiz* [GC], nr 27798/95, 16 februari 2000, punkt. 50, se även Europadomstolen, *Kopp mot Schweiz*, nr 23224/94, 25 mars 1998, punkt 55 och EU-domstolen, *Iordachi m.fl. mot Moldavien*, nr 25198/02, 10 februari 2009, punkt 50.

uppträdande".[109] "Graden av precision som krävs i 'lagen' i detta sammanhang beror på det enskilda ämnet."[110]

Exempel: I målet *Rotaru mot Rumänien*[111] ansåg Europadomstolen att artikel 8 hade överträtts eftersom den rumänska lagen medgav insamling, registrering och arkivering i hemliga arkiv av information som berör nationell säkerhet utan att fastställa gränser för utövandet av denna befogenhet, som fortfarande låg hos myndigheterna. Exempelvis fastställdes inte i den inhemska lagen typen av information som kunde behandlas, de kategorier människor mot vilka övervakningsåtgärder kunde vidtas, de omständigheter under vilka dessa åtgärder kunde vidtas eller vilket förfarande som skulle tillämpas. På grund av dessa brister drog domstolen slutsatsen att inhemsk lag inte uppfyllde kraven på förutsebarhet i artikel 8 i Europakonventionen och att denna artikel därför hade överträtts.

Exempel: I målet *Taylor-Sabori mot Förenade kungariket*[112] hade den klagande varit övervakad av polisen. Genom att använda en "klon" av den klagandes personsökare hade polisen kunnat avlyssna meddelanden som sändes till honom. Den klagande arresterades sedan och anklagades för konspiration för att leverera en kontrollerad drog. Delar av åklagarens mål mot honom bestod av de samtida skriftliga anteckningarna av personsökarens meddelanden som polisen hade transkriberat. Emellertid fanns vid tiden för den klagandes rättegång ingen bestämmelse i brittisk lag som reglerade avlyssning av kommunikationer som förmedlades via ett privat telekommunikationssystem. Intrånget i hans rättigheter hade därför inte skett "i enlighet med lagen". Europadomstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

109 Europadomstolen, *Amann mot Schweiz* [GC], nr 27798/95, 16 februari 2000, punkt 56, se även Europadomstolen, *Malone mot Förenade kungariket*, nr 8691/79, 2 augusti 1984, punkt 66, Europadomstolen, *Silver m.fl. mot Förenade kungariket*, nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, punkt 88.

110 Europadomstolen, *Sunday Times mot Förenade kungariket*, nr 6538/74, 26 april 1979, punkt 49, se även Europadomstolen, *Silver m.fl. mot Förenade kungariket*, nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, punkt 88.

111 Europadomstolen, *Rotaru mot Rumänien* [GC], nr 28341/95, 4 maj 2000, punkt 57, se även Europadomstolen, *Association for European Integration and Human Rights och Ekimdzhiev mot Bulgarien*, nr 62540/00, 28 juni 2007, Europadomstolen, *Shimovolos mot Ryssland*, nr 30194/09, 21 juni 2011, och Europadomstolen, *Vetter mot Frankrike*, nr 59842/00, 31 maj 2005.

112 Europadomstolen, *Taylor-Sabori mot Förenade kungariket*, nr 47114/99, 22 oktober 2002.

Utövande av berättigat syfte

Det berättigade syftet kan antingen vara ett av de nämnda allmänna intressena eller andra personers rättigheter och friheter.

Exempel: I målet *Peck mot Förenade kungariket*[113] försökte den klagande begå självmord på gatan genom att skära upp sina handleder, men var omedveten om att en övervakningskamera hade filmat honom under försöket. Efter att polisen, som hade tittat på övervakningskameran, hade räddat honom överlämnade polismyndigheten övervakningskamerans film till media som publicerade den utan att dölja den klagandes ansikte. Europadomstolen ansåg att det inte fanns några relevanta eller tillräckliga skäl för att direkt överlämna filmen från myndigheterna till allmänheten utan att ha erhållit den klagandes samtycke eller ha dolt hans identitet. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Nödvändigt i ett demokratiskt samhälle

Europadomstolen har slagit fast att ”begreppet nödvändighet innebär att intrång motsvarar ett trängande socialt behov och framför allt att det är proportionerligt mot det eftersträvade berättigade syftet”.[114]

Exempel: I målet *Khelili mot Schweiz*[115] upptäckte polisen under en poliskontroll att den klagande bar på kort med texten: ”Trevlig, snygg kvinna, drygt 30 år, vill träffa en man för gemensam drink eller för att gå ut då och då. Tfn [...]”. Den klagande påstod att polisen efter upptäckten skrivit in hennes namn i sina register som prostituerad, en sysselsättning som hon konsekvent förnekade. Den klagande krävde att ordet prostituerad skulle strykas från polisens dataregister. Europadomstolen erkände i princip att lagring av en persons personuppgifter på grund av att personen eventuellt begår ett annat brott under vissa förhållanden kan vara proportionerligt. I den klagandes fall föreföll emellertid påståendet om otillåten prostitution alltför vagt och allmänt, det stöddes inte av konkreta fakta eftersom hon aldrig hade dömts för olaglig prostitution, och kunde därför inte anses uppfylla ”tvingande sociala hänsyn” i den mening som avses i artikel 8 i

113 Europadomstolen, *Peck mot Förenade kungariket*, nr 44647/98, 28 januari 2003, särskilt punkt 85.

114 Europadomstolen, *Leander mot Sverige*, nr 9248/81, 26 mars 1987, punkt 58.

115 Europadomstolen, *Khelili mot Schweiz*, nr 16188/07, 18 oktober 2011.

Europakonventionen. Domstolen ansåg att myndigheterna måste bevisa att de uppgifter som lagrats om den klagande var korrekta, och med tanke på det allvarliga intrånget i den klagandes rättigheter beslutade den att registreringen av ordet ”prostituerad” i polisregistret under fyra år inte hade varit nödvändigt i ett demokratiskt samhälle. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Exempel: I målet *Leander mot Sverige*[116] beslutade Europadomstolen att hemlig kontroll av personer som söker tjänster som är viktiga för den nationella säkerheten inte i sig själv stred mot kravet på att vara nödvändigt i ett demokratiskt samhälle. De särskilda garantierna i nationell lagstiftning för att skydda den registrerades intressen – exempelvis kontroller som utövas av parlamentet och justitiekanslern – ledde till att Europadomstolen drog slutsatsen att det svenska systemet för kontroll av personal uppfyllde kraven i artikel 8.2 i Europakonventionen. Med beaktande av det omfattande manöverutrymmet kunde den svarande staten anse att i den klagandes fall hade nationella säkerhetsintressen företräde före den enskilda personens intresse. Domstolen drog slutsatsen att artikel 8 i Europakonventionen inte hade överträtts.

3.1.2. Förutsättning för tillåtna begränsningar enligt EU:s stadga

Strukturen och lydelsen i stadgan skiljer sig från den i Europakonventionen. I stadgan talas inte om intrång i garanterade rättigheter utan den innehåller bestämmelser om begränsningar i utövandet av de rättigheter och friheter som medges i stadgan.

Enligt artikel 5.2 är begränsningar i utövandet av rättigheter och friheter som medges i stadgan och, därmed, i utövandet av rätten till skydd av personuppgifter, exempelvis behandling av personuppgifter, tillåtna endast om de:

- föreskrivs i lagen;
- respekterar den centrala i rätten till uppgiftsskydd;
- är nödvändiga med tanke på proportionalitetsprincipen; och

116 Europadomstolen, *Leander mot Sverige*, nr 9248/81, 26 mars 1987, punkterna 59 och 67.

- uppfyller målsättningarna med allmänt intresse som medges av unionen eller behovet att skydda andras rättigheter och friheter.

Exempel: I målet *Volker och Markus Schecke*[117] drog EU-domstolen slutsatsen att genom att införa en skyldighet att offentliggöra personuppgifter rörande alla fysiska personer som erhöll hjälp från [vissa jordbruksfonder] utan att göra någon skillnad baserad på relevanta kriterier såsom perioder under vilka dessa personer erhöll hjälpen, hur ofta de fick hjälp eller arten eller beloppet, hade rådet och kommissionen överträtt gränserna enligt proportionalitetsprincipen.

EU-domstolen ansåg det därför nödvändigt att förklara vissa bestämmelser ogiltiga i rådets förordning (EG) nr 1290/2005 och förklara förordning nr 259/2008 ogiltig i sin helhet.[118]

Trots de olika lydelserna påminner villkoren för tillåten behandling i artikel 52.1 i stadgan om artikel 8.2 i Europakonventionen. De villkor som anges i artikel 52.1 i stadgan måste definitivt anses överensstämma med de som anges i artikel 8.2 i Europakonventionen, eftersom det i stadgans artikel 52.3, första meningen, slås fast att ”i den mån som denna stadga omfattar rättigheter som motsvarar sådana som garanteras av europeiska konventionen om skydd för de mänskliga rättigheterna och grundläggande friheterna ska de ha samma innebörd och räckvidd som i konventionen.”

I den sista meningen i artikel 52.3 står emellertid att ”denna bestämmelse hindrar inte unionsrätten från att tillförsäkra ett mer långtgående skydd”. En jämförelse av artikel 8.2 i Europakonventionen och första meningen i artikel 52.3 kan endast innebära att villkoren för berättigat ingripande enligt artikel 8.2 i Europakonventionen är minimikravet för tillåtna begränsningar av rätten till uppgiftsskydd enligt stadgan. Tillåten behandling av personuppgifter kräver därför enligt EU:s lagstiftning att villkoren i artikel 8.2 i Europakonventionen minst är uppfyllda. Ytterligare krav kan emellertid fastställas i EU:s lagstiftning för särskilda fall.

117 EU-domstolen, förenade målen C-92/09 och C-93/09, *Volker und Markus Schecke GbR och Hartmut Eifert mot Land Hessen*, 9 november 2010, punkt 89 och 86.

118 Rådets förordning (EG) nr 1290/2005 av den 21 juni 2005 om finansieringen av den gemensamma jordbrukspolitiken, EUT 2005 L 209 Kommissionens förordning (EG) nr 259/2008 av den 18 mars 2008 om tillämpningsföreskrifter för rådets förordning (EG) nr 1290/2005 när det gäller offentliggörande av uppgifter om de stödmottagare som får stöd från Europeiska garantifonden för jordbruket (EGFJ) och Europeiska jordbruksfonden för landsbygdsutveckling (EJFLU), EUT 2008 L 76.

Överensstämmelse mellan principen om tillåten behandling enligt EU:s lagstiftning och relevanta bestämmelser i Europakonventionen främjas ytterligare genom artikel 6.3 i EU-fördraget där det föreskrivs att ”de grundläggande rättigheterna, såsom de garanteras i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna […], ska ingå i unionsrätten som allmänna principer”.

3.2. Principen om specifikation och begränsning av syftet

Viktiga punkter

- Syftet med behandlingen av uppgifter måste vara tydligt definierat innan behandlingen inleds.
- Enligt EU:s lagstiftning måste syftet med behandling definieras uttryckligen, enligt Europarådets lagstiftning hör frågan till inhemsk lagstiftning.
- Behandling för odefinierade syften är inte förenligt med dataskyddslagstiftningen.
- Ytterligare användning av uppgifter för ett annat syfte kräver ytterligare en rättslig grund om det nya syftet med behandlingen är oförenligt med det ursprungliga.
- Överföring av uppgifter till tredje part är ett nytt syfte som kräver ytterligare rättslig grund.

I grund och botten innebär principen med specifikation och begränsning av syftet att berättigandet i behandlingen av personuppgifter beror på syftet med behandlingen.[119] Syftet måste ha specificerats och gjorts uppenbart av den registeransvariga innan behandlingen av uppgifter inleds.[120] **Enligt EU:s lagstiftning** måste detta ske antingen genom förklaring, med andra ord genom anmälan, till lämplig tillsynsmyndighet eller åtminstone genom intern dokumentation som måste göras tillgänglig av den registeransvariga för tillsynsmyndigheternas inspektion och den registrerades tillträde.

119 Konvention 108, artikel 5 b, dataskyddsdirektivet, artikel 6.1 b.

120 Se även artikel 29-gruppen (2013), Yttrande 03/2013 om begränsning av syftet, WP 203, Bryssel, 2 april 2013.

Behandling av personuppgifter för odefinierade och/eller obegränsade syften är inte tillåtet.

Varje nytt syfte för att behandla uppgifter måste ha sin egen särskilda rättsliga grund och kan inte baseras på att uppgifterna inledningsvis förvärvades eller behandlades för att annat berättigat syfte. Berättigad behandling är i sin tur begränsad till det ursprungligen angivna syftet och varje nytt syfte för behandling kommer att kräva en separat ny rättslig grund. Överlämning av uppgifter till tredje part måste övervägas extra noga, eftersom det vanligtvis utgör ett nytt syfte och därför kräver en rättslig grund som skiljer sig från den som behövs för att samla in uppgifter.

Exempel: Ett flygbolag samlar in uppgifter från sina passagerare för att göra bokningar så att flygningen kan genomföras korrekt. Flygbolaget behöver uppgifter om passagerarnas stolsnummer, särskilda fysiska begränsningar, exempelvis behov av rullstol och särskilda krav när det gäller mat såsom kosher eller halal. Om flygbolagen ombeds att överföra dessa uppgifter som finns i PNR till invandrarmyndigheterna vid landningen, används uppgifterna för invandringskontroll, vilket skiljer sig från det ursprungliga syftet med insamlingen. Överföringen av uppgifterna till en invandrarmyndighet kommer därför att kräva en ny och separat rättslig grund.

Vid beaktande av omfattningen och begränsningarna av ett särskilt syfte används i konvention 108 och dataskyddsdirektivet begreppet förenlighet: användningen av uppgifterna för förenliga syften är tillåtet utifrån den ursprungliga rättsliga grunden. Vad ”förenlighet” innebär definieras emellertid inte utan lämnas öppet för tolkning från fall till fall.

Exempel: En försäljning av företaget Sunshines kunduppgifter, som förvärvats genom kundrelationshanteringen (Customer Relationship Management, CRM), till ett direktmarknadsföringsföretag, Moonlight, som vill använda uppgifterna för att bistå tredjepartsföretags marknadsföringskampanjer, utgör ett nytt syfte, vilket inte är förenligt med CRM, dvs. företaget Sunshines ursprungliga syfte för att samla in kunduppgifterna. Försäljningen av uppgifterna till företaget Moonlight behöver därför en egen rättslig grund.

Företaget Sunshines användning av CRM-uppgifter för egna marknadsföringssyften, det vill säga skicka marknadsföringsmeddelanden till sina egna kunder

om de egna produkterna, är däremot i allmänhet accepterat som ett förenligt syfte.

I dataskyddsdirektivet står uttryckligen att ”senare behandling av uppgifter för historiska, statistiska eller vetenskapliga ändamål skall inte anses oförenlig med dessa ändamål förutsatt att medlemsstaterna beslutar om lämpliga skyddsåtgärder”.[121]

Exempel: Företaget Sunshine har samlat in och lagrat CRM-uppgifter om sina kunder. Ytterligare användning av dessa uppgifter från Sunshines sida för statistiska analyser av kundernas köpbeteende är tillåtet eftersom statistik är ett förenligt syfte. Det krävs ingen ytterligare rättslig grund, såsom samtycke från de registrerade.

Om samma uppgifter skulle överlämnas till en tredje part, företaget Starlight, för enbart statistiska syften, skulle överlämnandet vara tillåtet utan ytterligare rättslig grund, men endast under förutsättning att lämpliga garantier fanns, såsom att dölja de registrerades identitet, eftersom identitet vanligtvis inte krävs för statistiska syften.

3.3. Principer för uppgiftskvalitet

Viktiga punkter

- Principerna för uppgiftskvalitet måste genomföras av den registeransvariga vid all behandling av uppgifter.
- Principen om begränsad lagring av uppgifter gör det nödvändigt att radera uppgifter så snart de inte längre behövs för det syfte de samlades in för.
- Undantag från principen om begränsad lagring måste anges i lagen och behöver särskilda garantier för skydd av de registrerade.

121 Ett exempel på sådana nationella bestämmelser är den österrikiska lagen om dataskydd (*Datenschutzgesetz*), Fed. Law Gazette I nr 165/1999, punkt 46, tillgänglig på engelska på: www.dsk.gv.at/DocView.axd?CobId=41936.

3.3.1. Principen om uppgifternas relevans

Endast sådana uppgifter ska behandlas som är ”adekvata och relevanta och inte omfattar mer än vad som är nödvändigt med hänsyn till de ändamål för vilka de har samlats in och för vilka de senare behandlas”.[122] De kategorier uppgifter som väljs ut för behandling måste vara nödvändiga för att uppnå det angivna övergripande syftet med behandlingen, och en registeransvarig bör strikt begränsa insamlingen av uppgifter till sådan information som är direkt relevant för behandlingens specifika syfte.

I det moderna samhället måste principen om uppgifternas relevans beaktas ytterligare: genom att använda särskild teknik som är integritetsfrämjande är det ibland möjligt att undvika att använda personuppgifter överhuvudtaget, eller att använda pseudonymiserade uppgifter, vilket är en integritetsvänlig lösning. Detta är särskilt lämpligt i mer omfattande system för behandling av uppgifter.

Exempel: Kommunen i en stad erbjuder mot en viss avgift ett kort med chip för dem som regelbundet använder stadens kollektivtrafik. På kortets yta står användarens namn skrivet och det ingår även i elektronisk form i chipet. När användaren reser med buss eller spårvagn måste kortet hållas framför den läsare som finns i bussar och spårvagnar. De uppgifter som avläsningsutrustningen läser kontrolleras elektroniskt mot en databas som innehåller namnen på de personer som har köpt kortet.

Systemet ansluter sig inte till principen om relevans på ett optimalt sätt: att kontrollera om en person har rätt att använda transportmedel kan ske utan att jämföra personuppgifter på kortets chip med en databas. Det skulle exempelvis räcka med att ha en särskild elektronisk bild, såsom en streckkod, i kortets chip som när det hålls mot avläsningsutrustningen bekräftar om kortet är giltigt eller ej. Ett sådant kort skulle inte registrera vem som använder vilket transportsätt vid vilket tillfälle. Inga personuppgifter skulle samlas in, vilket är den optimala lösningen enligt principen om relevans, eftersom den resulterar i skyldigheten att minimera insamlingen av uppgifter.

122 Konvention 108, artikel 5 c och dataskyddsdirektivet, artikel 6.1 c.

3.3.2. Principen om uppgifternas korrekthet

En registeransvarig som innehar personlig information ska inte använda informationen utan att vidta åtgärder för att med rimlig visshet säkerställa att uppgifterna är korrekta och aktuella.

Skyldigheten att säkerställa uppgifternas korrekthet måste ses mot bakgrund av syftet med behandlingen av uppgifterna.

Exempel: Ett företag som säljer möbler registrerade en kunds identitet och adressuppgifter för att fakturera honom eller henne. Sex månader senare vill företaget inleda en marknadsföringskampanj och vill kontakta tidigare kunder. För att nå dem vill företaget få tillgång till det nationella bostadsregistret, som sannolikt innehåller aktuella adresser, eftersom de boende enligt lag är skyldiga att anmäla sin nuvarande adress till registret. Tillgång till uppgifter från registret är begränsad till personer och enheter som kan lämna ett motiverat skäl.

I denna situation kan företaget inte använda argumentet att uppgifterna måste hållas korrekta och aktuella för att hävda att det har rätt att samla in nya adressuppgifter om sina tidigare kunder från bostadsregistret. Uppgifterna samlades in i samband med fakturering och för det syfte är adressen vid tiden för försäljningen relevant. Det finns ingen rättslig grund för att samla in nya adressuppgifter, eftersom marknadsföringen inte är ett intresse som åsidosätter rätten till dataskydd och därför inte kan motivera tillgång till registrets uppgifter.

Det kan också finnas fall där uppdatering av lagrade uppgifter är förbjudna enligt lag eftersom syftet med att lagra uppgifterna principiellt är att dokumentera händelser.

Exempel: En redogörelse av en medicinsk operation får inte ändras, med andra ord ”uppdateras”, även om resultat som nämns i redogörelsen senare visar sig ha varit felaktiga. Under dessa förhållanden kan endast tillägg till kommentarerna i redogörelsen göras, så länge det markeras tydligt att de lagts till i efterhand.

Å andra sidan finns det situationer när regelbunden kontroll av uppgifternas korrekthet, inklusive uppdatering, är absolut nödvändigt på grund av den eventuella skada som kan drabba den registrerade om uppgifterna fortsatte att vara felaktiga.

Exempel: Om någon vill sluta ett avtal med en bankinstitution kontrollerar banken vanligtvis den framtida kundens kreditvärdighet. För detta syfte finns särskilda databaser som innehåller uppgifter om privatpersoners kredithistoria. Om en sådan databas innehåller felaktiga eller gamla uppgifter om en person kan han eller hon få allvarliga problem. Registeransvariga för dessa databaser måste därför särskilt anstränga sig för att följa principen om korrekthet.

Ytterligare uppgifter som rör fakta och inte misstankar, exempelvis brottsutredningar, kan samlas in och lagras under förutsättning att den registeransvariga har en rättslig grund för att samla in informationen och är tillräckligt motiverad när det gäller en sådan misstanke.

3.3.3. Principen om begränsad lagring av uppgifter

I artikel 6.1 e i dataskyddsdirektivet och även i artikel 5 e i konvention 108 uppmanas medlemsstaterna att se till att personuppgifter ”förvaras på ett sätt som förhindrar identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna samlades in eller för vilka de senare behandlades.” Uppgifterna måste därför raderas när dessa syften har uppnåtts.

I målet S. och Marper drog Europadomstolen slutsatsen att huvudprinciperna i Europarådets relevanta instrument och lag och praxis från andra avtalsparter krävde att lagringen av uppgifter skulle vara proportionerlig mot syftet med insamlingen och begränsad i tid, särskilt inom polissektorn.[123]

Tidsbegränsningen för att lagra personuppgifter gäller emellertid endast uppgifter som lagras i en form som möjliggör identifiering av de registrerade. Tillåten lagring av uppgifter som inte längre behövs kan därför åstadkommas genom anonymisering eller pseudonymisering av uppgifterna.

Att spara uppgifter för framtida vetenskaplig, historisk eller statistisk användning är uttryckligen undantaget från principen om begränsad lagring av uppgifter i dataskyddsdirektivet.[124] Sådan fortsatt lagring och användning av personuppgifter måste emellertid åtföljas av särskilda garantier enligt nationell lag.

123 Europadomstolen, *S. och Marper mot Förenade kungariket*, nr 30562/04 och 30566/04, 4 december 2008, se även exempelvis Europadomstolen, *M.M. mot Förenade kungariket*, nr 24029/07, 13 november 2012.

124 Dataskyddsdirektivet, artikel 6.1 e.

3.4. Principen om rättvis behandling

Viktiga punkter

- Rättvis behandling innebär öppen behandling, särskilt gentemot de registrerade.
- De registeransvariga måste informera de registrerade innan deras uppgifter behandlas, åtminstone om syftet med behandlingen och om den registeransvarigas identitet och adress.
- Om det inte uttryckligen är tillåtet enligt lag får ingen hemlig eller förtäckt behandling av personuppgifter förekomma.
- De registrerade har rätt att få tillgång till sina uppgifter oavsett var de behandlas.

Principen om rättvis behandling styr i första hand förhållandet mellan den registeransvariga och den registrerade.

3.4.1. Öppenhet

Genom principen införs en skyldighet för den registeransvariga att hålla de registrerade informerade om hur deras uppgifter används.

Exempel: I målet *Haralambie mot Rumänien*[125] begärde den klagande tillgång till den akt som säkerhetstjänsten hade lagrat om honom, men hans begäran beviljades först fem år senare. Europadomstolen upprepade att enskilda som var föremål för personliga akter som innehas av offentliga myndigheter hade ett väsentligt intresse av att kunna få tillgång till dem. Myndigheterna var skyldiga att erbjuda ett effektivt förfarande för att få tillgång till informationen. Europadomstolen ansåg att varken mängden överförda akter eller bristerna i arkiveringssystemet motiverade en försening på fem år när det gäller att bevilja den klagandes begäran om tillgång till sina akter. Myndigheterna hade inte erbjudit den klagande något effektivt och tillgängligt förfarande för att göra det möjligt för honom att få tillgång till sina personliga akter inom rimlig tid. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Behandlingen av uppgifter måste förklaras för de registrerade på ett lättåtkomligt sätt som innebär att de förstår vad som kommer att hända med deras uppgifter.

125 Europadomstolen, *Haralambie mot Rumänien*, nr 21737/03, 27 oktober 2009.

Den registrerade har också rätt att på begäran få veta av den registeransvariga om hans eller hennes uppgifter behandlas och i så fall vilka.

3.4.2. Att skapa tillit

De registeransvariga ska dokumentera för de registrerade och för allmänheten att de kommer att behandla uppgifter på ett tillåtet och öppet sätt. Behandlingen får inte ske i hemlighet och bör inte få oförutsebara negativa effekter. De registeransvariga bör se till att kunder, klienter eller medborgare informeras om att deras uppgifter används. De registeransvariga måste dessutom så långt det är möjligt agera på ett sätt som omgående överensstämmer med den registrerades önskemål, särskilt om hans eller hennes samtycke utgör den rättsliga grunden för behandlingen av uppgifterna.

Exempel: I målet *K.H. m.fl. mot Slovakien*[126] var de klagande åtta kvinnor av romskt ursprung som hade behandlats i två sjukhus i östra Slovakien under graviditet och förlossning. Därefter kunde ingen av dem bli gravid igen, trots upprepade försök. De nationella domstolarna ålade sjukhusen att låta de klagande och deras representanter läsa och göra avskrifter av journalerna, men avslog deras begäran att fotokopiera handlingarna efter vad som uppgavs i syfte att förhindra missbruk. Statens positiva skyldigheter enligt artikel 8 i Europakonventionen innefattar definitivt en skyldighet att göra kopior av datafiler tillgängliga för de registrerade. Det var statens uppgift att fastställa arrangemangen för att kopiera filer med personuppgifter eller i förekommande fall lämna övertygande skäl till att vägra att göra det. I de klagandes fall motiverade de inhemska domstolarna förbudet mot att göra kopior av medicinska journaler med behovet att skydda relevant information från att missbrukas. Europadomstolen kunde emellertid inte se hur de klagande, som i vilket fall som helst hade fått tillgång till sina medicinska journaler i sin helhet, skulle ha kunnat missbruka information som gällde dem själva. Risken för sådant missbruk kunde dessutom ha förebyggts på andra sätt än genom att vägra de klagande kopiering av filerna, exempelvis genom att begränsa antalet personer som har rätt att få tillgång till filerna. Staten lyckades inte visa på förekomsten av tillräckligt övertygande skäl till att neka de klagande faktisk tillgång till information om deras hälsa. Domstolen drog därför slutsatsen att artikel 8 i Europakonventionen hade överträtts.

126 Europadomstolen, *K.H. m.fl. mot Slovakien*, nr 32881/04, 28 april 2009.

När det gäller internettjänster måste databehandlingssystemens egenskaper göra det möjligt för de registrerade att verkligen förstå vad som händer med deras uppgifter.

Rättvis behandling innebär också att registeransvariga är beredda att gå längre än de obligatoriska rättsliga minimikraven för tjänster till den registrerade, om dennas berättigade intressen skulle kräva det.

3.5. Principen om ansvarighet

Viktiga punkter

- Ansvarighet kräver aktivt genomförande av åtgärder av registeransvariga för att främja och garantera skydd av uppgifterna vid behandling.
- De registeransvariga är ansvariga för att deras behandling överensstämmer med lagstiftningen om uppgiftsskydd.
- De registeransvariga ska när som helst kunna visa de registrerade, allmänheten och tillsynsmyndigheter att de uppfyller bestämmelserna om skydd av personuppgifter.

Organisationen för ekonomiskt samarbete och utveckling (OECD) antog riktlinjer för skydd av privatlivet 2013 som visade att de registeransvariga spelar en viktig roll när det gäller att få skyddet av personuppgifter att fungera i praktiken. Riktlinjerna innehåller en princip om ansvarighet som innebär att en registeransvarig ska vara ansvarig för att utföra åtgärder som verkställer [de avgörande] principerna ovan.[127]

Medan konvention 108 inte innehåller någon hänvisning till de registeransvarigas ansvarighet, och huvudsakligen överlåter det till inhemsk lagstiftning, anges i artikel 6.2 i dataskyddsdirektivet att den registeransvariga ska se till att principerna om uppgiftskvalitet i punkt 1 efterlevs.

127 OECD (2013), *Guidelines on governing the Protection of Privacy and Transborder Flows of Personal Data* (riktlinjer för skydd av privatlivet och gränsöverskridande flöden av personuppgifter), artikel 14.

Exempel: Ett exempel från lagstiftningen för att betona principen om ansvarighet är ändringen från 2009[128] i direktivet om integritet och elektronisk kommunikation 2002/58/EG. Enligt artikel 4 i dess ändrade form införs genom direktivet en skyldighet att införa en säkerhetspolicy som innebär att säkerställa införlivandet av en säkerhetspolicy vad gäller behandlingen av personuppgifter. När det gäller säkerhetsbestämmelserna i det direktivet beslutade lagstiftaren alltså att det var nödvändigt att införa ett uttryckligt krav på att ha och införliva en säkerhetspolicy.

Enligt artikel 29-gruppens uppfattning[129] är det viktigaste när det gäller ansvarighet den registeransvarigas skyldighet att:

- införa åtgärder som – under normala förhållanden – garanterar att regler för skydd av personuppgifter respekteras vid behandling av uppgifter; och

- ha dokumentation beredd som visar för de registrerade och för tillsynsmyndigheter vilka åtgärder som har vidtagits för att reglerna för uppgiftsskydd ska kunna följas.

Principen om ansvarsskyldighet kräver därför att de registeransvariga aktivt visar att reglerna följs och inte endast väntar på att de registrerade eller tillsynsmyndigheterna visar på brister.

128 Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbete mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen, EUT 2009 L 337, s. 11.

129 Artikel 29-gruppen, *Yttrande 3/2010 om principen om ansvarsskyldighet*, WP 173, Bryssel, 13 juli 2011.

4

Bestämmelser i den europeiska lagstiftningen om skydd av personuppgifter

EU	Frågor som täcks	Europarådet
Bestämmelser om tillåten behandling av icke känsliga uppgifter		
Dataskyddsdirektivet, artikel 7 a	Samtycke	Rekommendation om profilering, artikel 3.4 b och 3.6
Dataskyddsdirektivet, artikel 7 b	Relation före avtal	Rekommendation om profilering, artikel 3.4 b
Dataskyddsdirektivet, artikel 7 c	Den registeransvarigas juridiska skyldigheter	Rekommendation om profilering, artikel 3.4 a
Dataskyddsdirektivet, artikel 7 d	Den registrerades avgörande intressen	Rekommendation om profilering, artikel 3.4 b
Dataskyddsdirektivet, artikel 7 e och artikel 8.4 EU-domstolen, C-524/06, *Huber mot Bundesrepublik Deutschland*, 16 december 2008	Offentligt intresse och utövande av officiellt mandat	Rekommendation om profilering, artikel 3.4 b
Dataskyddsdirektivet, artikel 7 f, artikel 8.2 och 8.3 EU-domstolen, förenade målen C-468/10 och C469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado*, 24 november 2011	Andras berättigade intressen	Rekommendation om profilering, artikel 3.4 b

EU	Frågor som täcks	Europarådet
Bestämmelser om tillåten behandling av känsliga uppgifter		
Dataskyddsdirektivet, artikel 8.1	Allmänt förbud mot behandling	Konvention 108, artikel 6
Dataskyddsdirektivet, artikel 8.2–8.4	Undantag från det allmänna förbudet	Konvention 108, artikel 6
Dataskyddsdirektivet, artikel 8.5	Behandling av uppgifter om (fällande) domar i brottmål	Konvention 108, artikel 6
Dataskyddsdirektivet, artikel 8.7	Behandling av id-nummer	
Bestämmelser om säker behandling		
Dataskyddsdirektivet, artikel 17	Skyldighet att åstadkomma säker behandling	Konvention 108, artikel 7
		Europadomstolen, *I. mot Finland*, nr 20511/03, 17 juli 2008
Direktiv om integritet och elektronisk kommunikation, Artikel 4.2	Anmälningar om överträdelse av uppgifter	
Dataskyddsdirektivet, artikel 16	Krav på sekretess	
Bestämmelser om öppenhet vid behandling		
	Öppenhet i allmänhet	Konvention 108, artikel 8 a
Dataskyddsdirektivet, artiklarna 10 och 11	Information	Konvention 108, artikel 8 a
Dataskyddsdirektivet, artiklarna 10 och 11	Undantag från skyldigheten att informera	Konvention 108, artikel 9
Dataskyddsdirektivet, artiklarna 18 och 19	Anmälan	Rekommendation om profilering, artikel 9.2 a
Bestämmelser om främjande av överensstämmelse		
Dataskyddsdirektivet, artikel 20	Förhandskontroll	
Dataskyddsdirektivet, artikel 18.2	Uppgiftsskydds-ombud	Rekommendation om profilering, artikel 8.3
Dataskyddsdirektivet, artikel 27	Uppförandekoder	

Principerna är vanligtvis av allmänt slag. Deras tillämpning på konkreta situationer ger utrymme för ett visst tolkningsutrymme och val av medel. Enligt **Europarådets lagstiftning** får parterna till konvention 108 klargöra detta tolkningsutrymme

i sin inhemska lagstiftning. Situationen i **EU:s lagstiftning** är annorlunda: för fastställande av uppgiftsskydd på den inre marknaden ansågs det nödvändigt att ha mer detaljerade uppgifter redan på EU-nivå för att harmonisera nivån på uppgiftsskydd i medlemsstaternas nationella lagstiftning. I dataskyddsdirektivet fastställs, enligt principer som anges i artikel 6, en rad detaljerade bestämmelser som noga måste införlivas i nationell lag. Följande kommentarer om detaljerade bestämmelser om skydd av personuppgifter på europeisk nivå handlar därför huvudsakligen om EU-lagstiftning.

4.1. Bestämmelser om tillåten behandling

Viktiga punkter

- Personuppgifter kan behandlas lagligt om:
  - behandlingen bygger på samtycke från den registrerade; eller
  - den registrerades grundläggande intressen kräver behandling av dennas uppgifter; eller
  - andras berättigade intressen är skälet till behandlingen, men endast så länge de inte åsidosätts av intressen för att skydda de registrerades grundläggande rättigheter.
- Tillåten behandling av känsliga personuppgifter omfattas av särskilda striktare regler.

Dataskyddsdirektivet innehåller två olika uppsättningar bestämmelser om tillåten behandling av uppgifter: en för icke känsliga uppgifter i artikel 7 och en för känsliga uppgifter i artikel 8.

4.1.1. Tillåten behandling av icke känsliga uppgifter

I kapitel II i direktiv 95/46, med rubriken ”Allmänna bestämmelser om när personuppgifter får behandlas”, föreskrivs, beroende på undantagen som tillåts enligt artikel 13, att all behandling av personuppgifter måste överensstämma för det första med principerna rörande uppgiftskvalitet som anges i artikel 6 i dataskyddsdirektivet och för det andra med ett av kriterierna för att behandlingen av uppgifterna ska

vara berättigad, enligt artikel 7.[130] Detta förklarar fallen som berättigar behandling av icke-känsliga personuppgifter.

Samtycke

I **Europarådets lagstiftning** nämns inte samtycke i artikel 8 i Europakonventionen eller i konvention 108. Det nämns däremot i Europadomstolens rättspraxis och flera rekommendationer från Europarådet. **I EU:s lagstiftning** är samtycke tydligt fastställt som en grund för berättigad behandling av uppgifter genom artikel 7 a i dataskyddsdirektivet och det nämns också uttryckligen i artikel 8 i stadgan.

Avtalsmässig relation

En annan grund för berättigad behandling av personuppgifter **enligt EU:s lagstiftning**, som räknas upp i artikel 7 b i dataskyddsdirektivet, är om den är ”nödvändig för att fullgöra ett avtal i vilket den registrerade är part”. Bestämmelsen omfattar också relationer före avtalet. En part avser exempelvis att träffa ett avtal, men har ännu inte gjort det, sannolikt för att några kontroller fortfarande behöver göras. Om en part behöver behandla uppgifter för detta syfte är denna behandling berättigad så länge som det sker ”för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås”.

När det gäller Europarådets lagstiftning nämns ”skydd av andras rättigheter och friheter” i artikel 8.2 i Europakonventionen som ett skäl till berättigat ingripande i rätten till dataskydd.

Den registeransvarigas juridiska skyldigheter

I **EU-rätten** nämns sedan uttryckligen ett annat kriterium för att göra behandling av uppgifter berättigad, nämligen om ”behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige” (artikel 7 c i dataskyddsdirektivet). Bestämmelsen hänför sig till registeransvariga som verkar inom den privata sektorn. De juridiska skyldigheterna för registeransvariga inom den offentliga sektorn faller under artikel 7 e i direktivet. Det finns många fall där registeransvariga

130 EU-domstolen, förenade målen C-465/00, C-138/01 och C-139/01. *Rechnungshof mot Österreichischer Rundfunk m.fl* och Christa Neukomm och Joseph Lauermann mot Osterreichischer, 20 maj 2003, punkt 65, EU-domstolen, C-524/06, *Huber mot Bundesrepublik Deutschland*, 16 december 2008, punkt 48, EU-domstolen, förenade målen C-468/10 och C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado*, 24 november 2011, punkt 26.

inom den privata sektorn är skyldiga enligt lag att behandla uppgifter om andra. Exempelvis läkare och sjukhus har en juridisk skyldighet att lagra uppgifter om behandling av patienter under flera år, arbetsgivare måste behandla uppgifter om sina anställda som rör socialförsäkring och beskattning och företag måste behandla uppgifter om sina kunder av skatteskäl.

När det gäller den obligatoriska överföringen av passageraruppgifter från flygbolag till utländska myndigheter för invandringskontroll, uppstod frågan om huruvida juridiska skyldigheter enligt *utländsk* lag kunde utgöra en berättigad grund för att behandla uppgifter enligt EU-lagstiftningen (frågan diskuteras mer i detalj i avsnitt 6.2).

Den registeransvarigas juridiska skyldigheter fungerar som en rättslig grund för berättigad behandling av uppgifter även **enligt Europarådets lagstiftning.** Såsom påpekats tidigare är de juridiska skyldigheterna för en registeransvarig inom den privata sektorn bara ett specifikt fall av andras berättigade intressen, något som framgår i artikel 8.2 i Europakonventionen. Exemplet ovan är därför också relevant när det gäller Europarådets lagstiftning.

Intressen som är av grundläggande betydelse för den registrerade

I EU-lagstiftningen föreskrivs i artikel 7 d i dataskyddsdirektivet att behandlingen av personuppgifter är tillåten om den ”är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade”. Dessa intressen, som är nära förbundna med den registrerades överlevnad, kan ligga till grund för berättigad användning av hälsouppgifter eller uppgifter om försvunna personer, exempelvis.

När det gäller Europarådets lagstiftning nämns inte intressen som är av grundläggande betydelse för den registrerade i artikel 8.2 i Europakonventionen som ett skäl till berättigat ingripande i rätten till dataskydd. I vissa av Europarådets rekommendationer som kompletterar konvention 108 på vissa områden nämns emellertid intressen som är av avgörande betydelse för den registrerade som en grund för berättigad behandling av uppgifter.[131] Intressen som är av avgörande betydelse för den registrerade anses självklart ingå i de skäl som motiverar behandling av uppgifterna: skydd av grundläggande rättigheter bör aldrig äventyra de intressen som är av avgörande betydelse för den person som skyddas.

131 Rekommendation om profilering, artikel 3.4 b.

Allmänt intresse och utövande av myndighetsutövning

Med tanke på de många möjligheterna att organisera offentliga ärenden föreskrivs i artikel 7 e i dataskyddsdirektivet att behandling av personuppgifter kan tillåtas om den är ”nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den registeransvarige eller tredje man till vilken uppgifterna har lämnats ut […]”.[132]

Exempel: I målet *Huber mot Bundesrepublik Deutschland*[133] bad herr Huber, en österrikisk medborgare boende i Tyskland, det federala kontoret för migration och flyktingar att radera uppgifter om honom i det centrala registret över utländska medborgare (”AZR”). Registret som innehåller personuppgifter om EU-medborgare som inte är tyska medborgare men som bor i Tyskland mer än tre månader, används för statistiska syften av brottsbekämpande och rättsliga myndigheter vid utredning och åtal av brottslig verksamhet eller sådan som hotar den allmänna säkerheten. Den hänvisande domstolen frågade huruvida behandling av personuppgifter som genomförs i ett register såsom det centrala registret över utländska medborgare, som andra offentliga myndigheter också har tillgång till, är förenligt med EU:s lagstiftning, under förutsättning att inget sådant register finns för tyska medborgare.

EU-domstolen anser för det första att enligt artikel 7 e i direktivet får personuppgifter behandlas endast om det är nödvändigt för utförande av en uppgift som genomförs i allmänhetens intresse eller vid utövandet av ett officiellt bemyndigande.

Domstolen påpekar att ”med beaktande av målet att göra skyddsnivån likvärdig i alla medlemsstater kan begreppet nödvändighet såsom det följer av artikel 7 e i direktiv 95/46 […] således inte förstås olika från medlemsstat till medlemsstat. Det rör sig därmed om ett självständigt gemenskapsrättsligt begrepp som ska tolkas så, att det till fullo uppfyller syftet med detta direktiv, såsom det definieras i artikel 1.1”.[134]

Domstolen noterar att rätten till fri rörlighet för en unionsmedborgare på en medlemsstats territorium där han eller hon inte är medborgare inte är

132 Se även dataskyddsdirektivet, skäl 32.

133 EU-domstolen, C-524/06, *Huber mot Bundesrepublik Deutschland*, 16 december 2008.

134 *Ibid.*, punkt 52.

villkorslös, men kan omfattas av begränsningar och villkor enligt fördraget och av åtgärder som antagits för att det ska träda i kraft. Så om det i princip är berättigat för en medlemsstat att använda ett register som AZR för att stödja myndigheterna som är ansvariga för att tillämpa lagstiftningen rörande rätten till boende, får detta register inte innehålla någon annan information än vad som krävs för detta syfte. Domstolen drar slutsatsen att ett sådant system för att behandla personuppgifter överensstämmer med EU:s lagstiftning om det enbart innehåller de uppgifter som krävs för att tillämpa lagstiftningen och om dess centraliserade utformning gör att lagstiftningen kan tillämpas effektivare. Den nationella domstolen måste förvissa sig om huruvida dessa villkor är uppfyllda i detta särskilda fall. Om inte, kan inte lagring och behandling av personuppgifter i ett register som AZR för statistiska syften, på någon grund, anses som nödvändigt i den mening som avses i artikel 7 e i direktiv 95/46/EG.[135]

Avslutningsvis, vad gäller frågan om användning av uppgifter i registret för att bekämpa brott anser domstolen att denna kamp måste ”med nödvändighet föras mot brott och överträdelser oberoende av gärningsmännens nationalitet”. Registret i fråga innehåller inte personuppgifter rörande medborgare i de berörda medlemsstaterna och denna skillnad i behandling utgör en diskriminering som är förbjuden enligt artikel 18 i EUF-fördraget. Denna bestämmelse tolkas därför av domstolen som att ”den utgör hinder för att en medlemsstat inför ett särskilt system för behandling av personuppgifter avseende unionsmedborgare som inte är medborgare i denna medlemsstat i syfte att bekämpa kriminalitet.”[136]

Användningen av uppgifter vid myndigheter som agerar på den offentliga arenan omfattas också av artikel 8 i **Europakonventionen**.

Berättigade intressen som utövas av den registeransvariga eller av en tredje part

Den registrerade är inte den enda med berättigade intressen. I artikel 7 f i dataskyddsdirektivet föreskrivs att personuppgifter får behandlas om det är nödvändigt ”för ändamål som rör berättigade intressen hos den registeransvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut, utom när sådana intressen

135 *Ibid.*, punkterna 54, 58, 59 och 66–68.

136 *Ibid.*, punkterna 78 och 81.

uppvägs av den registrerades intressen eller dennes grundläggande fri- och rättigheter som kräver skydd […]".

I följande dom fattade domstolen beslut uttryckligen utifrån artikel 7 f i direktivet:

Exempel: I målen *ASNEF och FECEMD*[137] klargjorde EU-domstolen att det inte är tillåtet i nationell lagstiftning att lägga till villkor utöver dem som nämns i artikel 7 f i direktivet om tillåten behandling av uppgifter. Detta gällde en situation där den spanska lagstiftningen för uppgiftsskydd innehöll en bestämmelse genom vilken andra privata parter kan hävda ett berättigat intresse i att behandla personuppgifter endast om informationen redan har förekommit i offentliga källor.

Domstolen noterade först att direktiv 95/46 är avsett att se till att skyddsnivån för individers rättigheter och friheter när det gäller behandling av personuppgifter är densamma i alla medlemsstater. Inte heller behöver närmandet av de nationella lagarna som är tillämpliga på detta område resultera i någon minskning av det skydd de erbjuder. Det måste i stället eftersträva en hög nivå av skydd inom EU.[138] EU-domstolen ansåg därför att "det framgår följaktligen av ändamålet – säkerställandet av en likvärdig skyddsnivå i alla medlemsstater – att det i artikel 7 i direktiv 95/46 görs en uttömmande uppräkning av de situationer när en behandling av personuppgifter kan anses vara tillåten". Dessutom är det så att "medlemsstaterna varken får foga ytterligare principer för tillåtligheten av behandlingen av personuppgifter till dem som nämns i artikel 7 i direktiv 95/46 eller föreskriva ytterligare villkor som påverkar räckvidden av de sex principer som föreskrivs i nämnda artikel".[139] Domstolen medgav att "när det gäller den nödvändiga avvägningen enligt artikel 7 f i direktiv 95/46 är det möjligt att beakta det faktum att allvaret i kränkningen av den registrerades grundläggande rättigheter som nämnda behandling innebär kan variera beroende på om uppgifterna i fråga redan finns i källor tillgängliga för allmänheten".

137 EU-domstolen, förenade målen C-468/10 och C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado*, 24 november 2011.

138 *Ibid.*, punkt 28. Se dataskyddsdirektivet, skälen 8 och 10.

139 EU-domstolen, förenade målen C-468/10 och C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado*, 24 november 2011, punkterna 30 och 32.

Vidare föreslås att ”artikel 7 f i direktivet utgör följaktligen hinder för att en medlemsstat kategoriskt och generellt utesluter möjligheten att behandla vissa typer av personuppgifter, utan att tillåta en avvägning mellan de motstående rättigheterna och intressena i det enskilda fallet”.

Mot bakgrund av dessa överväganden drog domstolen slutsatsen att ”artikel 7 f i direktiv 95/46/EG ska tolkas på så sätt att den utgör hinder för nationell lagstiftning i vilken det – såsom villkor för behandling av personuppgifter som är nödvändig för att tillgodose berättigade intressen hos den registeransvarige eller hos den tredje man eller de tredje män till vilka uppgifterna ska lämnas ut, när den registrerade inte har lämnat sitt samtycke – föreskrivs, förutom att den registrerades grundläggande fri- och rättigheter inte får åsidosättas, att uppgifterna ska finnas i källor tillgängliga för allmänheten, vilket kategoriskt och generellt utesluter all behandling av uppgifter som inte finns i sådana källor”.[140]

Liknande formuleringar kan hittas i Europarådets rekommendationer. I rekommendationen om profilering erkänns behandlingen av personuppgifter i profileringssyfte som berättigade, vid behov för andras berättigade intressen, ”förutom när dessa intressen åsidosätts av de registrerades grundläggande rättigheter och friheter”.[141]

4.1.2. Tillåten behandling av känsliga uppgifter

Enligt Europarådets lagstiftning är det den inhemska lagstiftningens uppgift att fastställa lämpligt skydd för användning av känsliga uppgifter, medan **EU:s lagstiftning** i artikel 8 i dataskyddsdirektivet innehåller detaljerade bestämmelser om behandling av kategorier uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller information om hälsa eller sexualliv. Behandling av känsliga uppgifter är i princip förbjudet.[142] Det finns emellertid en omfattande förteckning över undantag från detta förbud i artikel 8.2 och 8.3 i direktivet. Dessa undantag innefattar uttryckligt samtycke från den registrerade, den registrerades grundläggande intressen, berättigade intressen hos andra och offentliga intressen.

Till skillnad från behandling av icke känsliga uppgifter ses ett avtalsförhållande med den registrerade inte som en allmän grund för berättigad behandling av känsliga

140 *Ibid.*, punkterna 40, 44, 48 och 49.

141 Rekommendation om profilering, artikel 3.4 b.

142 Dataskyddsdirektivet, artikel 8.1.

uppgifter. Om känsliga uppgifter ska behandlas i samband med ett avtal med den registrerade kräver därför användning av dessa uppgifter den registrerades separata uttryckliga samtycke, utöver att samtycka till att träffa avtalet. En uttrycklig begäran från den registrerade om varor eller tjänster som nödvändigtvis avslöjar känsliga uppgifter bör emellertid betraktas som likvärdig med ett uttryckligt samtycke.

Exempel: Om en flygpassagerare i samband med bokning av en flygning kräver att flygbolaget tillhandahåller en rullstol och koshermat har flygbolaget tillåtelse att använda dessa uppgifter även om passageraren inte undertecknade någon extra samtyckesklausul som innebär att han eller hon samtycker till att de uppgifter används som ger information om hans eller hennes hälsa eller religiösa övertygelse.

Den registrerades uttryckliga samtycke

Det första villkoret för tillåten behandling av alla uppgifter, oavsett om de är icke känsliga eller känsliga uppgifter, är att den registrerade ger sitt samtycke. Vid känsliga uppgifter måste detta samtycke vara uttryckligt. Nationell lag kan emellertid innebära att samtycke till användningen av känsliga uppgifter inte är en tillräcklig rättslig grund för att göra det möjligt att behandla dem[143], exempelvis när behandlingen i undantagsfall innefattar ovanliga risker för den registrerade.

I ett speciellt fall erkänns även underförstått samtycke som en rättslig grund för behandling av känsliga uppgifter: i artikel 8.2 e i direktivet föreskrivs att behandling inte är förbjuden om den gäller uppgifter som uppenbart har offentliggjorts av den registrerade. Denna bestämmelse förutsätter naturligtvis att den registrerades åtgärder för att göra hans eller hennes uppgifter offentliga måste tolkas som att de förutsätter den registrerades samtycke till användningen av dessa uppgifter.

Den registrerades grundläggande intressen

Som i fallet med icke känsliga uppgifter kan känsliga uppgifter behandlas på grund av den registrerades grundläggande intressen.[144]

143 *Ibid.,* artikel 8.2 a.

144 *Ibid.,* artikel 8.2 c.

För att behandling av känsliga uppgifter ska vara berättigad på denna grund måste det ha varit omöjligt att ställa frågan till den registrerade för beslut, på grund av att den registrerade exempelvis var medvetslös eller frånvarande och inte kunde nås.

Övrigas berättigade intressen

Som vid fallet med icke känsliga uppgifter kan andras berättigade intressen fungera som grund för behandling av känsliga uppgifter. För känsliga uppgifter, och enligt artikel 8.2 i dataskyddsdirektivet, gäller detta emellertid endast i följande fall:

- när behandling är nödvändig på grund av en annan persons grundläggande intressen[145] när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke;

- när känsliga uppgifter är relevanta på området anställningslagstiftning, såsom uppgifter om hälsa i samband med specifikt farliga arbetsplatser eller uppgifter om religiösa övertygelser, såsom i samband med helgdagar;[146]

- när stiftelser, föreningar eller andra icke vinstdrivande organ med ett politiskt, filosofiskt, religiöst eller fackligt syfte behandlar uppgifter om sina medlemmar eller sponsorer eller andra berörda parter (sådana uppgifter är känsliga eftersom de kan avslöja religiösa eller politiska övertygelser hos den berörda personen);[147]

- när känsliga uppgifter används i samband med rättsliga förhandlingar inför en domstol eller administrativ myndighet för att fastslå, göra gällande eller försvara rättsliga anspråk.[148]

- Enligt artikel 8.3 i dataskyddsdirektivet ingår, när uppgifter om hälsa används för medicinsk undersökning och behandling av vårdgivare, administration av dessa tjänster dessutom i undantaget. Som en särskild säkerhet erkänns personer som ”vårdgivare” endast om de omfattas av specifika yrkesmässiga skyldigheter när det gäller tystnadsplikt.

145 *Ibid.*

146 *Ibid.,* artikel 8.2 b.

147 *Ibid.,* artikel 8 2 d.

148 *Ibid.*, artikel 8.2 e.

Allmänt intresse

Enligt artikel 8.4 i dataskyddsdirektivet kan medlemsstaterna införa ytterligare syften för vilka känsliga uppgifter kan behandlas, så länge som:

- behandlingen av uppgifter sker på grund av ett viktigt allmänt intresse;
- det föreskrivs i nationell lag eller genom beslut av tillsynsmyndigheten; och
- den nationella lagen eller beslutet från tillsynsmyndigheten innehåller nödvändiga garantier för att effektivt skydda den registrerades intressen.[149]

Ett iögonfallande exempel är elektroniska journalsystem som håller på att införas i många medlemsstater. Systemen gör att hälsouppgifter, som samlats in av hälsovårdande leverantörer under behandling av en patient, kan göras tillgängliga för andra hälsovårdande leverantörer för denna patient i stor skala, vanligtvis i hela landet.

Artikel 29-gruppen drog slutsatsen att inrättandet av ett sådant system inte kunde ske enligt befintliga rättsliga regler för behandling av uppgifter om patienter, baserat på artikel 8.3 i dataskyddsdirektivet. Om man emellertid antar att förekomsten av ett sådant elektroniskt journalsystem utgör ett viktigt allmänt intresse kan det baseras på artikel 8.4 i direktivet och kräva en explicit rättslig grund för inrättandet, som också innehåller nödvändiga garantier för att säkerställa att systemet tillämpas säkert.[150]

4.2. Säkerhetsregler vid behandling

Viktiga punkter

- Reglerna för säker behandling inbegriper en skyldighet hos den registeransvariga och registerföraren att införa lämpliga tekniska och organisatoriska åtgärder i syfte att förebygga eventuellt otillåtet intrång i samband med uppgiftsbehandling.

149 *Ibid.*, artikel 8.4.

150 Artikel 29-gruppen (2007), *Arbetsdokument om behandling av hälsorelaterade personuppgifter i elektroniska patientjournaler (EPJ)*, WP 131, Bryssel, 15 februari 2007.

- Den nödvändiga nivån på dataskyddet fastställs av:
  - de säkerhetsinslag som är tillgängliga på marknaden för alla typer av behandling;
  - kostnaden;
  - känsligheten i de behandlade uppgifterna;
- Säker behandling av uppgifter garanteras ytterligare av den allmänna skyldigheten för alla personer, registeransvariga eller registerförare att se till att uppgifterna förblir konfidentiella.

Registeransvarigas och registerförares skyldighet att ha lämpliga åtgärder för att säkerställa säkerhet för uppgifterna ingår därför i både **Europarådets** och **EU:s dataskyddslagstiftning**.

4.2.1. Beståndsdelar i datasäkerhet

Enligt relevanta bestämmelser föreskrivs i **EU-lagstiftningen**:

> *"Medlemsstaterna skall föreskriva att den registeransvarige skall genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling".*[151]

En liknande bestämmelse finns i **Europarådets lagstiftning**:

> *"Lämpliga säkerhetsåtgärder skall vidtas för att skydda personuppgifter som lagras i automatiserade register gentemot oavsiktlig eller otillåten förstörelse eller oavsiktlig förlust liksom gentemot otillåten tillgång, ändring eller spridning."*[152]

Det finns ofta också industriella, nationella och internationella standarder som har utvecklats för säker behandling av uppgifter. European Privacy Seal (EuroPriSe), exempelvis, är ett eTEN-projekt (transeuropeiska telekommunikationsnät) inom EU som har undersökt möjligheterna att certifiera produkter, särskilt programvara, som överensstämmer med europeisk dataskyddslagstiftning. Europeiska unionens byrå för nät- och informationssäkerhet (ENISA) inrättades för att förbättra EU:s,

151 Dataskyddsdirektivet, artikel 17.1.

152 Konvention 108, artikel 7.

medlemsstaternas och företagens möjligheter förebygga, ta upp och bemöta säkerhetsproblem inom nätverk och information.[153] ENISA publicerar regelbundet analyser av aktuella säkerhetshot och råd om hur de ska hanteras.

Datasäkerhet uppnås inte enbart genom att ha rätt utrustning – hård- och mjukvara. Det krävs också lämpliga interna organisatoriska regler. Dessa interna regler bör under idealiska förhållanden omfatta följande ämnen:

- regelbundet tillhandahållande av information till samtliga anställda om datasäkerhetsregler och deras skyldigheter enligt dataskyddslagen, särskilt vad gäller skyldigheten till sekretess;

- tydlig uppdelning av ansvar och en tydlig sammanfattning av behörighet när det gäller behandling av uppgifter, särskilt vad gäller beslut att behandla personuppgifter och överföra uppgifter till tredje part;

- användning av personuppgifter endast enligt instruktionerna från den behöriga personen eller enligt allmänt fastställda regler;

- skydd för tillträde till platser och till hård- och mjukvara som tillhör den registrerade eller registeföraren, inbegripet kontroller av tillstånd för tillträde;

- säkerställande av att tillstånd för tillgång till personuppgifter har utfärdats av den behöriga personen och kräver korrekt dokumentation;

- automatiska protokoll för att få tillgång till personuppgifter på elektronisk väg och regelbundna kontroller av dessa protokoll utförda av den interna tillsynsavdelningen;

- noggrann dokumentation för andra former av spridning än automatisk tillgång till uppgifter för att kunna visa att inga olagliga överföringar har skett.

Att erbjuda lämplig utbildning inom datasäkerhet för personalen är också ett viktigt inslag i effektiva säkerhetsåtgärder. Kontrollförfaranden måste också införas för att säkerställa att lämpliga åtgärder inte enbart finns på papper utan genomförs och fungerar i praktiken (exempelvis intern eller extern revision).

153 Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet, EUT 2004, L 77.

Åtgärder för att förbättra säkerhetsnivån för en registeransvarig eller registerförare innefattar instrument såsom uppgiftsskyddsombud, säkerhetsutbildning för anställda, regelbundna revisioner, intrångstester och kvalitetsstämplar.

Exempel: I målet *I. mot Finland*[154] kunde den klagande inte bevisa att andra anställda vid det sjukhus där hon arbetade olagligt hade haft tillgång till hennes sjukjournal. Hennes yrkande på att hennes rätt till dataskydd hade överträtts avvisades därför av de inhemska domstolarna. Europadomstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts eftersom sjukhusets registreringssystem för sjukjournaler var sådant att det inte var möjligt att retroaktivt klargöra användningen av patientregister eftersom det visade endast de fem senaste konsultationerna och den informationen raderades när väl filen hade återlämnats till arkiven. För domstolen var det avgörande att registersystemet på sjukhuset uppenbart inte överensstämde med de rättsliga kraven i inhemsk lag, ett faktum som inte gavs vederbörlig betydelse i de inhemska domstolarna.

Anmälningar om uppgiftsbrott

Ett nytt instrument för att hantera överträdelser av datasäkerheten har införts i dataskyddslagen i flera europeiska länder: skyldigheten för leverantörer av elektroniska kommunikationstjänster att anmäla överträdelser till de sannolika offren och till tillsynsmyndigheter. För telekommunikationsleverantörer är detta obligatoriskt enligt EU-lagstiftninge.[155] Syftet med anmälan om överträdelse till de registrerade är att undvika skada: anmälan om överträdelse och deras möjliga konsekvenser minimerar risken för negativa effekter för de registrerade. Vid fall av allvarlig försumlighet kan leverantörerna också bötfällas.

Att inrätta interna förfaranden i förväg för en effektiv förvaltning och redovisning av överträdelser av säkerhetsbestämmelser kommer att bli nödvändigt eftersom

154 Europadomstolen, *I. mot Finland*, nr 20511/03, 17 juli 2008.

155 Se Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT 2002 L 201, artikel 4.3, ändrad genom Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbetet mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen EUT 2009 L 337.

tidsramen för skyldigheten att rapportera de registrerade och/eller tillsynsmyndigheterna vanligtvis är kort enligt nationell lag.

4.2.2. Sekretess

Enligt EU:s lagstiftning garanteras säker behandling av uppgifter ytterligare av den allmänna skyldigheten för alla personer, registeransvariga eller registerförare, att trygga att uppgifterna förblir konfidentiella.

Exempel: En anställd vid ett försäkringsbolag får ett telefonsamtal på sin arbetsplats från någon som säger att han är en kund, och ber om information rörande sitt försäkringsavtal.

Skyldigheten att bevara sekretessen kring kundernas uppgifter kräver att den anställda minst tillämpar minimisäkerhetsåtgärder innan några personuppgifter lämnas ut. Detta kan exempelvis ske genom att den anställda erbjuder sig att ringa tillbaka till ett telefonnummer som är angivet i kundens akt.

Artikel 16 i dataskyddsdirektivet gäller sekretess endast i förhållandet mellan registeransvarig och registerförare. Huruvida registeransvariga måste hålla uppgifter konfidentiella, i den meningen att de inte får lämna dem till tredje part, tas upp under artikel 7 och 8 i direktivet.

Skyldigheten till sekretess utvidgas inte till situationer där uppgifter kommer till en persons kännedom i dennas egenskap av privat enskild och inte som en anställd hos en registeransvarig eller registerförare. I detta fall gäller inte artikel 16 i dataskyddsdirektivet eftersom privatpersoners användning av personuppgifter är fullständigt undantagen från direktivets ansvarsområde när sådan användning faller inom gränserna för det så kallade hushållsundantaget.[156] Hushållsundantaget är användning av personuppgifter ”av en fysisk person vid en rent personlig verksamhet eller hushållsverksamhet”.[157] Sedan EU-domstolens beslut i målet *Bodil Lindqvist*[158] måste detta undantag emellertid tolkas inskränkt, särskilt vad gäller spridning av uppgifter. Framför allt utvidgas inte hushållsundantaget till publicering av personuppgifter till ett obegränsat antal mottagare på internet (för ytterligare detaljer i målet, se avsnitt 2.1.2, 2.2, 2.3.1 och 6.1)

156 Dataskyddsdirektivet, artikel 3.2, andra strecksatsen.

157 *Ibid.*

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

Enligt Europarådets lagstiftning förutsätts skyldigheten till sekretess i begreppet datasäkerhet i artikel 7 i konvention 108 som handlar om datasäkerhet.

För registerförare innebär sekretess att de kan använda personuppgifter som anförtrotts dem av den registeransvariga endast enligt instruktionerna från den registeransvariga. För en registeransvarigs eller registerförares anställda kräver sekretessen att de använder personuppgifter endast enligt instruktionerna från sina behöriga överordnade.

Skyldigheten till sekretess måste ingå i alla avtal mellan registeransvariga och deras registerförare. Registeransvariga och registerförare måste dessutom vidta särskilda åtgärder för att för sina anställda inrätta en juridisk skyldighet till sekretess, som normalt uppnås genom att sekretessklausuler ingår i de anställdas anställningsavtal.

Överträdelse av den yrkesmässiga skyldigheten till sekretess är straffbar enligt straffrätten i många av EU:s medlemsstater och parter till konvention 108.

4.3. Bestämmelser om öppenhet vid behandling

Viktiga punkter

- Innan personuppgifter börjar behandlas måste den registeransvariga åtminstone informera de registrerade om den registeransvarigas identitet och syftet med behandlingen av uppgifterna, om inte den registrerade redan har informationen.
- Om uppgifterna samlas in från tredje part gäller skyldigheten att lämna information inte om:
  - databehandlingen föreskrivs i lagen; eller
  - tillhandahållande av information visar sig omöjlig eller skulle innebära oproportionerliga ansträngningar.
- Innan den registeransvariga börjar behandla personuppgifter måste han eller hon dessutom:
  - informera tillsynsmyndigheten om de avsedda behandlingarna; eller
  - få behandlingen dokumenterad internt av ett oberoende uppgiftsskyddsombud, om nationell lagstiftning föreskriver sådana förfaranden.

Principen om rättvis behandling kräver en öppen behandling. I **Europaparlamentets lagstiftning** slås i detta syfte fast att alla personer måste kunna fastställa förekomsten av databehandlingsfiler, deras syfte och ansvariga registeransvarig.[159] Hur detta ska uppnås åligger den inhemska lagstiftningen att lösa. **EU-lagstiftningen** är mer specifik, tryggar öppenhet för den registrerade genom den registeransvarigas skyldighet att informera den registrerade och för allmänheten genom anmälan.

Enligt båda rättssystemen kan undantag och restriktioner när det gäller skyldigheten till öppenhet för den registeransvariga finnas i nationell lagstiftning när en sådan restriktion utgör en nödvändig åtgärd för att trygga vissa offentliga intressen eller skydd av den registrerade eller andras rättigheter och friheter, så länge detta är nödvändigt i ett demokratiskt samhälle.[160] Sådana undantag kan exempelvis bli nödvändiga när det gäller brottsutredningar, men kan också motiveras under andra omständigheter.

4.3.1. Information

Enligt Europarådets lagstiftning liksom EU-lagstiftningen är registeransvariga för behandlingar skyldiga att informera den registrerade i förväg om sin avsedda behandling.[161] Denna skyldighet beror inte på en begäran från den registrerade utan måste uppfyllas proaktivt av den registeransvariga, oavsett om den registrerade visar intresse för informationen eller ej.

Informationens innehåll

Informationen måste innehålla syftet med behandlingen, liksom identitet och kontaktuppgifter för den registeransvariga.[162] I dataskyddsdirektivet krävs att ytterligare information ska lämnas när den ”med hänsyn till de särskilda omständigheter under vilka uppgifterna samlas in – är nödvändig för att tillförsäkra den registrerade en korrekt behandling”. I artiklarna 10 och 11 i direktivet anges bland annat kategorier av uppgifter som behandlas och mottagarna av dessa uppgifter, liksom förekomsten av rätten till tillgång till och rätten att ändra uppgifter. När uppgifter samlas

159 Konvention 108, artikel 8 a.

160 *Ibid.*, artikel 9.2, och dataskyddsdirektivet, artikel 13.1.

161 Konvention 108, artikel 8 a och dataskyddsdirektivet, artiklarna 10 och 11.

162 Konvention 108, artikel 8 a och dataskyddsdirektivet, artikel 10 a och 10 b.

in från de registrerade ska informationen klargöra huruvida svar på frågorna är obligatoriska eller frivilliga, liksom de möjliga konsekvenserna av att inte svara.[163]

Enligt **Europarådets lagstiftning** kan tillhandahållandet av sådan information betraktas som god praxis enligt principen om rättvis behandling av uppgifter och är, i denna mån, också en del av Europarådets lagstiftning.

Principen om rättvis behandling kräver att informationen är lätt att förstå för de registrerade. Språket måste anpassas till mottagarna. Olika nivåer och typ av språk kan behöva användas beroende på om de avsedda mottagarna är exempelvis vuxna eller barn, allmänheten eller akademiska experter.

Vissa registrerade kommer att vilja bli informerade endast i korthet om hur och varför deras uppgifter behandlas, medan andra kommer att kräva en detaljerad förklaring. Hur man ska kunna väga in denna aspekt av rättvis information tas upp i ett yttrande från artikel 29-gruppen som främjar idén med ”informationsmeddelanden i flera nivåer”[164], som innebär att den registrerade kan bestämma vilken nivå av detaljer han eller hon föredrar.

Tid för tillhandahållande av information

Dataskyddsdirektivet innehåller något annorlunda bestämmelser rörande tiden när information måste lämnas, beroende på om uppgifterna samlas in från den registrerade (artikel 10) eller från en tredje part (artikel 11). När uppgifterna samlas in från den registrerade ska informationen lämnas senast vid insamlingen. När uppgifterna samlas in från tredje part måste information lämnas senast antingen när den registeransvariga registrerar uppgifterna eller innan uppgifterna lämnas till en tredje part för första gången.

Undantag från skyldigheten att informera

Enligt EU-lagstiftningen finns ett allmänt undantag från skyldigheten att informera den registrerade när han eller hon redan har informationen.[165] Detta gäller situationer när den registrerade, beroende på omständigheterna kring fallet, redan är med-

163 Dataskyddsdirektivet, artikel 10 c.

164 Artikel 29-gruppen (2004), *Yttrande 10/2004 om mer harmoniserade bestämmelser om informationsplikt*, WP 100, Bryssel, 25 november 2004.

165 Dataskyddsdirektivet, artiklarna 10 och 11.1.

veten om att hans eller hennes uppgifter kommer att behandlas för ett visst syfte av en viss registeransvarig.

I artikel 11 i direktivet, som hänför sig till skyldigheten att informera en registrerad när uppgifterna inte har erhållits från honom eller henne, sägs också att det inte finns någon sådan skyldighet, framför allt för behandling i statistiksyfte eller för historisk eller vetenskaplig forskning, om:

- tillhandahållandet av denna information visar sig omöjlig; eller
- det skulle innebära en oproportionerlig ansträngning; eller
- registrering eller spridning av uppgifterna uttryckligen anges i lagen.[166]

Endast i artikel 11.2 i dataskyddsdirektivet anges att registrerade inte behöver informeras om behandlingar om de anges i lagen. Med tanke på det allmänna juridiska antagandet att lagen är känd av de registrerade, kan det hävdas att när uppgifter samlas in från en registrerad enligt artikel 10 i direktivet har han eller hon fått informationen. Men med tanke på att kunskap om lagen endast är ett antagande skulle principen om rättvis behandling enligt artikel 10 kräva att den registrerade informeras även om behandlingen fastställs i lagen, särskilt som det inte är särskilt betungande att informera den registrerade när uppgifterna samlas in direkt från honom eller henne.

När det gäller Europarådets lagstiftning föreskrivs i konvention 108 uttryckligen undantag från artikel 8. Återigen kan undantagen som anges i artiklarna 10 och 11 i dataskyddsdirektivet ses som exempel på god praxis för undantag enligt artikel 9 i konvention 108.

Olika sätt att tillhandahålla information

Det idealiska sättet att tillhandahålla information skulle vara att vända sig till varje registrerad, muntligt eller skriftligt. Om uppgifterna samlas in från den registrerade bör information lämnas i samband med insamlingen. Särskilt när uppgifter samlas in från tredje parter kan information emellertid även lämnas genom lämplig publicering, med tanke på de uppenbara praktiska svårigheterna med att nå de registrerade personligen.

166 *Ibid.*, skäl 40 och artikel 11.2.

Ett av de effektivaste sätten att tillhandahålla information kommer att vara att ha lämpliga informationsklausuler på den registeransvarigas hemsida, exempelvis en policy för integritet på webbplatsen. En betydande andel av befolkningen använder emellertid inte internet och detta bör beaktas i ett företags eller offentlig myndighets informationspolicy.

4.3.2. Anmälan

Enligt nationell lag kan registeransvariga tvingas informera behörig tillsynsmyndighet om behandling av uppgifter så att dessa kan offentliggöras. Alternativt kan det i nationell lag föreskrivas att registeransvariga kan anställa ett uppgiftsskyddsombud, som är ansvarig framför allt för att hålla ett register över behandlingar som den registeransvariga utför.[167] Detta interna register måste göras tillgängligt för allmänheten på begäran.

Exempel: En anmälan, liksom dokumentation av ett uppgiftsskyddsombud, måste beskriva huvudinslagen i den aktuella behandlingen av uppgifter. Detta innefattar information om den registeransvariga, syftet med behandlingen, den rättsliga grunden för behandlingen, vilka kategorier av uppgifter som behandlas, vilka tredje parter som sannolikt är mottagare och huruvida gränsöverskridande flöden planeras, och i så fall vilka.

Publiceringen av anmälningar från tillsynsmyndigheten måste ske i form av ett särskilt register. För att uppfylla målsättningen måste det vara enkelt och kostnadsfritt att få tillgång till registret. Detsamma gäller dokumentationen som innehas av en registeransvarigs uppgiftsskyddsombud.

De fall i vilka undantag från skyldigheten att informera behörig tillsynsmyndighet eller anställa ett uppgiftsskyddsombud får föreskrivas i nationell lag, förutsatt att behandlingen av uppgifter sannolikt inte kan innebära någon specifik risk för de registrerade, anges i artikel 18.2 i dataskyddsdirektivet.[168]

167 *Ibid*., artikel 18.2, andra strecksatsen.

168 *Ibid*., artikel 18.2, första strecksatsen.

4.4. Bestämmelser om främjande av överensstämmelse

Viktiga punkter

- Vid utveckling av principen om ansvarighet nämns i dataskyddsdirektivet bland annat följande instrument för att främja överensstämmelse:
  - förhandskontroll av avsedd behandling, som utförs av den nationella tillsynsmyndigheten;
  - uppgiftsskyddsombud, som ska förse den registeransvariga med särskilda expertkunskaper inom dataskyddsområdet;
  - uppförandekodexar som specificerar hur befintliga bestämmelser om dataskydd ska tillämpas inom ett område i samhället och framför allt näringslivet.
- I Europarådets lagstiftning föreslås liknande instrument för att främja överensstämmelse i dess rekommendationer om profilering.

4.4.1. Förhandskontroll

Enligt artikel 20 i dataskyddsdirektivet måste tillsynsmyndigheten förhandskontrollera sådan behandling av uppgifter som kan orsaka specifika risker för de registrerades rättigheter och friheter – på grund av antingen syftet eller omständigheterna kring behandlingen – innan denna inleds. Nationell lag måste fastställa vilka behandlingar som ska omfattas av förhandskontroll. En sådan kontroll kan leda till att behandlingar av uppgifter förbjuds, eller till att utformningen av den föreslagna behandlingen måste ändras på vissa punkter. Artikel 20 i direktivet syftar till att säkerställa att onödigt riskfyllda behandlingar inte ens inleds, eftersom tillsynsmyndigheten har befogenhet att förbjuda sådan behandling. Förutsättningen för att detta system ska fungera är att tillsynsmyndigheten verkligen informeras. För att säkerställa att de registeransvariga uppfyller sin skyldighet att informera behöver tillsynsmyndigheterna tvingande befogenheter, såsom möjligheten att bötfälla registeransvariga.

Exempel: Om ett företag genomför sådan uppgiftsbehandling som enligt nationell lagstiftning omfattas av obligatorisk förhandskontroll måste företaget lämna dokumentation om den planerade behandlingen av uppgifter till

tillsynsmyndigheten. Företaget får inte inleda behandlingen innan det fått ett positivt svar från tillsynsmyndigheten.

I vissa medlemsstater föreskrivs i nationell lag alternativt att behandlingen kan inledas om inte tillsynsmyndigheten har hört av sig inom en viss tid, exempelvis tre månader.

4.4.2. Uppgiftsskyddsombud

Enligt dataskyddsdirektivet är det möjligt att i nationell lag föreskriva att registeransvariga kan utnämna en tjänsteman som fungerar som uppgiftsskyddsombud.[169] Syftet med en sådan funktion är att säkerställa att den registrerades rättigheter och friheter sannolikt inte påverkas negativt av behandlingen av uppgifterna.[170]

Exempel: I Tyskland är, enligt avsnitt 4f, underavsnitt 1, i den tyska federala dataskyddslagstiftningen (*Bundesdatenschutzgesetz*), privatägda företag skyldiga att utse ett internt uppgiftsskyddsombud för skydd av personuppgifter om de permanent har tio eller fler anställda som hanterar den automatiska behandlingen av personuppgifter.

Förmågan att uppnå målet kräver att ombudet har ett visst mått av oberoende inom den registeransvarigas organisation, vilket uttryckligen påpekas i direktivet. Tydliga anställningsrättigheter för att skydda mot eventualiteter som omotiverad uppsägning kan också behövas för att bidra till att funktionen fungerar effektivt.

I syfte att främja överensstämmelse med nationell dataskyddslagstiftning har begreppet internt uppgiftsskyddsombud också antagits i vissa av Europarådets rekommendationer.[171]

4.4.3. Uppförandekoder

För att främja överensstämmelse kan företagen och andra sektorer skapa detaljerade regler som styr deras representativa behandling av uppgifter, och kodifierar bästa praxis. Expertkunskaperna bland medlemmarna i sektorn bidrar till att hitta lösningar som är praktiska och därför sannolikt följs. På samma sätt uppmuntras

169 *Ibid.*, artikel 18.2, andra strecksatsen.

170 *Ibid.*

171 Se exempelvis rekommendationen om profilering, artikel 8.3.

medlemsstaterna – liksom Europeiska kommissionen – att främja inrättande av uppförandekoder avsedda att bidra till ett korrekt införlivande av de nationella bestämmelserna som antagits av medlemsstaterna enligt direktivet, och med beaktande av de specifika egenskaperna hos de olika sektorerna.[172]

I syfte att säkerställa att dessa uppförandekoder följer nationella bestämmelser som antagits i enlighet med dataskyddsdirektivet måste medlemsstaterna fastställa ett förfarande för att utvärdera koderna. Förfarandet kräver normalt att den nationella myndigheten, branschorganisationer och andra organ som företräder andra kategorier av registeransvariga är delaktiga.[173]

Förslag till gemenskapskoder och ändringar eller utvidgningar av befintliga gemenskapskoder kan lämnas till artikel 29-gruppen för utvärdering. Efter gruppens godkännande kan Europeiska kommissionen se till att koderna offentliggörs på lämpligt sätt.[174]

Exempel: Den europeiska föreningen för direktmarknadsföring (FEDMA) utarbetade en europeisk uppförandekod för användning av personuppgifter i direktmarknadsföring. Uppförandekoden lades framgångsrikt fram för artikel 29-gruppen. En bilaga om elektronisk marknadskommunikation lades till koden 2010.[175]

172 Se dataskyddsdirektivet, artikel 27.1.

173 *Ibid.*, artikel 27.2.

174 *Ibid.,* artikel 27.3.

175 Artikel 29-gruppen (2010), *Yttrande 4/2010 över FEDMA:s europeiska uppförandekodex för användning av personuppgifter i direkt marknadsföring*, WP 174, Bryssel, 13 juli 2010.

5

Den registrerades rättigheter och dessas genomförande

EU	Frågor som täcks	Europarådet
Rätt till tillträde		
Dataskyddsdirektivet, artikel 12 EU-domstolen, C-553/07, *College van burgemeester en wethouders van Rotterdam mot M.E.E. Rijkeboer*, 7 maj 2009	**Rätt att få tillgång till egna uppgifter**	Konvention 108, artikel 8 b
	Rätt till ändring, strykning (radering) eller blockering	Konvention 108, artikel 8 c Europadomstolen, *Cemalettin Canli mot Turkiet*, nr 22427/04, 18 november 2008 Europadomstolen, *Segerstedt-Wiberg m.fl. mot Sverige*, nr 62332/00, 6 juni 2006 Europadomstolen, *Ciubotaru mot Moldavien*, nr 27138/04, 27 april 2010
Rätt till invändning		
Dataskyddsdirektivet, artikel 14.1 a	**Rätt till invändning på grund av den registrerades särskilda situation**	Rekommendation om profilering, artikel 5.3
Dataskyddsdirektivet, artikel 14.1 b	**Rätt att invända mot ytterligare användning av uppgifterna i marknadsföringssyfte**	Rekommendation om direktmarknadsföring, artikel 4.1
Dataskyddsdirektivet, artikel 15	**Rätt att invända mot automatiska beslut**	Rekommendation om profilering, artikel 5.5

EU	Frågor som täcks	Europarådet
Oberoende tillsyn		
Stadgan, artikel 8.3 Dataskyddsdirektivet, artikel 28 Dataskyddsförordningen, kapitel V Allmänna uppgiftsskyddsförordningen EU-domstolen, C-518/07, *Europeiska kommissionen mot Förbundsrepubliken Tyskland*, 9 mars 2010 EU-domstolen, C-614/10, *Europeiska kommissionen mot Förbundsrepubliken Österrike*, 16 oktober 2012 EU-domstolen, C-288/12, *Europeiska kommissionen mot Ungern*, 8 april 2014	**Nationella tillsynsmyndigheter**	Konvention 108, tilläggsprotokoll, artikel 1
Prövning och sanktioner		
Dataskyddsdirektivet, artikel 12	**Begäran till den registeransvariga**	Konvention 108, artikel 8 b
Dataskyddsdirektivet, artikel 28.4 Dataskyddsförordningen, artikel 32.2	**Klagomål framförda till en tillsynsmyndighet**	Konvention 108, tilläggsprotokoll, artikel 1.2. b
Stadgan, artikel 47	**Domstolar (i allmänhet)**	Europakonventionen, artikel 13
Dataskyddsdirektivet, artikel 28.3	**Nationella domstolar**	Konvention 108, tilläggsprotokoll, artikel 1.4
EUF-fördraget, artikel 263.4 Dataskyddsförordningen, artikel 32.1 FUF-fördraget, artikel 267	**EU-domstolen**	
	Europadomstolen	Europakonventionen, artikel 34
Prövning och sanktioner		
Stadgan, artikel 47 Dataskyddsdirektivet, artiklarna 22 och 23 EU-domstolen, C-14/83, *Sabine von Colson och Elisabeth Kamann mot Land Nordrhein-Westfalen*, 10 april 1984 EU-domstolen, C-152/84, *M.H. Marshall mot Southampton och South-West Hampshire Area Health Authority*, 26 februari 1986	**För överträdelser av nationell lagstiftning om skydd av personuppgifter**	Europakonventionen, artikel 13 (endast för Europarådets medlemmar) Konvention 108, artikel 10 *Europadomstolen, K.U. mot Finland*, nr 2872/02, 2 december 2008 *Europadomstolen, Biriuk mot Litauen*, nr 23373/03, 25 november 2008

EU	Frågor som täcks	Europarådet
Dataskyddsförordningen, artiklarna 34 och 49 EU-domstolen, C-28/08 P, *Europeiska kommissionen mot The Bavarian Lager Co. Ltd*, 29 juni 2010	För EU-institutionernas och organens överträdelse av EU-lagstiftning	

Rättsreglernas effektivitet i allmänhet, och de registrerades rättigheter i synnerhet, beror i avsevärd utsträckning på förekomsten av lämpliga mekanismer för att genomföra dem. I den europeiska dataskyddslagstiftningen måste den registrerade vara berättigad att enligt nationell lag skydda sina uppgifter. Oberoende tillsynsmyndigheter måste också inrättas enligt nationell lag för att bistå de registrerade i utövandet av deras rättigheter och övervaka behandlingen av personuppgifter. Rätten till effektiv prövning, som garanteras enligt Europakonventionen och stadgan, kräver att rättslig prövning är tillgänglig för alla.

5.1. De registrerades rättigheter

Viktiga punkter

- Alla ska enligt nationell lag ha rätt att från alla registeransvariga begära information om huruvida den registeransvariga behandlar hans eller hennes uppgifter.
- De registrerade ska enligt nationell lag ha rätt att:
  - få tillgång till sina egna uppgifter från alla registeransvariga som behandlar dessa uppgifter;
  - få sina uppgifter korrigerade (eller blockerade, i förekommande fall) av den registeransvariga som behandlar deras uppgifter om dessa är felaktiga;
  - få sina uppgifter raderade eller blockerade, i förekommande fall, av den registeransvariga om han eller hon behandlar uppgifterna olagligt.
- De registrerade ska dessutom ha rätt att invända mot registeransvariga när det gäller:
  - automatiska beslut (fattade med hjälp av personuppgifter som behandlas enbart automatiskt);
  - behandling av deras uppgifter om det leder till oproportionerliga resultat;
  - användningen av deras uppgifter för direktmarknadsföring.

5.1.1. Rätt till tillträde

I EU-lagstiftningen anges i artikel 12 i dataskyddsdirektivet en rad bestämmelser rörande den registrerades rätt till tillgång, inbegripet rätten att från den registeransvariga erhålla ”bekräftelse på om uppgifter som rör honom behandlas eller inte och information om åtminstone ändamålen med behandlingen, de berörda uppgiftskategorierna och mottagarna eller mottagarkategorierna till vilka uppgifterna utlämnas” liksom att ”få sådana uppgifter som inte behandlats i enlighet med bestämmelserna i detta direktiv rättade, utplånade eller blockerade, särskilt om dessa är ofullständiga eller felaktiga”.

I Europarådets lagstiftning finns samma rättigheter och måste tillhandahållas i den inhemska lagstiftningen (artikel 8 i konvention 108). I flera av Europarådets rekommendationer används begreppet ”tillgång” och de olika aspekterna av rätten till tillgång beskrivs och föreslås för genomförande i inhemsk lag på samma sätt som anges i stycket ovan.

Enligt artikel 9 i konvention 108 och artikel 13 i dataskyddsdirektivet kan den registeransvarigas skyldighet att bemöta en registrerads begäran om tillgång begränsas som ett resultat av andras överordnade rättsliga intressen. Att åsidosätta rättsliga intressen kan innefatta offentliga intressen såsom nationell säkerhet, offentlig säkerhet och åtal av brott liksom privata intressen som är mer tvingande än dataskyddsintressen. Eventuella undantag eller restriktioner måste vara nödvändiga i ett demokratiskt samhälle och proportionerliga mot det eftersträvade syftet. I mycket exceptionella fall, exempelvis på grund av medicinska indikationer, kan skyddet av den registrerade i sig kräva en restriktion när det gäller öppenhet. Detta gäller särskilt vid begränsning av rätten till tillgång för alla registrerade.

Närhelst uppgifter behandlas enbart för vetenskaplig forskning eller för statistiska syften möjliggör dataskyddsdirektivet att rätten till tillgång kan begränsas i nationell lag. Lämpliga rättsliga garantier måste emellertid finnas. Det måste framför allt säkerställas att inga åtgärder eller beslut rörande någon enskild individ vidtas i samband med denna behandling av uppgifter och att det ”tydligt inte finns någon risk för att den registrerades integritet ska överträdas”.[176] Liknande bestämmelser finns i artikel 9.3 i konvention 108.

176 Dataskyddsdirektivet, artikel 13.2.

Rätt att få tillgång till egna uppgifter

Enligt Europarådets lagstiftning medges uttryckligen rätten till tillgång till de egna uppgifterna i artikel 8 i konvention 108. Europadomstolen har vid flera tillfällen ansett att man har rätt att få tillgång till information om de egna personuppgifterna som innehas eller används av andra, och att denna rätt härrör ur behovet av att respektera privatlivet.[177] I målet *Leander*[178] drog Europadomstolen slutsatsen att rätten till tillgång till personuppgifter som lagras av offentliga myndigheter emellertid kan begränsas under vissa omständigheter.

Enligt EU-lagstiftningen medges rätten till tillgång till de egna uppgifterna uttryckligen i artikel 12 i dataskyddsdirektivet och som en grundläggande rättighet i artikel 8.2 i stadgan.

I artikel 12 a i stadgan föreskrivs att medlemsstaterna ska garantera alla registrerade rätten till tillgång till deras personuppgifter och till information. Framför allt har alla registrerade rätt att från den registeransvariga erhålla bekräftelse huruvida uppgifter rörande honom eller henne behandlas och information rörande åtminstone följande:

- syftet med behandlingen;
- berörda kategorier av uppgifter;
- vilka uppgifter som behandlas;
- mottagare eller kategorier av mottagare som uppgifterna lämnas till;
- eventuell tillgänglig information om källan till de uppgifter som behandlas;
- vid automatiska beslut, logiken bakom all automatisk behandling av uppgifterna.

Nationell lag kan lägga till information som den registeransvariga ska lämna, exempelvis citera den rättsliga grund som tillåter behandling av uppgifterna.

177 Europadomstolen, *Gaskin mot Förenade kungariket*, nr 10454/83, 7 juli 1989, Europadomstolen, *Odièvre mot Frankrike* [GC], nr 42326/98, 13 februari 2003, Europadomstolen, *K.H. m.fl. mot Slovakien*, nr 32881/04, 28 april 2009, Europadomstolen, *Godelli mot Italien*, nr 33783/09, 25 september 2012.

178 Europadomstolen, *Leander mot Sverige*, nr 9248/81, 26 mars 1987.

Exempel: Genom att få tillgång till någons personuppgifter kan man fastställa huruvida uppgifterna är korrekta. Det är därför nödvändigt att den registrerade informeras om de kategorier uppgifter som behandlas, liksom om innehållet i uppgifterna. Det är därför otillräckligt för en registeransvarig att helt enkelt berätta för den registrerade att hans eller hennes namn, adress, födelsedatum och intresseområden behandlas. Den registeransvariga måste också berätta för den registrerade att han eller hon behandlar ”namnet: N.N.; en adress: 1040 Wien, Schwarzenbergplatz 11, Österrike; födelsedatumet: 10.10.1974; och intresseområdet (enligt den registrerades förklaring): klassisk musik.” Den sista punkten innehåller dessutom information om uppgiftskällan.

Information till den registrerade om de uppgifter som behandlas och om eventuell tillgänglig information om deras källa måste lämnas i en begriplig form, vilket innebär att den registeransvariga kan behöva förklara för den registrerade mer i detalj vad som behandlas. Att exempelvis endast citera tekniska förkortningar eller medicinska termer som svar på en begäran om tillgång räcker vanligtvis inte, även om endast dessa förkortningar eller begrepp lagras.

Information om källan till uppgifter som behandlas av den registeransvariga måste lämnas som svar på en begäran om tillgång, under förutsättning att denna information är tillgänglig. Bestämmelsen måste ses mot bakgrund av principerna om rättvisa och ansvarighet. En registeransvarig får inte förstöra information om källan till uppgifter i syfte att slippa lämna ut den, han eller hon får inte heller bortse från gängse standarder och de erkända behoven av dokumentation inom sina verksamhetsområden. Att inte behålla någon dokumentation om källan till de behandlade uppgifterna uppfyller vanligtvis inte den registeransvarigas skyldigheter enligt rätten till tillgång.

När automatiska utvärderingar genomförs behöver den allmänna logiken i utvärderingen förklaras, inbegripet de särskilda kriterierna som har övervägts vid utvärderingen av den registrerade.

I direktivet framgår inte tydligt huruvida rätten att få tillgång till information gäller det förflutna och i så fall vilken period. I det hänseendet får, såsom betonas i EU-domstolens rättspraxis, inte rätten att få tillgång till någons uppgifter otillbörligt begränsas av tidsfrister. De registrerade måste också få en rimlig möjlighet att få information om tidigare behandling av uppgifter.

Exempel: I målet *Rijkeboer*[179] ombads EU-domstolen att fastställa huruvida, enligt artikel 12 a i direktivet, en enskilds rätt till tillgång till information om mottagarna eller kategorier av mottagare av personuppgifter och om innehållet i de uppgifter som lämnas får begränsas till ett år före hans eller hennes begäran om tillgång.

För att avgöra huruvida artikel 12 a i direktivet tillåter en sådan tidsgräns beslutade domstolen att tolka artikeln mot bakgrund av direktivets syften. Domstolen slog först fast att rätten till tillgång är nödvändig för att den registrerade ska kunna utöva sin rätt att be den registeransvariga ändra, radera eller blockera hans eller hennes uppgifter (artikel 12 b), eller informera tredje part till vilka uppgifterna har lämnats om ändringen, raderingen eller blockeringen (artikel 12 c). Rätten till tillgång är också nödvändig för att den registrerade ska kunna utöva sin rätt att invända mot att hans eller hennes personuppgifter behandlas (artikel 14), eller sin rätt till agerande om han eller hon lider skada (artiklarna 22 och 23).

I syfte att säkerställa de praktiska effekterna av de bestämmelser som hänvisas till ovan ansåg domstolen att ”den rätten av nödvändighet måste gälla det förgångna. Om så inte var fallet skulle den registrerade inte effektivt kunna utöva sin rätt att få uppgifter som anses otillåtna eller felaktiga rättade, raderade eller blockerade eller vidta rättsliga åtgärder mot och erhålla ersättning för den skada som lidits”.

Rätten till ändring, radering och blockering av uppgifter

”Alla måste kunna utöva sin rätt att få tillgång till uppgifter som rör dem och som är föremål för behandling, för att i detalj kunna försäkra sig om att uppgifterna är korrekta och om att behandlingen är tillåten.”[180] I linje med dessa principer måste de registrerade ha rätt att enligt nationell lag från den registeransvariga erhålla ändring, radering eller blockering av sina uppgifter, om de anser att behandlingen av dem inte överensstämmer med bestämmelserna i direktivet, särskilt på grund av de felaktiga och ofullständiga uppgifterna.[181]

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

180 Dataskyddsdirektivet, skäl 41.

181 *Ibid.*, artikel 12 b.

Exempel: I målet *Cemalettin Canli mot Turkiet*[182] ansåg Europadomstolen att artikel 8 i Europakonventionen hade överträtts på grund av felaktig polisrapportering i rättegångsförfaranden.

Den klagande hade två gånger varit delaktig i rättegångsförfaranden på grund av påstått medlemskap i olagliga organisationer, men dömdes aldrig. När den klagande återigen arresterades och åtalades för ytterligare ett brott lämnade polisen en rapport till brottmålsdomstolen med titeln "*informationsblankett om ytterligare brott*", där den klagande förekom som medlem i två olagliga organisationer. Den klagandes begäran att få rapporten och polisregistret ändrade var utan framgång. Europadomstolen ansåg att informationen i polisens rapport låg inom omfattningen av artikel 8 i Europakonvention, eftersom offentlig information också kunde falla inom omfattningen av "privatlivet" där den systematiskt samlades in och lagrades i register som innehades av myndigheterna. Polisrapporten var dessutom felaktig och dess redogörelse och överlämnande till brottmålsdomstolen hade inte skett i enlighet med lagen. Domstolen drog därför slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Exempel: I målet *Segerstedt-Wiberg m.fl. mot Sverige*[183] hade de klagande anslutits till vissa liberala och kommunistiska politiska partier. De misstänkte att information om dem hade förts in i säkerhetspolisens register. Europadomstolen var tillfreds med att lagringen av de aktuella uppgifterna hade en rättslig grund och ett berättigat syfte. När det gäller vissa av de klagande fann Europadomstolen att den fortsatta lagringen av uppgifterna var ett oproportionerligt intrång i deras privatliv. I fallet med herr Schmid lagrade exempelvis myndigheterna information om att han 1969 lär ha förespråkat våldsamt motstånd mot polisen under demonstrationer. Europadomstolen ansåg att informationen inte kan ha gällt något nationellt säkerhetsintresse, särskilt med tanke på att det var så pass länge sedan. Europadomstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts när det gäller fyra av de fem klagande.

I vissa fall räcker det att den registrerade helt enkelt begär ändring av exempelvis ett namns stavning, ändring av adress eller telefonnummer. Om en sådan begäran emellertid är förbunden med rättsliga frågor, såsom den registrerades juridiska identitet, eller korrekt bostadsadress för leverans av juridiska handlingar, kanske en

182 Europadomstolen, *Cemalettin Canli mot Turkiet*, nr 22427/04, 18 november 2008, punkterna 33, 42 och 43, Europadomstolen, *Dalea mot Frankrike*, nr 964/07, 2 februari 2010.

183 Europadomstolen, *Segerstedt-Wiberg m.fl. mot Sverige*, nr 62332/00, 6 juni 2006, punkterna 89 och 90; se även exempelvis: Europadomstolen, *M.K. mot Frankrike*, nr 19522/09, 18 april 2013.

begäran om ändring inte är tillräckligt och den registeransvariga kan behöva begära bevis för den påstådda felaktigheten. Dessa krav får inte innebära en orimlig bevisbörda för den registrerade och på så sätt hindra honom eller henne från att få sina uppgifter ändrade. Europadomstolen har funnit att artikel 8 i Europakonventionen har överträtts i flera fall när den klagande inte har kunnat ifrågasätt korrektheten i den information som de hemliga registren innehåller.[184]

Exempel: I målet *Ciubotaru mot Moldavien*[185] kunde inte den klagande ändra registreringen av sitt etniska ursprung i officiella register från moldavier till rumän eftersom han inte ansågs kunna underbygga sin begäran. Europadomstolen ansåg det acceptabelt att stater kräver objektiva bevis vid registrering av en individs etniska identitet. När en sådan begäran baserades enbart på subjektiva och obestyrkta grunder kan myndigheterna vägra. Den klagandes begäran hade emellertid baserats på mer än den subjektiva uppfattningen om hans egen etnicitet. Han hade kunnat tillhandahålla objektivt verifierbara länkar till den rumänska etniska gruppen såsom språk, namn, empati och annat. Enligt inhemsk lag begärdes emellertid att den klagande skulle lämna bevis för att hans föräldrar hade tillhört den rumänska etniska gruppen. Med tanke på Moldaviens historiska verklighet hade ett sådant krav skapat ett oöverstigligt hinder mot att registrera en annan etnisk identitet än den som de sovjetiska myndigheterna hade registrerat för hans föräldrar. Genom att hindra den klagande från att få sitt krav granskat mot bakgrund av objektivt verifierbara bevis hade staten inte uppfyllt sin positiva skyldighet att trygga den klagandes faktiska respekt för hans privatliv. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Under en civil tvist eller förhandlingar inför en offentlig myndighet för att besluta om huruvida uppgifter är korrekta eller ej kan den registrerade begära att en uppgift eller anteckning registreras in i hans eller hennes datafil om att korrektheten ifrågasätts, och att ett officiellt beslut ännu inte har fattats. Under denna period får den registeransvariga inte lägga fram uppgifterna som säkra eller slutgiltiga, särskilt inte till tredje part.

En registrerads begäran att få uppgifter raderade eller strukna baseras ofta på ett klagomål om att databehandlingen inte har en berättigad grund. Ett sådant krav uppstår ofta när samtycke har dragits tillbaka, eller när vissa uppgifter inte längre

184 Europadomstolen, *Rotaru mot Rumänien*, nr 28341/95, 4 maj 2000.

185 Europadomstolen, *Ciubotaru mot Moldavien*, nr 27138/04, 27 april 2010, punkterna 51 och 59.

behövs för att uppfylla syftet med insamlingen av uppgifter. Bevisbördan för att databehandlingen är berättigad faller på den registeransvariga, eftersom han eller hon är ansvarig för att behandlingen är berättigad. Enligt principen om ansvarighet måste den registeransvariga när som helst kunna visa att det finns en sund rättslig grund för behandlingen av uppgifterna, i annat fall måste behandlingen avbrytas.

Om behandlingen av uppgifterna ifrågasätts på grund av att uppgifterna påstås vara felaktiga eller otillåtet behandlade kan den registrerade, i enlighet med principen om rättvis behandling, kräva att de ifrågasätta uppgifterna blockeras. Det innebär att uppgifterna inte raderas men att den registeransvariga måste avstå från att använda dem under den tid de är blockerade. Det är särskilt nödvändigt om fortsatt användning av felaktiga eller olagligt innehavda uppgifter skulle kunna skada den registrerade. Nationell lag bör tillhandahålla mer detaljer om när skyldigheten att blockera användningen av uppgifter kan uppstå och hur den bör utövas.

De registrerade har dessutom rätt att från den registeransvariga erhålla meddelanden till tredje part om eventuell blockering, ändring eller radering, om de hade erhållit uppgifter före denna behandling. Eftersom spridning av uppgifter till tredje part skulle ha dokumenterats av den registeransvariga bör det vara möjligt att identifiera mottagarna av uppgifter och kräva att de raderas. Om uppgifterna emellertid under tiden har offentliggjorts, exempelvis på internet, kan det vara omöjligt att få uppgifterna raderade i alla instanser eftersom mottagarna av uppgifterna inte kan hittas. Enligt dataskyddsdirektivet är det obligatoriskt att kontakta mottagare av uppgifter för rättelse, utplåning eller blockering av uppgifterna ”om detta inte visar sig vara omöjligt eller innebär en oproportionerligt stor ansträngning”.[186]

5.1.2. Rätt till invändning

Rätten till invändning innefattar rätten att invända mot automatiska individuella beslut, rätten att invända på grund av den registrerades särskilda situation och rätten att invända mot ytterligare användning av uppgifterna för direktmarknadsföring.

Rätt att invända mot automatiska individuella beslut

Automatiska beslut fattas med hjälp av personuppgifter som behandlas enbart automatiskt. Om dessa beslut sannolikt får avsevärd inverkan på enskildas liv

186 Dataskyddsdirektivet, artikel 12 c, andra hälften av den sista meningen.

eftersom de exempelvis hänför sig till kreditvärdighet, arbetsprestation, uppförande eller tillförlitlighet krävs särskilt skydd för att undvika olämpliga konsekvenser. I dataskyddsdirektivet föreskrivs att automatiska beslut inte bör avgöra frågor som är viktiga för enskilda och kräver att den enskilda bör ha rätt att se över det automatiska beslutet.[187]

Exempel: Ett viktigt praktiskt exempel på automatiskt beslutsfattande är kreditbedömning. I syfte att snabbt besluta om en blivande kunds kreditvärdighet samlas vissa uppgifter, såsom yrke och familjesituation/civilstånd, in från kunden och kombineras med uppgifter om den registrerade som är tillgängliga från andra resurser, exempelvis kreditinformationssystem. Dessa uppgifter matas automatiskt in i en poängalgoritm, som beräknar ett övergripande värde som utgör den potentiella kundens kreditvärdighet. Den anställda vid företaget kan på så sätt på några sekunder avgöra om den registrerade kan godkännas som kund eller ej.

Enligt direktivet ska emellertid medlemsstaterna se till att en person kan omfattas av ett automatiskt individuellt beslut om den registrerades intressen antingen inte är aktuella, på grund av att beslutet var till den registrerades fördel, eller de skyddas på andra lämpliga sätt.[188] En rätt att invända mot automatiska beslut ingår även i **Europarådets lagstiftning**, vilket framgår av rekommendationen om profilering.[189]

Rätt till invändning på grund av den registrerades särskilda situation

Det finns ingen generell rätt för registrerade att invända mot behandling av deras uppgifter.[190] Artikel 14 a i dataskyddsdirektivet ger emellertid de registrerade möjlighet att invända mot tvingande berättigade grunder rörande den registrerades särskilda situation. En liknande rätt har medgivits i Europarådets rekommendation om profilering.[191] Dessa bestämmelser syftar till att hitta den korrekta balansen mellan den registrerades rätt till skydd av personuppgifter och andras berättigade rättigheter när det gäller behandling av den registrerades uppgifter.

187 *Ibid.*, artikel 15.1.

188 *Ibid.*, artikel 15.2.

189 Rekommendation om profilering, artikel 5.5.

190 Se även Europadomstolen, *M.S. mot Sverige*, nr 20837/92, 27 augusti 1997, där medicinska uppgifter förmedlades utan samtycke eller möjlighet att invända, eller Europadomstolen, *Leander mot Sverige*, nr 9248/81, 26 mars 1987, eller Europadomstolen, *Mosley mot Förenade kungariket*, nr 48009/08, 10 maj 2011.

191 Rekommendation om profilering, artikel 5.3.

Exempel: En bank lagrar uppgifter i sju år om sina kunder som missköter betalningen av sina lån. En kund vars uppgifter lagras i denna databas ansöker om ett nytt lån. Databasen konsulteras, en utvärdering av den ekonomiska situationen görs och kunden förvägras lånet. Kunden kan emellertid invända mot att ha personuppgifter lagrade i databasen och kräva att uppgifterna raderas om han eller hon kan bevisa att den uteblivna betalningen endast var resultatet av ett misstag som omedelbart hade korrigeras efter att kunden blivit medveten om det.

Resultatet av en framgångsrik invändning är att uppgifterna i fråga inte längre behandlas av den registeransvariga. Behandling av den registrerades uppgifter som skett före invändningen är emellertid berättigade.

Rätt att invända mot ytterligare användning av uppgifterna för direktmarknadsföring

I artikel 14 b i dataskyddsdirektivet föreskrivs en specifik rätt att invända mot användningen av personuppgifter för direktmarknadsföring. En sådan rätt fastställs även i Europarådets rekommendation om direktmarknadsföring.[192] Detta slag av invändning ska göras innan uppgifterna görs tillgängliga för tredje part i direktmarknadsföringssyfte. Den registrerade måste därför få möjlighet att invända innan uppgifterna överförs.

5.2. Oberoende tillsyn

Viktiga punkter

- För att effektivt skydda personuppgifter måste oberoende tillsynsmyndigheter inrättas enligt nationell lag.
- Nationella tillsynsmyndigheter måste agera fullständigt oberoende, vilket måste garanteras genom lagen om inrättandet och återspeglas i tillsynsmyndighetens specifika organisatoriska struktur.
- Tillsynsmyndigheter har särskilda uppgifter, bland annat, att:
  - övervaka och främja uppgiftsskydd på nationell nivå;

192 Europarådet, ministerkommittén (1985), rekommendation Rec (85)20 till medlemsstaterna om skydd av personuppgifter som används för direktmarknadsföring, 25 oktober 1985, artikel 4.1.

- ge råd till registrerade och registeransvariga samt till staten och den stora allmänheten;
- lyssna på klagomål och bistå den registrerade vid påstådda överträdelser av rättigheter när det gäller skydd av personuppgifter;
- övervaka registeransvariga och registerförare;
- ingripa vid behov genom att
  - varna, tillrättavisa eller till och med bötfälla registeransvariga och registerförare,
  - kräva att uppgifter ändras, blockeras eller raderas,
  - införa förbud mot behandling;
- hänvisa ärenden till domstol.

I dataskyddsdirektivet krävs oberoende tillsyn för att säkerställa effektivt skydd av uppgifter. Genom direktivet infördes ett instrument för skydd av uppgifter som inte inledningsvis fanns i konvention 108 eller i OECD:s riktlinjer för skydd av privatlivet.

Med tanke på att oberoende tillsyn visade sig vara nödvändig för att utveckla ett effektivt skydd av uppgifter innebär en ny bestämmelse i de reviderade riktlinjerna för skydd av privatlivet från OECD som antogs 2013 att medlemsstaterna uppmanas att inrätta och upprätthålla myndigheter för genomförande av integritet med styrning, resurser och tekniska expertkunskaper som krävs för att utöva deras befogenheter effektivt och fatta beslut på en objektiv, opartisk och konsekvent grund.[193]

I Europarådets lagstiftning har tillsynsmyndigheterna blivit obligatoriska genom tilläggsprotokollet till konvention 108. Instrumentet innehåller i artikel 1 den rättsliga ramen för oberoende tillsynsmyndigheter som avtalsparterna måste införliva i sin inhemska lagstiftning. Där används liknande formuleringar för att beskriva uppgifter och befogenheter för dessa myndigheter såsom de används i dataskyddsdirektivet. I princip bör tillsynsmyndigheter därför fungera på samma sätt enligt EU:s och Europarådets lagstiftning.

I EU:s lagstiftning angavs behörigheter och organisatorisk struktur för tillsynsmyndigheter inledningsvis i artikel 28.1 i dataskyddsdirektivet. I

193 OECD (2013), *Guidelines on governing the Protection of Privacy and Transborder Flows of Personal Data (riktlinjer för skydd av privatlivet och gränsöverskridande flöden av personuppgifter)*, punkt 19 c.

dataskyddsförordningen[194] fastställs Europeiska datatillsynsmannen som tillsynsmyndighet för behandling av uppgifter i EU:s institutioner och organ. Vid fastställande av tillsynsmyndighetens roll och ansvar tas i förordningen hänsyn till den erfarenhet som samlats sedan dataskyddsdirektivet utfärdades.

Dataskyddsmyndigheternas oberoende garanteras enligt artikel 16.2 i EUF-fördraget och artikel 8.3 i stadgan. Den sista bestämmelsen avser specifikt kontroll av en oberoende myndighet som en viktig beståndsdel i den grundläggande rätten till skydd av personuppgifter. I dataskyddsdirektivet krävs dessutom att medlemsstaterna ska inrätta tillsynsmyndigheter för att övervaka tillämpningen av direktivet, och att de ska agera fullständigt oberoende.[195] Den lag som stödjer inrättandet av ett tillsynsorgan måste inte bara innehålla bestämmelser som specifikt garanterar oberoende utan myndighetens specifika organisatoriska struktur måste även visa på oberoende.

År 2010 hanterade EU-domstolen för första gången frågan om omfattningen av kraven på oberoende för tillsynsmyndigheterna inom uppgiftsskydd.[196] Följande exempel illustrerar tankesättet.

Exempel: I målet *Europeiska kommissionen mot Tyskland*[197] hade Europeiska kommissionen begärt att EU-domstolen skulle förklara att Tyskland på ett felaktigt sätt hade införlivat kraven på ”fullständigt oberoende” för tillsynsmyndigheterna som är ansvariga för att säkerställa uppgiftsskydd, och därmed åsidosatt sin skyldighet enligt artikel 28.1 i dataskyddsdirektivet. Enligt kommissionens uppfattning var problemet att Tyskland ställt de myndigheter som ansvarar för att övervaka behandlingen av personuppgifter inom den icke-offentliga sektorn under statligt ansvar, i de olika förbundsländerna (*Länder*).

194 Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, EGT L 8, 12.1.2001, artiklarna 41–48.

195 Dataskyddsdirektivet, artikel 28.1, sista meningen, konvention 108, tilläggsprotokoll, artikel 1.3.

196 Se FRA (2010), *Grundläggande rättigheter: utmaningar och resultat 2010*, årsrapport 2010, s. 59. FRA tog upp frågan i större utsträckning i sin rapport *Data protection in the European Union: the role of National Data Protection Authorities* (Personuppgiftsskydd inom EU: nationella dataskyddsmyndigheters roll), som offentliggjordes i maj 2010.

197 EU-domstolens dom av den 9 mars 2010 i mål C-518/07, *Europeiska kommissionen mot Förbundsrepubliken Tyskland*, punkt 27.

Bedömningen av innehållet i åtgärden berodde enligt domstolen på omfattningen av kravet på oberoende i den bestämmelsen och därför på dess tolkning.

Domstolen underströk att orden ”med fullständigt oberoende” i artikel 28.1 i direktivet måste tolkas baserat på faktisk lydelse i den bestämmelsen och på målen och systemen i dataskyddsdirektivet.[198] Domstolen betonade att tillsynsmyndigheterna är ”väktare” av rättigheterna kopplade till behandlingen av personuppgifter som säkerställs i direktivet, och att deras inrättande i medlemsstaterna därför anses vara ”av avgörande betydelse för skyddet av enskilda personer med avseende på behandlingen av personuppgifter.”[199] Domstolen drog slutsatsen att ”tillsynsmyndigheterna i utövande av sina uppgifter måste kunna handla objektivt och opartiskt. De får för detta ändamål inte vara utsatta för någon påverkan utifrån. Detta gäller inte bara påverkan från de organ som är föremål för övervakning, utan även, direkt eller indirekt, från staten eller förbundsländerna *(Länder)*”.[200]

EU-domstolen fann även att betydelsen av ”fullständigt oberoende” bör tolkas mot bakgrund av Europeiska datatillsynsmannens oberoende enligt definitionen i dataskyddsförordningen. Såsom understryks av domstolen klargörs i artikel 44.2 i denna förordning begreppet oberoende genom att tillägga att Europeiska datatillsynsmannen vid utförandet av sina skyldigheter inte får be om eller få instruktioner från någon. Detta utesluter statlig tillsyn från en oberoende tillsynsmyndighet för skydd av personuppgifter.[201]

EU-domstolen ansåg därför att de tyska dataskyddsinstitutionerna i de förbundsländer som är ansvariga för att övervaka de icke statliga organens behandling av personuppgifter inte var tillräckligt oberoende eftersom de omfattas av statens tillsyn.

Exempel: I målet *Europeiska kommissionen mot Österrike*[202] belyste EU-domstolen liknande problem rörande vissa medlemmars och anställdas ställning i den österrikiska dataskyddsmyndigheten (DSK). Domstolen drog i

198 *Ibid*, punkterna 17 och 29.

199 *Ibid.*, punkt 23.

200 *Ibid.*, punkt 25.

201 *Ibid.*, punkt 27.

202 EU-domstolen, C-614/10, *Europeiska kommissionen mot Republiken Österrike*, 16 oktober 2012, punkterna 59 och 63.

detta fall slutsatsen att österrikisk lagstiftning hindrade den österrikiska dataskyddsmyndigheten från att utöva sina funktioner fullständigt oberoende i den mening som avses i dataskyddsdirektivet. Österrikiska DPA:s oberoende var inte tillräckligt tryggat, eftersom det federala kansliet stödjer DSK med arbetskraft, har tillsyn över DSK och har rätt att när som helst få information om dess arbete.

Exempel: I målet *Europeiska kommissionen mot Ungern*[203] påpekade EU-domstolen att ”kravet […] enligt vilket tillsynsmyndigheterna ska utöva de uppgifter som åläggs dem fullständigt oberoende, innebär att den berörda medlemsstaten är skyldig att respektera en sådan myndighets mandattid ända fram till den ursprungligen föreskrivna tidpunkten”. Domstolen ansåg även att Ungern har ”underlåtit att uppfylla sina skyldigheter enligt direktiv 95/46/EG genom att avsluta datatillsynsmyndighetens mandat i förtid […].”

Tillsynsmyndigheter har enligt nationell lag befogenheter och kapacitet att:[204]

- ge råd till registeransvariga och registrerade om alla frågor som rör dataskydd;
- undersöka behandling och ingripa vid behov;
- varna eller tillrättavisa registeransvariga;
- begära ändring, blockering, radering eller förstörelse av uppgifter;
- införa ett tillfälligt eller definitivt förbud mot behandling;
- hänvisa ärendet till domstol.

För att utöva sina befogenheter måste en tillsynsmyndighet ha tillgång till alla personuppgifter och all information som krävs för en utredning, liksom tillgång till eventuella lokaler där en registeransvarig förvarar relevant information.

Det är avsevärda skillnader mellan inhemsk jurisdiktion som hänför sig till förfarandena och de rättsliga effekterna av en tillsynsmyndighets resultat. Det kan röra sig om alltifrån ombudsmannaliknande rekommendationer till omedelbart verkställbara

203 EU-domstolen, C-288/12, *Europeiska kommissionen mot Ungern*, 8 april 2014, punkterna 50 och 67.

204 Dataskyddsdirektivet, artikel 28, se vidare konvention 108, tilläggsprotokoll, artikel 1.

beslut. Vid analys av hur effektiva de prövningar är som är tillgängliga inom en jurisdiktion måste prövningsinstrumentet bedömas i sitt sammanhang.

5.3. Prövning och sanktioner

Viktiga punkter

- Enligt konvention 108 och dataskyddsdirektivet måste nationell lag innehålla lämpliga prövningar och sanktioner mot överträdelser av rätten till skydd av personuppgifter.
  - Rätten till effektiv prövning kräver enligt EU-lagstiftningen att nationell lag anger rättsliga prövningar mot överträdelser av dataskyddsrättigheter, oberoende av möjligheten att vända sig till en tillsynsmyndighet.
  - Sanktioner ska anges i nationell lag och ska vara effektiva, likvärdiga, proportionerliga och avvärjande.
- Innan någon vänder sig till domstol måste personen först kontakta en registeransvarig. Huruvida det även är obligatoriskt att kontakta en tillsynsmyndighet innan man vänder sig till domstolen avgörs i nationell lag.
- De registrerade kan som en sista utväg och under vissa villkor ta överträdelser av dataskyddslagstiftning till Europadomstolen.
- De registrerade kan dessutom kontakta EU-domstolen, men endast i mycket begränsad utsträckning.

Rättigheter enligt dataskyddslagstiftningen kan utövas endast av den person vars rättigheter står på spel. Detta är någon som är, eller åtminstone hävdar att han eller hon är, den registrerade. Dessa personer kan representeras i utövandet av sina rättigheter av personer som, enligt nationell lagstiftning, uppfyller de nödvändiga kraven. Minderåriga måste företrädas av sina föräldrar eller vårdnadshavare. Inför tillsynsmyndigheterna kan en person även företrädas av föreningar vars tillåtna syfte är att främja dataskyddsrättigheter.

5.3.1. Begäran till den registeransvariga

Rättigheter som anges i avsnitt 3.2 måste först utövas gentemot den registeransvariga. Att kontakta den nationella tillsynsmyndigheten eller en domstol direkt skulle inte hjälpa, eftersom domstolen endast kan ge rådet att den registeransvariga först måste kontaktas, och domstolen skulle anse en ansökan otillåtlig. De formella

kraven för en juridiskt relevant begäran till en registeransvarig, särskilt huruvida det inte behöver vara en skriftlig begäran, bör regleras i nationell lag.

Den enhet som kontaktades som registeransvarig måste reagera på en begäran även om enheten inte är den registeransvariga. Ett svar måste i vilket fall som helst lämnas till den registrerade inom den tidsgräns som anges i nationell lag, även om det endast innebär att inga uppgifter behandlas om frågeställaren. I enlighet med bestämmelserna i artikel 12 a i dataskyddsdirektivet och artikel 8 b i konvention 108 ska begäran hanteras ”utan större tidsutdräkt”. I nationell lag bör därför föreskrivas en svarsperiod som är tillräckligt kort men som ändå gör det möjligt för den registeransvariga att hantera begäran på lämpligt sätt.

Innan begäran besvaras måste den enhet som kontaktats i sin egenskap av registeransvarig fastställa frågeställarens identitet för att avgöra om han eller hon verkligen är den person han eller hon utger sig för att vara, och på så sätt undvika en allvarlig överträdelse av sekretessen. Om kraven för att fastställa identiteten inte regleras specifikt i nationell lag måste de fastställas av den registeransvariga. Principen om rättvis behandling kräver emellertid att registeransvariga inte föreskriver alltför betungande villkor för att fastställa identifiering (och autenticiteten i begäran enligt diskussionen i avsnitt 2.1.1).

Nationell lagstiftning måste även hantera frågan om huruvida registeransvariga kan kräva att frågeställaren betalar en avgift innan en begäran besvaras: I artikel 12 a i direktivet och artikel 8 b i konvention 108 föreskrivs att svaret på en begäran om tillgång måste lämnas ”utan större […] kostnader”. I nationell lag i många europeiska länder föreskrivs att begäran enligt dataskyddslagen ska besvaras kostnadsfritt, så länge som svaret inte orsakar alltför stor eller ovanlig ansträngning. Registeransvariga är i sin tur skyddade av nationell lag mot missbruk av rätten att erhålla svar på sin begäran.

Om personen, institutionen eller organet som kontaktas i egenskap av registeransvarig inte förnekar att den är registeransvarig, ska enheten inom den tidsram som föreskrivs i nationell lag:

- antingen gå med på begäran och meddela frågeställaren hur begäran uppfylldes; eller

- informera frågeställaren om varför hans eller hennes begäran inte kommer att uppfyllas.

5.3.2. Klagomål lämnade till tillsynsmyndigheten

Om en person som lämnat en begäran om tillgång eller har framfört en invändning till en registeransvarig inte får ett svar i tid som är tillfredsställande kan personen kontakta den nationella tillsynsmyndigheten för skydd av personuppgifter och begära stöd. Under förhandlingarna vid tillsynsmyndigheten bör det klargöras huruvida personen, institutionen eller organet som kontaktats av frågeställaren verkligen var skyldig att reagera på begäran om huruvida reaktionen var korrekt och tillräcklig. Den berörda personen måste informeras av tillsynsmyndigheten om resultatet av förhandlingarna om överklagandet.[205] De rättsliga effekterna av resultatet av förhandlingarna vid en nationell tillsynsmyndighet beror på nationell lag: huruvida myndighetens beslut kan verkställas lagligt, vilket innebär att de kan verkställas av en officiell myndighet, eller huruvida det är nödvändigt att vända sig till en domstol om den registeransvariga inte följer tillsynsmyndighetens beslut (yttrande, varning etc.).

I den händelse dataskyddsrättigheter som garanteras enligt artikel 16 i EUF-fördraget påstås överträdas av EU:s institutioner eller organ kan den registrerade lämna in ett klagomål till Europeiska datatillsynsmannen[206], den oberoende tillsynsmyndigheten för dataskydd enligt dataskyddsförordningen som innehåller datatillsynsmannens skyldigheter och befogenheter. I avsaknad av ett svar från Europeiska datatillsynsmannen inom sex månader ska klagomålet anses ha avvisats.

Det måste finnas möjlighet att överklaga en nationell tillsynsmyndighets beslut i domstol. Detta gäller för den registrerade såväl som för registeransvariga eftersom de är part i förhandlingarna vid en tillsynsmyndighet.

Exempel: Förenade kungarikets dataskyddsmyndighet utfärdade ett beslut den 24 juli 2013 och bad Hertfordshires polis att sluta använda ett system för att spåra registreringsskyltar som den bedömde som otillåtet. De uppgifter som samlades in av kameror lagrades både i den lokala polisens databaser och i en central databas. Foton av registreringsskyltar lagrades i två år och foton av bilar i 90 dagar. En så omfattande användning av kameror och andra former av övervakning ansågs inte stå i proportion till det problem man försökte lösa.

205 Dataskyddsdirektivet, artikel 28.4.

206 Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, EGT L 8, 12.1.2001, s. 1.

5.3.3. Överklagande till domstol

Enligt dataskyddsdirektivet har en person som lämnat en begäran enligt dataskyddslagen till en registeransvarig och inte är nöjd med den registeransvarigas svar rätt att överklaga till en nationell domstol.[207]

Huruvida det är obligatoriskt att kontakta en tillsynsmyndighet först, innan man vänder sig till domstolen, avgörs i nationell lag. I de flesta fall är det emellertid en fördel för personer som utövar sina rättigheter till dataskydd, att kontakta tillsynsmyndigheten först eftersom förhandlingar om begäran om deras stöd bör vara obyråkratiskt och kostnadsfritt. De expertkunskaper som dokumenteras i tillsynsmyndighetens beslut (yttrande, varning etc.) kan även hjälpa den registrerade att hävda sina rättigheter inför domstolen.

Enligt Europarådets lagstiftning kan överträdelser av dataskyddsrättigheter, som påstås utövade på nationell nivå av en avtalspart till Europakonventionen, och som samtidigt utgör en överträdelse av artikel 8 i Europakonventionen, dessutom tas upp i Europadomstolen efter att alla inhemska möjligheter har uttömts. För att överträdelse av artikel 8 i Europakonventionen ska kunna hävdas vid Europadomstolen måste också andra kriterier om tillåtlighet vara uppfyllda (artiklarna 34–37 i Europakonventionen).[208]

Även om klagomål till Europadomstolen kan ske endast mot avtalsparter kan de också indirekt handla om åtgärder eller underlåtenheter från privata parter, om en avtalspart inte har uppfyllt sina positiva skyldigheter enligt Europakonventionen och inte tillhandahållit tillräckligt skydd mot överträdelser av dataskyddsrättigheter i sin nationella lagstiftning.

> Exempel: I målet *K.U. mot Finland*[209] hävdade den klagande, en minderårig, att en annons av sexuell art hade lagts upp om honom på en dejtingsajt på internet. Identiteten på den person som hade lagt upp informationen avslöjades inte av tjänsteleverantören på grund av skyldigheten till sekretess enligt finsk lag. Den klagande hävdade att den finska lagen inte erbjöd tillräckligt skydd mot åtgärder när en privatperson lägger ut komprometterande uppgifter om

207 Dataskyddsdirektivet, artikel 22.

208 Europakonventionen, artikel 34–37, tillgänglig på www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 Europadomstolen, *K.U. mot Finland*, nr 2872/02, 2 december 2008.

den klagande på internet. Europadomstolen hävdade att staterna inte bara var tvungna att avstå från godtyckligt ingripande i enskildas privatliv, utan att de också kan omfattas av positiva skyldigheter som innefattar ”att införa åtgärder i syfte att garantera respekten för privatlivet, till och med inom ramen för fysiska personers förhållanden gentemot varandra.” I den klagandes fall krävdes för ett praktiskt och effektivt skydd att faktiska åtgärder skulle vidtas för att identifiera och åtala förövaren. Detta skydd erbjöds emellertid inte av staten och domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Exempel: I målet *Köpke mot Tyskland*[210] hade den klagande misstänkts för stöld på sin arbetsplats och omfattades därför av hemlig videoövervakning. Europadomstolen drog slutsatsen att inget tydde på att de inhemska myndigheterna hade underlåtit att uppnå en korrekt balans inom manöverutrymmet mellan den klagandes rätt till respekt för sitt privatliv, enligt artikel 8, och både hennes arbetsgivares intressen i att skydda sina egendomsrättigheter och det offentliga intresset av korrekt hantering av rättvisan. Ansökan förklarades därför otillåtlig.

Om Europadomstolen anser att en stat har överträtt någon av rättigheterna som skyddas i Europakonventionen är den staten skyldig att verkställa Europadomstolens dom. Verkställandeåtgärder måste först sätta stopp för överträdelsen och så långt det är möjligt åtgärda dess negativa konsekvenser för den klagande. Verkställande av domar kan även kräva allmänna åtgärder för att förebygga överträdelser liknande de som domstolen funnit, oavsett om det sker genom ändring av lagstiftningen, rättspraxis eller andra åtgärder.

Om Europadomstolen anser att Europakonventionen har överträtts föreskrivs i artikel 41 i Europakonventionen att den klagande kan tillerkännas skälig gottgörelse.

Enligt EU:s lagstiftning[211] kan offer för överträdelser av nationell dataskyddslagstiftning, som genomför EU:s dataskyddslagstiftning, i vissa fall ta sitt ärende till EU-domstolen. Det finns två möjliga scenarier för hur en registrerads klagomål om att hans eller hennes dataskyddsrättigheter har överträtts kan leda till förhandlingar inför EU-domstolen.

210 Europadomstolen, *Köpke mot Tyskland* (beslut), nr 420/07, 5 oktober 2010.

211 EU (2007), Lissabonfördraget om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, undertecknat i Lissabon den 13 december 2007, EUT C 306, 17.12.2007. Se även de konsoliderade versionerna av fördraget om Europeiska unionen, EUT C 326, 26.10.2012, s. 13, och fördraget om Europeiska unionens funktionssätt, EUT C 326, 26.10.2012, s. 47.

I det första scenariot behöver den registrerade vara det direkta offret för en administrativ eller juridisk handling inom EU som innebär överträdelse av den enskildas rätt till uppgiftsskydd. Så här står det i artikel 263.4 i EUF-fördraget:

> *”Alla fysiska eller juridiska personer får [...] väcka talan mot en akt som är riktad till dem eller som direkt och personligen berör dem samt mot en regleringsakt som direkt berör dem och som inte medför genomförandeåtgärder.”*

Offer för en otillåten behandling av deras uppgifter inom ett EU-organ kan därför överklaga direkt till tribunalen, som är det organ som har behörighet att döma i frågor som gäller dataskyddsförordningen. Möjligheten att klaga direkt till EU-domstolen finns, även om någons juridiska situation direkt påverkas av en av EU:s rättsliga bestämmelser.

Det andra scenariot gäller EU-domstolens behörighet att lämna ett förhandsavgörande enligt artikel 267 i EUF-fördraget.

Registrerade kan under ett inhemskt förfarande be den nationella domstolen att begära klargörande från EU-domstolen om tolkningen av EU-fördragen och om tolkningen och giltigheten i handlingar från EU:s institutioner, organ, kontor eller byråer. Dessa klargöranden kallas förhandsavgöranden. Det är inte en direkt prövning för den klagande men gör det möjligt för nationella domstolar att säkerställa att de tolkar EU-lagstiftningen korrekt.

Om en part i förhandlingarna vid de nationella domstolarna kräver att en fråga ska hänvisas till EU-domstolen är endast de nationella domstolar som fungerar som sista instans, mot vars beslut det inte finns någon rättslig prövning, skyldiga att följa uppmaningen.

Exempel: I målet *Kärntner Landesregierung m.fl.*[212] ställde den österrikiska författningsdomstolen frågor till EU-domstolen rörande giltigheten i artiklarna 3–9 i direktiv 2006/24/EG (*datalagringsdirektivet*) mot bakgrund av artiklarna 7, 9 och 11 i stadgan och huruvida vissa bestämmelser i den österrikiska federala lagen om telekommunikationer, som införlivar datalagringsdirektivet, var oförenliga med aspekter i dataskyddsdirektivet och dataskyddsförordningen.

212 EU-domstolen, förenade målen C-293/12 och C-594/12, *Digital Rights Irland och Seitling m.fl.*, 8 april 2014.

Seitlinger, en av de klagande i författningsdomstolens förhandlingar, ansåg att han använder telefon, internet och e-post både i sitt arbete och i sitt privatliv. Informationen som han sänder och tar emot passerar därför offentliga telekommunikationsnätverk. Enligt den österrikiska telekommunikationslagen från 2003 är hans telekommunikationsleverantör juridiskt skyldig att samla in och lagra uppgifter om hans användning av nätverket. Seitlinger insåg att denna insamling och lagring av hans personuppgifter inte på något sätt var nödvändiga för det tekniska syftet att förflytta informationen från A till B i nätverket. Inte heller var insamling och lagring av dessa uppgifter ens på avstånd nödvändiga i faktureringssyfte. Seitlinger hade definitivt inte samtyckt till denna användning av hans personuppgifter. Det enda skälet till att samla in och lagra alla dessa extra uppgifter var den österrikiska telekommunikationslagen från 2003.

Seitlinger vände sig därför till den österrikiska författningsdomstolen där han hävdade att hans telekommunikationsleverantörs lagenliga skyldigheter innebar överträdelse av hans grundläggande rättigheter enligt artikel 8 i EU-stadgan.

EU-domstolen fattar beslut endast om de beståndsdelar som ingår i begäran om förhandsavgörande som hänvisats till domstolen. De nationella domstolarna är fortfarande behöriga att fatta beslut i det ursprungliga målet.

I princip måste EU-domstolen besvara de frågor den tar emot. Den kan inte vägra att lämna ett förhandsavgörande på grund av att svaret varken skulle vara relevant eller i tid när det gäller det ursprungliga målet. Domstolen kan emellertid vägra om frågan inte hör till dess kompetensområde.

Om slutligen en EU-institution eller ett EU-organ vid behandling av personuppgifter påstås överträda dataskyddsrättigheter som garanteras genom artikel 16 i EUF-fördraget, kan den registrerade ta målet till EU-domstolens tribunal (artikel 32.1 och 32.4 i dataskyddsförordningen). Detsamma gäller Europeiska datatillsynsmannens beslut rörande dessa överträdelser (artikel 32.3 i dataskyddsförordningen).

Samtidigt som EU-domstolens tribunal är behörig att döma i frågor som rör dataskyddsförordningen, måste en person som är anställd vid en EU-institution eller ett EU-organ och vill överklaga vända sig till personaldomstolen.

Exempel: Målet *Europeiska kommissionen mot The Bavarian Lager Co. Ltd*[213] illustrerar de prövningar som är tillgängliga mot åtgärder och beslut inom EU-institutioner och EU-organ som rör skydd av personuppgifter.

Bavarian Lager begärde av Europeiska kommissionen tillgång till det fullständiga protokollet från ett möte som hållits av kommissionen och som sades ha gällt juridiska frågor som var relevanta för företaget. Kommissionen hade avvisat företagets begäran om tillgång för att det åsidosatte dataskyddsintressen.[214] Mot detta beslut hade Bavarian Lager, genom tillämpning av artikel 32 i dataskyddsförordningen, lämnat ett klagomål till EU-domstolen, mer exakt till förstainstansrätten (föregångaren till tribunalen). I sitt beslut i mål T194/04, *Bavarian Lager mot kommissionen*, upphävde förstainstansrätten kommissionens beslut att avvisa begäran om tillgång till handlingarna. Europeiska kommissionen överklagade beslutet till EU-domstolen. EU-domstolen dömde (i stora avdelningen) och upphävde domen från förstainstansrätten och bekräftade Europeiska kommissionens avvisande av begäran om tillgång.

5.3.4. Sanktioner

I Europarådets lagstiftning föreskrivs i artikel 10 i konvention 108 att lämpliga sanktioner och prövningar måste ske av alla parter vid överträdelser av bestämmelser i inhemsk lag som verkställer de grundläggande principerna i dataskyddet som anges i konvention 108.[215] **I EU-lagstiftningen** anges i artikel 24 i dataskyddsdirektivet att medlemsstaterna ”skall anta lämpliga bestämmelser för att säkerställa att detta direktiv genomförs fullständigt och skall särskilt besluta om de sanktioner som skall användas vid överträdelse av de bestämmelser som antagits […]”.

Båda instrumenten ger medlemsstaterna ett stort manöverutrymme när det gäller att välja lämpliga sanktioner och prövningar. Inget av instrumenten erbjuder särskild ledning om arten eller typen av lämpliga sanktioner och de ger heller inga exempel på sanktioner.

213 EU-domstolen, C-28/08 P, *Europeiska kommissionen mot The Bavarian Lager Co. Ltd*, 29 juni 2010.

214 För en analys av argumentet, se Europeiska datatillsynsmannen (2011), *Allmänhetens tillgång till handlingar som innehåller personuppgifter efter Bavarian Lager domen*, Bryssel, Europeiska datatillsynsmannen, tillgänglig på: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

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

Emellertid hävdar FRA att:

> *”även om EU:s medlemsstater har ett manöverutrymme när det gäller att fastställa vilka åtgärder som är lämpligast för att garantera enskildas rättigheter enligt EU-lagstiftningen, i linje med principen om lojalt samarbete som fastställs i artikel 4.3 i EU-fördraget, bör minimikraven på effektivitet, likvärdighet, proportionalitet och avskräckande effekt respekteras.”*[216]

EU-domstolen har upprepade gånger vidhållit att nationell lag inte är fullständigt fri att fastställa sanktioner.

Exempel: I målet *Von Colson och Kamann mot Land Nordrhein-Westfalen*[217] påpekade EU-domstolen att alla medlemsstater till vilka direktivet vände sig är skyldiga att i sina nationella rättssystem anta alla nödvändiga åtgärder för att säkerställa att det är fullt verksamt, i enlighet med målsättningarna. Domstolen ansåg att även om det är upp till medlemsstaterna att välja vägar och sätt att säkerställa att ett direktiv införlivas, påverkar den friheten inte skyldigheten som åligger dem. En effektiv rättslig prövning måste göra det möjligt för den enskilda att fortsätta och genomdriva rättigheten i fråga i dess fulla faktiska omfattning. I syfte att uppnå detta verkliga och effektiva skydd måste rättsliga prövningar leda till sanktioner som har en avskräckande effekt.

När det gäller sanktioner mot EU-institutionernas och EU-organens överträdelser av EU-lagstiftningen sker sanktioner endast i form av disciplinära åtgärder, på grund av de särskilda befogenheterna i dataskyddsförordningen. I artikel 49 i förordningen föreskrivs att ”om en tjänsteman eller annan anställd vid Europeiska gemenskaperna inte uppfyller de förpliktelser som åligger dem enligt denna förordning, avsiktligt eller på grund av försumlighet, skall denne bli föremål för disciplinära åtgärder […]”.

216 FRA (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 och Elisabeth Kamann mot Land Nordrhein-Westfalen*, 10 april 1984.

6

Gränsöverskridande flöden av personuppgifter

EU	Frågor som täcks	Europarådet
Gränsöverskridande flöden av personuppgifter		
Dataskyddsdirektivet, artikel 25.1 EU-domstolens dom av den 6 november 2003 i mål C-101/01, *Bodil Lindqvist*	**Definition**	Konvention 108, tilläggsprotokoll, artikel 2.1
Fritt flöde av uppgifter		
Dataskyddsdirektivet, artikel 1.2	**Mellan EU-stater**	
	Mellan avtalsparter till konvention 108	Konvention 108, artikel 12.2
Dataskyddsdirektivet, artikel 25	**Till tredjeländer med lämplig nivå av dataskydd**	Konvention 108, tilläggsprotokoll, artikel 2.1
Dataskyddsdirektivet, artikel 26.1	**Till tredjeländer i särskilda fall**	Konvention 108, tilläggsprotokoll, artikel 2.2 a
Begränsat flöde av uppgifter till tredjeländer		
Dataskyddsdirektivet, artikel 26.2 Dataskyddsdirektivet, artikel 26.4	**Avtalsklausuler**	Konvention 108, tilläggsprotokoll, artikel 2.2. b Riktlinjer för utarbetande av avtalsklausuler
Dataskyddsdirektivet, artikel 26.2	**Bindande företagsregler**	
Exempel: Avtal mellan EU och USA om passageraruppgifter Avtal mellan EU och USA om SWIFT	**Särskilda internationella avtal**	

Dataskyddsdirektivet föreskriver inte bara fritt flöde av uppgifter mellan medlemsstaterna utan innehåller också bestämmelser om kraven vid överföring av personuppgifter till tredjeländer utanför EU. Europarådet erkänner också betydelsen av att genomföra regler för gränsöverskridande uppgiftsflöden till tredjeländer och antog 2001 tilläggsprotokollet till konvention 108. I protokollet överfördes det viktigaste laginnehållet om gränsöverskridande flöden av personuppgifter från avtalsparterna och EU:s medlemsstater.

6.1. Typ av gränsöverskridande flöde av personuppgifter

Viktiga punkter

- Gränsöverskridande flöde av personuppgifter är en överföring av personuppgifter till en mottagare som omfattas av utländsk jurisdiktion.

I artikel 2.1 i tilläggsprotokollet till konvention 108 beskrivs gränsöverskridande flöde av personuppgifter som överföring av personuppgifter till en mottagare som omfattas av en utländsk jurisdiktion. I artikel 25.1 i dataskyddsdirektivet regleras ”överföringen av personuppgifter som är under behandling eller som är avsedda att behandlas efter överföring […]”. Denna överföring av uppgifter är tillåten endast enligt reglerna i artikel 2 i tilläggsprotokollet till konvention 108 och för EU:s medlemsstater, dessutom i artiklarna 25 och 26 i dataskyddsdirektivet.

Exempel: I målet *Bodil Lindqvist*[218] ansåg EU-domstolen att ”omnämnandet av olika personer – vilka identifieras med namn eller på annat sätt, till exempel med telefonnummer eller med uppgifter om deras arbetsförhållanden och fritidsintressen – på en webbsida utgör en ’behandling av personuppgifter som helt eller delvis företas på automatisk väg’, i den mening som avses i artikel 3.1 i direktiv 95/46.”

Domstolen påpekade sedan att direktivet också innehåller specifika regler avsedda att göra det möjligt för medlemsstater att övervaka överföringen av personuppgifter till tredjeländer.

218 EU-domstolen, C-101/01, *Bodil Lindqvist*, 6 november 2003, punkterna 27, 68 och 69.

Med tanke för det första på internets utveckling vid den tidpunkt när direktivet utarbetades och för det andra på avsaknaden i direktivet av kriterier tillämpliga på användningen av internet ”kan det inte presumeras att gemenskapslagstiftaren hade för avsikt att med tanke på framtiden låta utläggning av uppgifter på en webbsida av en person [...] omfattas av begreppet ’överföring [av uppgifter] till tredje land’, även om dessa uppgifter härigenom blir åtkomliga för de personer i tredje land som har tekniska möjligheter att få tillgång till sidan.”

Om direktivet däremot ”tolkades på så sätt att det förelåg en överföring av uppgifter till tredje land varje gång personuppgifter lades ut på en webbsida skulle denna överföring med nödvändighet vara en överföring till alla tredje länder där det fanns de tekniska medel som krävs för att få tillgång till internet. Särregleringen [i direktivet] skulle då med nödvändighet, vad gäller åtgärder som vidtas på internet, bli en generellt tillämplig ordning. Om kommissionen konstaterade [...] att det fanns ett enda tredje land som inte säkerställde en adekvat skyddsnivå skulle medlemsstaterna nämligen enligt en sådan tolkning vara skyldiga att hindra att personuppgifter över huvud taget lades ut på internet.”

Principen att endast offentliggörande av (person)uppgifter inte ska betraktas som gränsöverskridande flöde av personuppgifter gäller även för offentliga register på nätet eller massmedia, exempelvis (elektroniska) dagstidningar och tv. Endast kommunikation som är riktad till specifika mottagare kan omfattas av begreppet ”gränsöverskridande flöde av personuppgifter”.

6.2. Fritt flöde av personuppgifter mellan medlemsstater eller mellan avtalsparter

Viktiga punkter

- Överföring av personuppgifter till en annan medlemsstat i Europeiska ekonomiska samarbetsområdet eller till en annan avtalspart till konvention 108 får inte omfattas av restriktioner.

Enligt artikel 12.2 i konvention 108 måste det **enligt Europarådets lagstiftning** finnas ett fritt flöde av personuppgifter mellan parterna till konventionen. Inhemsk lag får inte begränsa exporten av personuppgifter till en avtalspart med mindre än att:

- uppgifternas särskilda art kräver det;[219] eller
- begränsningen är nödvändig för att undvika att inhemska rättsliga bestämmelser om gränsöverskridande flöde av personuppgifter till tredje part kringgås.[220]

Enligt EU-lagstiftningen är begränsningar eller förbud när det gäller fritt flöde av uppgifter mellan medlemsstater av dataskyddsskäl förbjudet enligt artikel 1.2 i dataskyddsdirektivet. Området för fritt uppgiftsflöde har utvidgats genom avtalet om det europeiska ekonomiska samarbetsområdet (EES),[221] som innebär att Island, Liechtenstein och Norge ingår i den inre marknaden.

Exempel: Om en filial till en internationell koncern av företag som är etablerad i flera av EU:s medlemsstater, däribland Slovenien och Frankrike, överför personuppgifter från Slovenien till Frankrike får dessa flöden av personuppgifter inte begränsas eller förbjudas av slovensk nationell lag.

Om emellertid samma slovenska filial vill överföra samma personuppgifter till moderbolaget i Förenta staterna måste den slovenska uppgiftsexportören gå via de bestämmelser som fastställts i slovensk lag för gränsöverskridande flöde av personuppgifter till tredjeländer utan lämpligt uppgiftsskydd, om inte moderbolaget hade anslutit sig till principerna om integritetsskydd (Safe Harbor Privacy Principles), en frivillig uppförandekod för att erbjuda en lämplig nivå av uppgiftsskydd (se avsnitt 6.3.1).

Gränsöverskridande flöden av personuppgifter till medlemsstater i EES för syften utanför den inre marknadens ansvarsområde, exempelvis utredning av brott, omfattas emellertid inte av bestämmelserna i dataskyddsdirektivet och därför inte heller av principerna om fritt flöde av uppgifter. När det gäller Europarådets lagstiftning omfattas alla områden av konvention 108 och tilläggsprotokollet till konvention 108, även om de avtalsslutande parterna kan göra undantag. Samtliga medlemmar i EES är också parter till konvention 108.

219 Konvention 108, artikel 12.3 a.

220 *Ibid.*, artikel 12.3 b.

221 Rådets och kommissionens beslut av den 13 december 1993 om ingående av avtalet om Europeiska ekonomiska samarbetsområdet mellan Europeiska gemenskaperna, deras medlemsstater och Finland, Island, Liechtenstein, Norge, Schweiz, Sverige och Österrike, EGT L 1, 3.1.1994, s. 1.

6.3. Fritt flöde av uppgifter till tredjeländer

Viktiga punkter

- Överföring av personuppgifter till tredjeländer ska inte omfattas av begränsningar enligt nationell dataskyddslagstiftning om:
  - korrekt dataskydd hos mottagaren har fastställts; eller
  - det är nödvändigt i de registrerades specifika intressen eller berättigade rådande intressen hos andra, särskilt viktiga offentliga intressen.
- Korrekt dataskydd i ett tredjeland innebär att huvudprinciperna för dataskydd effektivt har införlivats i nationell lag i det landet.
- Enligt EU-lagstiftningen bedöms korrekt dataskydd i ett tredjeland av Europeiska kommissionen. Enligt Europarådets lagstiftning är det inhemsk lag som reglerar hur korrektheten bedöms.

6.3.1. Fritt flöde av uppgifter på grund av lämpligt skydd

Enligt Europarådets lagstiftning är det tillåtet att enligt inhemsk lag möjliggöra fritt flöde av personuppgifter till stater som inte är parter i avtalet, om den mottagande staten eller organisationen säkerställer lämplig nivå av skydd för den avsedda överföringen av uppgifter.[222] I inhemsk lag beslutas hur nivån av uppgiftsskydd ska bedömas i ett annat land och vem som bör bedöma det.

Enligt EU:s lagstiftning medges fritt flöde av uppgifter till tredjeländer med lämplig nivå av uppgiftsskydd enligt artikel 25.1 i dataskyddsdirektivet. Kravet på lämplighet snarare än motsvarighet gör det möjligt att uppfylla olika sätt att införliva dataskyddet. Enligt artikel 25.6 i direktivet är Europeiska kommissionen behörig att bedöma nivån av dataskydd i andra länder genom en adekvat skyddsnivå och samråder kring bedömningen med artikel 29-gruppen som i stor utsträckning har bidragit till tolkningen av artikel 25 och 26.[223]

222 Konvention 108, tilläggsprotokoll, artikel 2.1

223 Se exempelvis artikel 29-gruppen (2003), *Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers*, WP 74, Bryssel, 3 juni 2003, och artikel 29-gruppen (2005), *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, WP 114, Bryssel, 25 november 2005.

En adekvat skyddsnivå från Europeiska kommissionen är bindande. Om Europeiska kommissionen offentliggör en adekvat skyddsnivå för ett visst land i *Europeiska unionens officiella tidning* är alla medlemsländer i EES och deras organ skyldiga att följa beslutet, vilket innebär att uppgifter kan överföras till detta land utan kontroll- eller licensieringsförfaranden vid nationella myndigheter.[224]

Europeiska kommissionen kan också bedöma delar av ett lands rättssystem eller begränsa sig till enskilda ämnen. Kommissionen garanterade exempelvis skyddsnivån enbart rörande Kanadas privata kommersiella lagstiftning.[225] Det finns även flera adekvata skyddsnivåer för överföringar baserade på överenskommelser mellan EU och utländska stater. Dessa beslut hänför sig enbart till en enskild typ av dataöverföring, såsom överföring av passageraruppgifter från flygbolag till utländska gränskontrollmyndigheter när bolaget flyger från EU till vissa utländska destinationer (se avsnitt 6.4.3). Nyare praxis för dataöverföring baserad på särskilda överenskommelser mellan EU och tredjeländer undanröjer i allmänhet behovet av adekvat skyddsnivå och det antas att överenskommelsen i sig erbjuder lämplig nivå av dataskydd.[226]

Ett av de viktigaste besluten om adekvat skydd gäller egentligen inte en uppsättning av rättsliga bestämmelser.[227] Det gäller snarare regler, i stor utsträckning som en uppförandekod, som kallas principerna om integritetsskydd (Safe Harbour Privacy Principles). Principerna utarbetades mellan EU och USA för amerikanska företag. Medlemskap i Safe Harbour uppnås genom frivilligt åtagande inför USA:s handelsministerium och dokumenteras i en förteckning som offentliggörs av ministeriet. Eftersom en av de viktiga beståndsdelarna i en adekvat skyddsnivå är hur effektivt dataskyddet har genomförts, innehåller Safe Harbour Arrangement även

224 För en kontinuerligt uppdaterad förteckning över länder som har fått en adekvat skyddsnivå, se Europeiska kommissionens webbsida, generaldirektoratet för rättsliga frågor, på http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm.

225 Europeiska kommissionen (2002), beslut 2002/2/EG av den 20 december 2001 i enlighet med Europaparlamentets och rådets direktiv 95/46/EG om adekvat skydd för personuppgifter genom den kanadensiska lagen om elektroniska handlingar och skydd för personuppgifter (Personal Information Protection and Electronic Documents Act), EGT 2002 L 2.

226 T.ex. avtalet mellan Amerikas förenta stater och Europeiska unionen om användning och överföring av passageraruppgifter till Förenta staternas *Department of Homeland Security* (EUT 2012, L 215, s. 5–14) eller avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden i enlighet med programmet för att spåra finansiering av terrorism, EUT 2010, L 8, s. 11–16.

227 Europeiska kommissionen (2000), kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (*Safe Harbor Privacy Principles*) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat, EGT 2000 L 215.

ett visst mått av statlig övervakning: endast de företag kan gå med i Safe Harbour som omfattas av övervakning från USA:s Federal Trade Commission.

6.3.2. Fritt flöde av uppgifter i specifika fall

Enligt Europarådets lagstiftning möjliggör artikel 2.2 i tilläggsprotokollet till konvention 108 överföring av personuppgifter till tredjeländer där det inte finns något adekvat dataskydd, under förutsättning att överföringen tillåts enligt inhemsk lag och är nödvändig för:

- den registrerades specifika intressen; eller
- berättigade rådande intressen hos andra, särskilt viktiga offentliga intressen.

I EU:s lagstiftning anges i artikel 26.1 i dataskyddsdirektivet bestämmelser som liknar dem i tilläggsprotokollet till konvention 108.

Enligt direktivet kan den registrerades intressen motivera ett fritt flöde av uppgifter till ett tredjeland om:

- den registrerade ger sitt otvetydiga samtycke till exporten av uppgifterna; eller
- den registrerade träffar – eller förbereder sig för att träffa – ett avtalsförhållande som tydligt kräver att uppgifterna överförs till en mottagare utomlands; eller
- ett avtal mellan en registeransvarig och en tredje part avslutats i den registrerades intresse; eller
- överföringen är nödvändig för att skydda den registrerades grundläggande intressen.
- det gäller överföring av uppgifter från offentliga register. Detta är ett exempel på faktiska intressen hos allmänheten att kunna få tillgång till information som lagras i offentliga register.

Andras berättigade intresse kan motivera fritt gränsöverskridande flöde av uppgifter:[228]

228 Dataskyddsdirektivet, artikel 26.1 d.

- på grund av ett stort allmänintresse, utöver frågor som rör nationell eller offentlig säkerhet, eftersom de inte omfattas av dataskyddsdirektivet; eller

- för att upprätta, utöva eller försvara rättsliga krav.

De fall som hänvisas till ovan måste ses som undantag från regeln att ohämmad överföring av uppgifter till andra länder kräver lämplig nivå av dataskydd i mottagarlandet. Undantag måste alltid tolkas restriktivt. Detta har betonats vid upprepade tillfällen av artikel 29-gruppen i samband med artikel 26.1 i dataskyddsdirektivet, särskilt om samtycke är den grund för överföring av uppgifter som avses.[229] Artikel 29-gruppen har dragit slutsatsen att den allmänna regeln om rättslig betydelse av samtycke också gäller artikel 26.1 i direktivet. Om det exempelvis i samband med arbetsmarknadsförhållanden är oklart om samtycke från de anställda verkligen var ett fritt samtycke kan överföringar av uppgifter inte grundas på artikel 26.1 a i direktivet. I dessa fall gäller artikel 26.2, som kräver att nationella dataskyddsmyndigheter ska utfärda en licens för överföringar av uppgifter.

6.4. Begränsat flöde av personuppgifter till tredjeländer

Viktiga punkter

- Innan uppgifter exporteras till tredjeländer som inte kan utlova en adekvat nivå av dataskydd kan den registeransvariga uppmanas att överlämna det avsedda flödet av personuppgifter för granskning av tillsynsmyndigheten.
- Den registeransvariga som vill exportera uppgifter måste visa två saker under granskningen:
  - att en rättslig grund finns för överföringen av uppgifter till mottagaren; och
  - att åtgärder finns för att säkerställa adekvat skydd av uppgifterna vid mottagandet.
- Åtgärder för att fastställa adekvat skydd av personuppgifterna vid mottagandet kan innefatta:

229 Se särskilt artikel 29-gruppen (2005), *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, WP 114, Bryssel, 25 november 2005.

  - kontraktsmässiga bestämmelser mellan den uppgiftsexporterande registeransvariga och den utländska datamottagaren; eller
  - bindande företagsregler, vanligtvis tillämpliga för överföring av uppgifter inom en multinationell grupp av företag.
- Överföringen av uppgifter till utländska myndigheter kan också styras av särskilda internationella avtal.

Dataskyddsdirektivet och tilläggsprotokollet till konvention 108 gör det möjligt att i inhemsk lag inrätta system för gränsöverskridande flöden av personuppgifter till tredjeländer som inte kan erbjuda en adekvat nivå av uppgiftsskydd, under förutsättning att den registeransvariga har gjort specialarrangemang för att säkerställa garantier för adekvat uppgiftsskydd hos mottagaren och under förutsättning att den registeransvariga kan bevisa detta för en behörig myndighet. Detta krav anges uttryckligen endast i tilläggsprotokollet till konvention 108 men det anses också vara standardförfarande enligt dataskyddsdirektivet.

6.4.1. Avtalsklausuler

Både i **Europarådets lagstiftning** och i **EU-lagstiftningen** nämns avtalsklausuler mellan den dataexporterande registeransvariga och mottagaren i tredjelandet som ett sätt att säkerställa en tillräcklig nivå av uppgiftsskydd hos mottagaren.

På **EU-nivå** har Europeiska kommissionen med stöd av artikel 29-gruppen utvecklat standardavtalsklausuler som officiellt certifierats genom ett kommissionsbeslut som bevis för adekvat uppgiftsskydd.[230] Eftersom kommissionsbeslut är bindande i sin helhet i medlemsstaterna måste de nationella myndigheterna med ansvar för tillsyns av gränsöverskridande flöden av personuppgifter godkänna dessa standardavtalsklausuler i sina förfaranden.[231] Om den uppgiftsexporterande registeransvariga och mottagaren i tredjelandet är överens och undertecknar dessa klausuler bör det därför ge tillsynsmyndigheten tillräckligt med bevis för att adekvata garantier finns.

Förekomsten av standardavtalsklausuler i EU:s rättsliga ram hindrar inte registeransvariga från att formulera andra tillfälliga avtalsklausuler. De måste emellertid erbjuda samma skyddsnivå som i standardavtalsklausulerna. De viktigaste inslagen i standardavtalsklausulerna är följande:

230 Dataskyddsdirektivet, artikel 26.4.

231 EUF-fördraget, artikel 288.

- en klausul om tredjepartsmottagare som gör att de registrerade kan utöva avtalsmässiga rättigheter även om de inte är part i avtalet;

- mottagaren av uppgifter eller importören som godkänner att vara föremål för förfarandet från den uppgiftsexporterande registeransvarigas nationella tillsynsmyndighet och/eller domstolar vid eventuell tvist.

Det finns nu två uppsättningar standardklausuler tillgängliga för överföringar mellan registeransvariga, från vilka den dataexporterande registeransvariga kan välja.[232] För överföringar från registeransvarig till registerförare finns endast en uppsättning standardavtalsklausuler.[233]

Inom **Europarådets lagstiftning** utarbetade den rådgivande kommittén för konvention 108 riktlinjer för utarbetande av avtalsklausuler.[234]

6.4.2. Bindande företagsregler

Multilaterala bindande företagsregler (binding corporate rules, BCR) involverar mycket ofta flera europeiska dataskyddsmyndigheter samtidigt.[235] Utkast till bindande företagsregler måste skickas in tillsammans med de standardiserade ansökningsformulären till ansvarig myndighet för godkännande.[236] Den ansvariga myndigheten kan identifieras utifrån det standardiserade ansökningsformuläret. Myndigheten informerar sedan alla tillsynsmyndigheter i EES medlemsländer där

232 Uppsättning I ingår i bilagan till Europeiska kommissionen (2001), kommissionens beslut 2001/497/EG av den 15 juni 2001 om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt direktiv 95/46/EG, EGT 2001 L 181. Uppsättning II ingår i bilagan till Europeiska kommissionen (2004), kommissionens beslut 2004/915/EG av den 27 december 2004 om ändring av beslut 2001/497/EG om standardavtalsklausuler för överföring av personuppgifter till tredje land, EUT 2004 L 385.

233 Europeiska kommissionen (2010), kommissionens beslut 2010/87/EU av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG, EUT 2010 L 39.

234 Europarådet, rådgivande kommittén för 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* (riktlinjer för utarbetande av avtalsklausuler för skydd av personuppgifter vid överföring av personuppgifter till tredje part som inte omfattas av adekvat nivå av skydd av personuppgifter).

235 Innehållet och strukturen i lämpliga bindande företagsregler förklaras i artikel 29-gruppen (2008), *Working document setting up a framework for the structure of Binding Corporate Rules*, WP 154, Bryssel, 24 juni 2008, och i artikel 29-gruppen (2008), *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules*,WP 153, Bryssel, 24 juni 2008.

236 Artikel 29-gruppen (2007), *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data* , WP 133, Bryssel, 10 januari 2007.

filialer till koncernen är etablerade, även om deras deltagande i förfarandet för utvärdering av bindande företagsregler är frivilligt. Även om det inte är bindande måste alla berörda dataskyddsmyndigheter införliva resultatet av utvärderingen i sina formella licensieringsförfaranden.

6.4.3. Särskilda internationella avtal

EU har slutit specialavtal för två typer av dataöverföring:

Register över passagerarnamn

Passageraruppgifter (PNR) samlas in av lufttrafikföretag under reservationsprocessen och innefattar namn, adress, kreditkortsdetaljer och stolsnummer för flygpassagerare. Enligt amerikansk lag är lufttrafikföretag skyldiga att göra dessa uppgifter tillgängliga för Department of Homeland Security innan avresan. Detta gäller flygresor till eller från Förenta staterna.

För att säkerställa adekvat skydd för passageraruppgifterna i enlighet med bestämmelserna i direktiv 95/46/EG antogs ett ”PNR-paket” [237] år 2004. Paketet innefattar adekvat skydd av behandlingen av uppgifter som genomförs av USA:s Department of Homeland Security (DHS).

Efter att EU-domstolen annullerat PNR-paketet[238] undertecknade EU och Förenta staterna två separata överenskommelser som hade två syften: för det första att åstadkomma en rättslig grund för att lämna ut PNR-uppgifter till de amerikanska myndigheterna och för det andra att inrätta adekvat uppgiftsskydd i mottagarlandet.

Den första överenskommelsen om hur EU-länderna och Förenta staterna delar och förvaltar uppgifter, som undertecknades 2012, hade flera brister och ersattes

237 Rådets beslut 2004/496/EG av den 17 maj 2004 om ingående av ett avtal mellan Europeiska gemenskapen och Amerikas förenta stater om lufttrafikföretags behandling och överföring av passageraruppgifter till Bureau of Customs and Border Protection inom Förenta staternas Department of Homeland Security, EUT 2004 L 183, s. 83, och kommissionens beslut 2004/535/EG av den 14 maj 2004 om adekvat skydd av personuppgifter som finns i Passenger Name Record för flygpassagerare som överförs till Förenta staternas tull- och gränsskyddsmyndighet EUT 2004, L 235, s. 11–22.

238 EU-domstolen, förenade målen C-317/04 och C-318/04, *Europaparlamentet mot Europeiska unionens råd*, 30 maj 2006, punkterna 57, 58 och 59 där domstolen beslutade att både beslutet om adekvat skydd och överenskommelsen om behandling av uppgifter utesluts från direktivet.

samma år med en annan överenskommelse för att skapa bättre rättssäkerhet.[239] Den nya överenskommelsen erbjuder betydande förbättringar. Den begränsar och klargör för vilka syften informationen får användas, såsom allvarliga gränsöverskridande brott och terrorism, och den fastställer den tidsperiod under vilken uppgifter kan lagras: efter sex månader måste uppgifterna avpersonifieras och maskeras. Om uppgifterna skulle användas felaktigt har alla rätt till administrativ och rättslig prövning i enlighet med amerikansk lag. De har också rätt till att få tillgång till sina egna PNR-uppgifter och få rättelse från USA:s Department of Homeland Security, inbegripet möjligheten att radera information som är felaktig.

Överenskommelsen som trädde i kraft den 1 juli 2012 ska gälla i sju år, fram till 2019.

I december 2011 godkände Europeiska unionens råd slutandet av ett uppdaterat avtal mellan EU och Australien om behandling och överföring av PNR-uppgifter.[240] Överenskommelsen mellan EU och Australien om PNR-uppgifter är ytterligare ett steg i EU:s agenda som innefattar globala PNR-riktlinjer[241] om inrättande av ett system[242] för EU-PNR och förhandlingar om avtal med tredjeländer.[243]

Uppgifter om finansiella betalningsmeddelanden

Belgienbaserade Society for Worldwide Interbank Financial Telecommunication (SWIFT) som är registerförare för merparten av de globala pengatransaktionerna från europeiska banker arbetade med ett "speglat" centrum i Förenta staterna

239 Rådets beslut 2012/472/EU av den 26 april 2012 om ingående av avtalet mellan Amerikas förenta stater och Europeiska unionen om användning och överföring av passageraruppgifter till Förenta staternas Department of Homeland Security EUT 2012, L 215, s. 4 Avtalets text bifogas beslutet, EUT 2012 L 215, s. 5–14.

240 Rådets beslut 2012/381/EU av den 13 december 2011 om ingående av avtalet mellan Europeiska unionen och Australien om lufttrafikföretags behandling av passageraruppgifter (PNR) och överföring av dessa till den australiska tull- och gränsbevakningsmyndigheten, EUT 2012 L 186, s. 3. Texten i avtalet, som ersätter ett tidigare avtal från 2008, bifogas beslutet, EUT 2012 L 186, s. 4–16.

241 Se särskilt kommissionens meddelande av den 21 september 2010 om ett globalt system för överföring av passageraruppgifter (PNR) till tredjeländer, KOM(2010) 492 slutlig, Bryssel, 21 september 2010. Se även artikel 29-gruppen (2010), *Yttrande 7/2010 om Europeiska kommissionens meddelande om en övergripande strategi när det gäller överföring av passageraruppgifter (PNR-uppgifter) till tredjeländer*, WP 178, Bryssel 12 november, 2010.

242 Förslag till Europaparlamentets och rådets direktiv om användning av PNR-uppgifter för att förebygga, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, KOM(2011) 32 slutlig, Bryssel, 2 februari 2011. I april 2011 bad Europaparlamentet FRA att yttra sig om förslaget och dess överensstämmelse med Europeiska unionens stadga om de grundläggande rättigheterna. Se: FRA (2011), *Yttrande 1/2011 – Passenger Name Record* , Wien, 14 juni 2011.

243 EU förhandlar om ett nytt PNR-avtal med Kanada som ska ersätta det avtal från 2006 som för närvarande gäller.

och ställdes inför begäran att lämna uppgifter till USA:s Department of the Treasury för terrrorism- och undersökningssyften.[244]

Ur ett EU-perspektiv fanns ingen tillräcklig rättslig grund för att lämna dessa huvudsakligen europeiska uppgifter, vilka var tillgängliga i Förenta staterna enbart på grund av att ett av SWIFT:s centrum för behandling av datatjänster var beläget där.

Ett särskilt avtal mellan EU och USA, kallat SWIFT-avtalet, slöts 2010 för att skapa den nödvändiga rättsliga grunden och säkerställa adekvat dataskydd.[245]

Enligt detta avtal fortsätter finansiella uppgifter som lagras av SWIFT att lämnas till USA:s Treasury Department för att förebygga, undersöka, upptäcka eller åtala terrorism eller finansiering av terrorism. USA:s Treasury Department kan begära finansiella uppgifter från SWIFT, under förutsättning att begäran:

- så tydligt som möjligt identifierar de finansiella uppgifterna;
- tydligt bevisar behovet av uppgifterna;
- är så begränsat som möjligt för att minimera mängden uppgifter som begärs;
- inte efterfrågar några uppgifter som hänför sig till det gemensamma eurobetalningsområdet (SEPA).

Europol måste få en kopia av varje begäran från USA:s Treasury Department och kontrollera huruvida principerna i SWIFT-avtalet följs.[246] Om det bekräftas att de följs måste SWIFT lämna de finansiella uppgifterna direkt till USA:s Treasury Department.

244 Se i detta sammanhang artikel 29-gruppen (2011), *Yttrande 14/2011 om dataskyddsfrågor i samband med förebyggande av penningtvätt och finansiering av terrorism*, WP 186, Bryssel, 13 juni 2011; artikel 29-arbetsgruppen (2006), *Yttrande 10/2006 om behandling av personuppgifter hos SWIFT (Society for Worldwide Interbank Financial Telecommunications)*, WP 128, Bryssel, 22 november 2006; *Commission de la protection de la vie privée* (kommissionen för skydd av privatlivet, Belgien) (2008), *Control and recommendation procedure initiated with respect to the company SWIFT scrl* , beslut, 9 december 2008.

245 Rådets beslut 2010/412/EU av den 13 juli 2010 om ingående av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (TFTP), EUT 2010 L 195, s. 3 och 4. Avtalets text bifogas beslutet, EUT 2010 L 195, s. 5–14.

246 Den gemensamma tillsynsmyndigheten för Europol har genomfört revisioner av Europols verksamhet på området och resultatet finns på: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=sv.

Där måste uppgifterna lagras i en säker fysisk miljö där de endast kan nås av analytiker som utreder terrorism eller dess finansiering, och de finansiella uppgifterna får inte vara sammankopplade med någon annan databas. Generellt ska finansiella uppgifter från SWIFT raderas senast fem år från mottagandet. Finansiella uppgifter som är relevanta för specifika utredningar eller åtal kan sparas så länge som uppgifterna är nödvändiga för dessa utredningar eller åtal.

USA:s Treasury Department kan överföra information från uppgifter som erhållits från SWIFT till specifika myndigheter för brottsbekämpning, allmän säkerhet eller antiterrorism i eller utanför Förenta staterna enbart för utredning, upptäckt, förebyggande eller åtal av terrorism eller dess finansiering. Om vidarebefordran av finansiella uppgifter innefattar en medborgare eller boende i en av EU:s medlemsstater, måste all delning av uppgifter med myndigheterna i ett tredjeland först godkännas av de behöriga myndigheterna i den berörda medlemsstaten. Undantag kan göras när delning av uppgifterna är avgörande för att förebygga ett omedelbart och allvarligt hot mot den allmänna säkerheten.

Oberoende ansvariga, inklusive en person utnämnd av Europeiska kommissionen, övervakar överensstämmelse med principerna i SWIFT-avtalet.

De registrerade har rätt att erhålla bekräftelse från behörig dataskyddsmyndighet inom EU på att deras rättigheter när det gäller skydd av personuppgifter har tillgodosetts. De registrerade har också rätt till ändring, radering eller blockering av sina uppgifter som samlats in och lagrats av USA:s Treasury Department enligt SWIFT-avtalet. De registrerades rätt till tillgång kan emellertid omfattas av vissa juridiska begränsningar. Om tillgång nekas måste den registrerade informeras skriftligt om detta, liksom om rätten att söka administrativ och juridisk prövning i Förenta staterna.

SWIFT-avtalet gäller i fem år, fram till augusti 2015. Det förlängs automatiskt i ettårsperioder om ingen av parterna meddelar den andra, minst sex månader i förväg, att den inte har för avsikt att förlänga avtalet.

7

Skydd av personuppgifter inom polisiära och straffrättsliga myndigheter

EU	Frågor som täcks	Europarådet
	Allmänt	Konvention 108
	Polis	Rekommendation från polisen
		Europadomstolen, *B.B. mot Frankrike*, nr 5335/06, 17 december 2009.
		Europadomstolen, *S. och Marper mot Förenade kungariket*, nr 30562/04 och 30566/04, 4 december 2008
		Europadomstolen, *Vetter mot Frankrike*, nr59842/00, 31 maj 2005
	It-brott	Konvention om it-brott
Skydd av personuppgifter i anslutning till gränsöverskridande samarbete mellan polis och rättsliga myndigheter		
Rambeslut om skydd av personuppgifter	Allmänt	Konvention 108 Rekommendation från polisen
Prümbeslutet	För särskilda uppgifter: fingeravtryck, DNA, huliganism, etc.	Konvention 108 Rekommendation från polisen
Beslut från Europol Beslut från Eurojust Förordning om Frontex	Av särskilda byråer	Konvention 108 Rekommendation från polisen
Schengen II-beslut Förordning om VIS Förordning om Eurodac Beslut om TIS	Av särskilda gemensamma informationssystem	Konvention 108 Rekommendation från polisen
		Europadomstolen, *Dalea mot Frankrike*, nr 964/07, 2 februari 2010

I syfte att väga den enskildas intressen när det gäller skydd av personuppgifter mot samhällets intressen när det gäller insamling av uppgifter för att bekämpa brott och säkerställa nationell och offentlig säkerhet har Europarådet och EU antagit specifika rättsliga instrument.

7.1. Europarådets lagstiftning om skydd av personuppgifter i frågor som rör polis och straffrättsligt samarbete

Viktiga punkter

- Konvention 108 och Europarådets polisrekommendation omfattar skydd av personuppgifter inom alla områden av polisarbete.
- Konventionen om it-brott (*Budapestkonventionen*) är ett bindande internationellt rättsligt instrument som hanterar brott som begåtts mot och med hjälp av elektroniska nätverk.

På europeisk nivå omfattar konvention 108 alla områden för behandling av personuppgifter och dess bestämmelser är avsedda att reglera behandlingen av personuppgifter i allmänhet. Konvention 108 gäller därför för skydd av personuppgifter inom området för polisiära och straffrättsliga myndigheter även om avtalsparterna kan begränsa dess tillämpning.

De juridiska uppgifterna för polisiära och straffrättsliga myndigheter kräver ofta behandling av personuppgifter som kan medföra allvarliga konsekvenser för de berörda personerna. Rekommendationen om användning av personuppgifter inom polissektorn som antogs av Europarådet 1987 innehåller riktlinjer till avtalsparterna för hur de bör verkställa principerna i konvention 108 när det gäller polismyndigheternas behandling av personuppgifter.[247]

7.1.1. Polisrekommendationen

Europadomstolen har konsekvent hävdat att polisens eller nationella säkerhetsmyndigheters lagring och behållning av personuppgifter utgör ett intrång enligt

247 Europarådet, ministerkommittén (1987), rekommendation Rec (87)15 till medlemsstaterna som reglerar användningen av personuppgifter inom polissektorn, 17 september 1987.

artikel 8.1 i Europakonventionen. Många domar från Europadomstolen handlar om motivering av dessa intrång.[248]

Exempel: I målet *B.B. mot Frankrike*[249] beslutade Europadomstolen att registrering av en dömd sexbrottsling i en nationell juridisk databas föll under artikel 8 i Europakonventionen. Med tanke på att tillräckliga garantier för skydd av personuppgifter hade genomförts, såsom den registrerades rätt att begära radering av uppgifterna, den begränsade lagringstiden för uppgifterna och den begränsade tillgången till dessa uppgifter, hade en korrekt balans uppnåtts mellan de konkurrerande privata och offentliga intressena i detta fall. Domstolen drog slutsatsen att artikel 8 i Europakonventionen inte hade överträtts.

Exempel: I målet *S. och Marper mot Förenade kungariket*[250] hade båda klagande åtalats, men inte dömts, för brott. Deras fingeravtryck, DNA-profiler och cellprov behölls och lagrades dock av polisen. Den obegränsade lagringen av biometriska uppgifter var tillåten genom en stadga där en person var misstänkt för brott även om den misstänkta senare frikändes eller frigavs. Europadomstolen ansåg att den övergripande och godartade lagringen av personuppgifter, som inte var tidsbegränsad och där frikända personer endast hade begränsade möjligheter att begära radering, utgjorde ett oproportionerligt intrång i den klagandes rätt till respekt för privatlivet. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Många fler domar från Europadomstolen tar upp motivering av intrång i rätten till uppgiftsskydd genom övervakning.

Exempel: I målet *Allan mot Förenade kungariket*[251] spelade myndigheterna i hemlighet in privata konversationer mellan en fånge och en vän i fängelsets besöksrum och med en medanklagad i en fängelsecell. Europadomstolen ansåg att användningen av ljud- och videoinspelningsutrustning i den klagandes cell, fängelsets besöksrum och hos en annan fånge utgjorde intrång i den klagan-

248 Se Europadomstolen, *Leander mot Sverige*, nr 9248/81, 26 mars 1987, Europadomstolen, *M.M. mot Förenade kungariket*, nr 24029/07, 13 november 2012, Europadomstolen, *M.K. mot Frankrike*, nr 19522/09, 18 april 2013.

249 Europadomstolen, *B.B. mot Frankrike*, nr 5335/06, 17 december 2009.

250 Europadomstolen, *S. och Marper mot Förenade kungariket*, nr 30562/04 och 30566/04, 4 december 2008, punkterna 119 och 125.

251 Europadomstolen, *Allan mot Förenade kungariket*, nr 48539/99, 5 november 2002.

des rätt till privatliv. Eftersom det inte fanns något regelsystem för polisens användning av hemlig inspelningsutrustning vid den aktuella tidpunkten var det påstådda intrånget inte förenligt med lagen. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Exempel: I målet *Klass m.fl. mot Tyskland*[252] hävdade de klagande att flera tyska lagstiftningsakter som tillät hemlig övervakning av e-post, post och telekommunikation innebar överträdelse av artikel 8 i Europakonventionen, bland annat på grund av att den berörda personen inte informerats om övervakningsåtgärderna och inte kunde vända sig till domstolen när åtgärderna väl avslutats. Europadomstolen ansåg att ett hot om övervakning definitivt var ett intrång i kommunikationsfriheten mellan användare av post- och telekommunikationstjänster. Domstolen fann emellertid att tillräckliga garantier mot missbruk hade införts. Den tyska lagstiftande församlingen hade rätt i att betrakta dessa åtgärder som nödvändiga i ett demokratiskt samhälle i den nationella säkerhetens intresse och för att förebygga oroligheter och brott. Domstolen drog slutsatsen att artikel 8 i Europakonventionen inte hade överträtts.

Eftersom polismyndigheternas behandling av uppgifter kan få en betydande inverkan på berörda personer är detaljerade bestämmelser om skydd av personuppgifter för att hålla databaser på detta område särskilt nödvändiga. Europarådets polisrekommendation var tänkt att hantera frågan genom att ange riktlinjer för hur uppgifter bör samlas in för polisarbete, hur datafiler inom området bör förvaras, vem som har rätt att få tillgång till filerna, inbegripet villkoren för att föra över uppgifter till utländska polismyndigheter, hur de registrerade ska kunna utöva sina rättigheter när det gäller skydd av uppgifter och hur kontroll av oberoende myndigheter ska genomföras. Skyldigheten att tillhandahålla adekvat skydd av uppgifter beaktas också.

Rekommendationen innehåller ingen obegränsad eller godtycklig insamling av uppgifter av polismyndigheterna. Den begränsar polismyndigheternas insamling av personuppgifter till vad som är nödvändigt för att förebygga verklig fara eller förhindra ett specifikt brott. Eventuell ytterligare insamling av uppgifter behöver baseras på en specifik nationell lagstiftning. Behandling av känsliga uppgifter bör begränsas till vad som är absolut nödvändigt mot bakgrund av en särskild undersökning.

252 Europadomstolen, *Klass m.fl. mot Tyskland*, nr 5029/71, 6 september 1978.

Om personuppgifter samlas in utan kunskap om den registrerade bör denna informeras om insamlingen av uppgifter så snart det inte längre hindrar utredningar. Insamlingen av uppgifter genom teknisk övervakning eller på andra automatiska sätt bör också baseras på specifika lagbestämmelser.

Exempel: I målet *Vetter mot Frankrike*[253] hade anonyma vittnen anklagat den klagande för mord. Eftersom den klagande regelbundet gick till en väns hem installerade polisen avlyssningsutrustning där efter tillstånd från undersökningsdomaren. Baserat på konversationerna som registrerades arresterades den klagande och åtalades för mord. Han ansökte om att få inspelningen förklarad otillåtlig som bevis och hävdade framför allt att det inte var tillåtet enligt lag. För Europadomstolen var frågan huruvida användningen av avlyssningsutrustning skedde "i enlighet med lagen". Buggning av privata lokaler låg uppenbarligen inte inom omfattningen av artikel 100 i *et seq.* i straffprocessrätten, eftersom dessa bestämmelser gällde avlyssning av telefonlinjer. I artikel 81 i lagen angavs inte med rimlig tydlighet omfattningen eller sättet för hur myndigheterna skulle tillämpa sitt omdöme när det gällde att tillåta övervakning av privata konversationer. Den klagande hade därför inte åtnjutit miniminivån av skydd som medborgare har rätt till enligt rättspraxis i ett demokratiskt samhälle. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

I rekommendationen dras slutsatsen att när personuppgifter lagras ska tydlig distinktion göras mellan administrativa uppgifter och polisuppgifter, olika typer av registrerade såsom misstänkta, dömda personer, offer och vittnen och uppgifter som betraktas som hårda fakta och de som baseras på misstankar eller spekulation.

Polisuppgifter ska vara strikt begränsade när det gäller syftet. Detta får konsekvenser för spridning av polisens uppgifter till tredje part: överföring eller spridning av dessa uppgifter inom polissektorn bör styras av huruvida det finns ett berättigat intresse av att dela informationen. Överföring eller spridning av dessa uppgifter utanför polissektorn bör vara tillåtet endast om det finns en tydlig rättslig skyldighet eller tillstånd. Internationell överföring eller spridning bör begränsas till utländska polismyndigheter och baseras på särskilda rättsliga bestämmelser, sannolikt internationella avtal, om det inte är nödvändigt för att förebygga allvarlig och omedelbar fara.

253 Europadomstolen, *Vetter mot Frankrike*, nr 59842/00, 31 maj 2005.

Polisens behandling av uppgifter måste omfattas av oberoende tillsyn för att säkerställa överensstämmelse med inhemsk lag om skydd av personuppgifter. De registrerade måste ha samtliga rättigheter till tillgång som ingår i konvention 108. Om de registrerades rätt till tillgång har begränsats enligt artikel 9 i konvention 108 på grund av faktisk polisutredning, måste den registrerade ha rätt att enligt inhemsk lag överklaga till den nationella tillsynsmyndigheten för skydd av personuppgifter eller till ett annat oberoende organ.

7.1.2. Budapestkonventionen om it-brott

Eftersom brottslig verksamhet i allt större utsträckning använder och påverkar elektroniska system för hantering av uppgifter behövs nya rättsliga bestämmelser för att möta utmaningen. Europarådet antog därför ett internationellt rättsligt instrument, konventionen om it-brott – även kallad Budapestkonventionen – för att hantera frågan om brott som begås mot och med hjälp av elektroniska nätverk.[254] Konventionen är öppen även för dem som inte är medlemmar i Europarådet och, från och med mitten av 2013, är fyra stater utanför Europarådet – Australien, Dominikanska republiken, Japan och Förenta staterna – parter till konventionen och 12 andra icke medlemmar hade undertecknat den eller bjudits in att bli medlemmar.

Konventionen om it-brott är det mest inflytelserika internationella fördraget om överträdelser av lagen över internet eller andra informationsnätverk. Den kräver att parterna ska uppdatera och harmonisera sin brottslagstiftning mot hackning och andra brott mot säkerhet, bland annat överträdelse av copyright, bedrägerier via dator, barnpornografi och annan olaglig it-verksamhet. Konventionen ger också processrättsliga befogenheter som omfattar sökning av datornätverk och avlyssning av kommunikationer i samband med bekämpning av it-brott. Den möjliggör slutligen effektivt internationellt samarbete. I ett tilläggsprotokoll till konventionen tas kriminalisering av rasistisk och främlingsfientlig propaganda i datornätverk upp.

Även om konventionen inte egentligen är ett instrument för att främja dataskydd kriminaliserar den verksamhet som riskerar att överträda en registrerads rätt till skydd av hans eller hennes uppgifter. Den ålägger även avtalsparterna när de införlivar konventionen att planera för adekvat skydd av mänskliga rättigheter och

254 Europarådet, ministerkommittén (2001), Konvention om it-brott, CETS nr 185, Budapest, 23 november 2001, trädde i kraft den 1 juli 2004.

friheter, inbegripet rättigheter som garanteras enligt Europakonventionen, såsom rätten till skydd av personuppgifter.[255]

7.2. EU:s lagstiftning om skydd av personuppgifter inom polisiära och rättsliga frågor

Viktiga punkter

- På EU-nivå regleras skydd av personuppgifter på det polisiära och straffrättsliga området endast i samband med gränsöverskridande samarbete mellan polis och rättsvårdande myndigheter.
- Särskilda system för skydd av personuppgifter finns för Europeiska polisbyrån (Europol) och den europeiska enheten för rättsligt samarbete (Eurojust) som är ett EU-organ som bistår och främjar gränsöverskridande brottsbekämpning.
- Särskilda system för skydd av personuppgifter finns även för de gemensamma informationssystem som inrättats på EU-nivå för gränsöverskridande informationsutbyte mellan behöriga polismyndigheter och rättsvårdande myndigheter. Viktiga exempel är Schengen II, informationssystemet för viseringar (VIS) och Eurodac, ett centraliserat system som innehåller uppgifter om fingeravtryck från tredjelandsmedborgare som ansöker om asyl i en av EU:s medlemsstater.

Dataskyddsdirektivet gäller inte för polisiära och straffrättsliga myndigheter. I avsnitt 7.2.1 beskrivs de viktigaste rättsliga instrumentet på området.

7.2.1. Rambeslut om skydd av personuppgifter

Rådets rambeslut 2008/977/RIF om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (*rambeslut om skydd av personuppgifter*)[256] syftar till att tillhandahålla skydd för personuppgifter för fysiska personer när deras personuppgifter behandlas för att förebygga, utreda, upptäcka eller åtala ett brott eller verkställa ett straff. Behöriga myndigheter på det polisiära och straffrättsliga området arbetar för medlemsstaterna eller EU. Dessa

255 *Ibid.*, artikel 15.1.

256 Europeiska unionens råd (2008), rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (*rambeslut om skydd av personuppgifter*), EUT 2008 L 350.

myndigheter är EU-byråer eller organ liksom myndigheter i medlemsstaterna.[257] Tillämpligheten i rambeslutet är begränsad till att säkerställa skydd av personuppgifter i det gränsöverskridande samarbetet mellan dessa myndigheter och utvidgas inte till nationell säkerhet.

Rambeslutet om skydd av personuppgifter bygger i stor utsträckning på principerna och definitionerna i konvention 108 och dataskyddsdirektivet.

Uppgifterna får endast användas av en behörig myndighet och endast för det syfte för vilket de överfördes eller gjordes tillgängliga. Den mottagande medlemsstaten måste respektera alla restriktioner om utbytet av uppgifter som föreskrivs i lagen i den översändande medlemsstaten. Den mottagande staten får emellertid använda uppgifterna i annat syfte enligt vissa villkor. Loggning och dokumentation av överföringar är en specifik uppgift för de behöriga myndigheterna för att bistå med klargörande av ansvar som uppstår genom klagomål. Vidarebefordran av uppgifter, som erhållits vid gränsöverskridande samarbete, till tredje part kräver samtycke från medlemsstaten från vilken uppgifterna härrörde, även om det finns undantag i brådskande fall.

Behöriga myndigheter måste vidta nödvändiga säkerhetsåtgärder för att skydda personuppgifter mot all otillåten form av behandling.

Alla medlemsstater måste se till att en eller fler av de oberoende nationella tillsynsmyndigheterna ansvarar för att ge råd och övervaka tillämpningen av bestämmelserna som antagits enligt rambeslutet om skydd av personuppgifter. De ska också lyssna till klagomål från alla om skydd av hans eller hennes rättigheter och friheter rörande behöriga myndigheters behandling av personuppgifter.

Den registrerade har rätt till information om behandling av hans eller hennes personuppgifter och har rätt till tillgång, ändring, radering eller blockering. Om utövande av dessa rättigheter nekas på tvingande grunder måste den registrerade ha rätt att överklaga till den behöriga nationella tillsynsmyndigheten och/eller till en domstol. Om en person lider skada på grund av att nationell lag som införlivar rambeslutet om skydd av personuppgifter överträds, har denna person rätt till ersättning från den registeransvariga.[258] Generellt sett måste de registrerade ha tillgång till en

257 *Ibid.*, artikel 2 h.

258 *Ibid.*, artikel 19.

rättslig prövning för alla överträdelser av deras rättigheter som garanteras i den nationella lag som införlivar rambeslutet om skydd av personuppgifter.[259]

Europeiska kommissionen föreslog en reform som består av en allmän uppgiftsskyddsförordning[260] och ett allmänt uppgiftsskyddsdirektiv.[261] Det nya direktivet ersätter det nuvarande rambeslutet om skydd av personuppgifter och tillämpar allmänna principer och regler på polissamarbete och straffrättsligt samarbete.

7.2.2. Mer specifika rättsliga instrument om skydd av personuppgifter vid gränsöverskridande samarbete mellan polis och rättsvårdande myndigheter

Utöver rambeslutet om skydd av personuppgifter regleras utbyte av information som innehas av medlemsstaterna inom specifika områden av ett antal rättsliga instrument såsom rådets rambeslut 2009/315/RIF om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll och rådets beslut om en samarbetsordning för medlemsstaternas finansunderrättelseenheter avseende utbyte av information.[262]

Nog så viktigt är att gränsöverskridande samarbete[263] mellan behöriga myndigheter i allt större utsträckning involverar utbyte av uppgifter om invandring. Detta område av lagen tillhör inte polisiära eller straffrättsliga frågor men är på många sätt relevant för arbetet inom polisen och rättsvårdande myndigheter. Detsamma

259 *Ibid.*, artikel 20.

260 Europeiska kommissionen (2012), *Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning)*, COM(2012) 11 final, Bryssel, 25 januari 2012.

261 Europeiska kommissionen (2012), *Förslag till Europaparlamentets och rådets direktiv om skydd för enskilda personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter*, COM(2012) 10 final, Bryssel, 25 januari 2012.

262 Europeiska unionens råd (2009), rådets rambeslut 2009/315/RIF av den 26 februari 2009 om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll EUT 2009 L 93, Europeiska unionens råd (2000), rådets beslut 2000/642/RIF av den 17 oktober 2000 om en samarbetsordning för medlemsstaternas finansunderrättelseenheter avseende utbyte av information, EGT 2000 L 271.

263 Europeiska kommissionen (2012), Meddelande från kommissionen till Europaparlamentet och rådet om ett stärkt EU-samarbete inom brottsbekämpningen: den europeiska modellen för informationsutbyte (Eixm) COM(2012) 735 final, Bryssel, 7 december 2012.

gäller för uppgifter om varor som importeras till eller exporteras från EU. Elimineringen av interna gränskontroller inom EU har ökat risken för bedrägeri och gjort det nödvändigt för medlemsstaterna att intensifiera samarbetet, bland annat genom att öka gränsöverskridande informationsutbyte för att effektivare upptäcka och åtala överträdelser av nationell tullagstiftning och tullagstiftning inom EU.

Prümbeslutet

Ett viktigt exempel på institutionaliserat gränsöverskridande samarbete genom utbyte av nationellt innehavda uppgifter är rådets beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (*Prümbeslutet*), som införlivade Prümfördraget i EU-lagstiftningen 2008.[264] Prümfördraget var ett internationellt avtal om polissamarbete som undertecknades 2005 av Österrike, Belgien, Frankrike, Tyskland, Luxemburg, Nederländerna och Spanien.[265]

Syftet med Prümbeslutet är att hjälpa medlemsstaterna att förbättra informationsdelningen i syfte att förebygga och bekämpa brott inom tre områden: terrorism, gränsöverskridande brott och olaglig invandring. I detta syfte innehåller beslutet bestämmelser som gäller:

- automatisk tillgång till DNA-profiler, fingeravtrycksuppgifter och vissa nationella fordonsregistreringsuppgifter;
- tillhandahållande av uppgifter i förhållande till stora händelser som har en gränsöverskridande omfattning;
- tillhandahållande av information i syfte att förebygga terroristbrott;
- andra åtgärder för att utvidga gränsöverskridande polissamarbete.

264 Europeiska unionens råd (2008), rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet, EUT 2008 L 210.

265 Konvention mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig invandring, tillgänglig på: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

Databaserna som har gjorts tillgängliga enligt Prümbeslutet styrs helt av nationell lag men utbytet av uppgifter styrs dessutom av beslutet och på senare tid även rambeslutet om skydd av personuppgifter. De nationella tillsynsmyndigheterna för skydd av personuppgifter är behöriga organ för tillsyn av dessa flöden av personuppgifter.

7.2.3. Skydd av personuppgifter vid Europol och Eurojust

Europol

Europol som är EU:s rättsvårdande byrå har sitt huvudkontor i Haag och nationella enheter i samtliga medlemsstater. Europol inrättades 1998 och dess nuvarande rättsliga status som EU-institution är baserad på rådets beslut om inrättande av europeiska poliskontoret (Europolbeslutet).[266] Syftet med Europol är att bistå med förebyggande och utredning av organiserad brottslighet, terrorism och andra former av allvarlig brottslighet, enligt förteckningen i beslutet om Europol, som påverkar två eller fler medlemsstater.

I syfte att uppnå sina mål har Europol inrättat Europols informationssystem, som tillhandahåller en databas för medlemsstater för utbyte av kriminalunderrättelser och information via de nationella enheterna. Europols informationssystem kan användas för att tillgängliggöra uppgifter som rör personer som är misstänkta eller som åtalats för ett brott som omfattas av Europols behörighet, eller personer om vilka det finns faktiska indikationer på att de kommer att begå sådana brott. Europol och de nationella enheterna kan lägga in uppgifter direkt i Europols informationssystem och även ta ut uppgifter därifrån. Endast den part som lagt in uppgifterna i systemet får ändra, korrigera eller radera dem.

Om det är nödvändigt för att kunna utföra uppgifterna får Europol lagra, ändra och använda uppgifter rörande brott i analysregister. Analysregister öppnas för att samla ihop, behandla eller använda uppgifter i syfte att bistå konkreta brottsutredningar som utförs av Europol, tillsammans med EU:s medlemsstater.

266 Europeiska unionens råd (2009), rådets beslut av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europol), EUT 2009 L 121. Se även kommissionens förslag till förordning som också innehåller en rättslig ram för ett nytt Europol som följer på och ersätter Europol i enlighet med rådets beslut 2009/371/RIF av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europol), och Cepol inrättat genom rådets beslut 2005/681/RIF om inrättande av Europeiska polisakademin (Cepol), COM(2013) 173 final.

Som svar på ny utveckling inrättades Europeiska it-brottscentrumet vid Europol den 1 januari 2013.[267] Centrumet fungerar som EU:s informationsnav för it-brott, bidrar till snabbare reaktioner vid brott på nätet, utvecklar och sprider digital kriminalteknisk kunskap och levererar bästa praxis om utredningar av it-brott. Centrumet fokuserar på it-brott som:

- begås av organiserade grupper för att generera stora brottsliga vinster, såsom bedrägeri på nätet;
- orsakar allvarlig skada för offret, exempelvis sexuellt utnyttjande av barn på nätet;
- påverkar kritisk infrastruktur och informationssystem i EU.

Dataskyddssystemet som styr Europols verksamhet har förbättrats. I Europols beslut fastställs i artikel 27 att de principer som anges i konvention 108 och i rekommendationen om användning av personuppgifter inom polissektorn, rörande behandlingen av automatiska och icke automatiska uppgifter, gäller. Överföring av uppgifter mellan Europol och medlemsstaterna måste också uppfylla reglerna i rambeslutet om skydd av personuppgifter.

För att säkerställa överensstämmelse med tillämplig dataskyddslagstiftning och framför allt för att rättigheterna för den enskilda inte ska överträdas genom behandlingen av personuppgifter, granskas och övervakas Europols verksamhet av den oberoende gemensamma tillsynsmyndigheten för Europol.[268] Alla enskilda har rätt att få tillgång till alla personuppgifter som Europol kan ha om honom eller henne, utöver rätten att begära att dessa personuppgifter kontrolleras, korrigeras eller raderas. Om en person inte är nöjd med Europols beslut rörande utövandet av dessa rättigheter kan han eller hon överklaga till den gemensamma tillsynsmyndighetens överklagandekommitté.

Om skada uppstår som ett resultat av rättsliga eller faktiska misstag i uppgifter som lagras eller behandlas av Europol kan den skadade parten kräva upprättelse endast inför den behöriga domstolen i den medlemsstat där händelsen som orsakat skadan

267 Se även Europeiska datatillsynsmannen (2012), *Yttrande från Europeiska datatillsynsmannen om meddelandet från Europeiska kommissionen till rådet och Europaparlamentet angående inrättande av ett Europeiskt centrum mot it-brottslighet*, Bryssel, 29 juni 2012.

268 Europolbeslutet, artikel 34.

uppstått.[269] Europol ersätter medlemsstaten om skadan beror på att Europol underlåtit att uppfylla sina rättsliga skyldigheter.

Eurojust

Eurojust inrättades 2002 och är ett EU-organ med huvudkontor i Haag som främjar rättsligt samarbete vid utredningar och åtal som gäller allvarligt brott i minst två medlemsstater.[270] Eurojust är behörigt att:

- stimulera och förbättra samordningen av utredningar och åtal mellan behöriga myndigheter i de olika medlemsstaterna;

- underlätta verkställande av begäran och beslut som gäller rättsligt samarbete.

Eurojusts funktioner utförs av nationella medlemmar. Varje medlemsstat utser en domare eller åklagare för Eurojust, vars ställning omfattas av nationell lag och förses med nödvändig behörighet för att utföra de uppgifter som krävs för att stimulera och förbättra rättsligt samarbete. De nationella medlemmarna agerar dessutom gemensamt som ett kollegium för att genomföra särskilda uppgifter för Eurojust.

Eurojust kan behandla personuppgifter under förutsättning att det är nödvändigt för att uppnå målsättningarna. Detta är emellertid begränsat till specifik information rörande personer som är misstänkta för att ha begått eller deltagit i eller har dömts för brott som ingår i Eurojusts behörighet. Eurojust kan även behandla viss information rörande vittnen eller offer för brott som omfattas av Eurojusts behörighet.[271] Under exceptionella omständigheter kan Eurojust, under en begränsad tidsperiod, behandla mer omfattande personuppgifter rörande omständigheterna kring en överträdelse om dessa uppgifter omedelbart är relevanta för en pågående utredning. Inom sina befogenheter kan Eurojust samarbeta med andra EU-institutioner,

269 *Ibid.*, artikel 52.

270 Europeiska unionens råd (2002), rådets beslut 2002/187/RIF av den 28 februari 2002 om inrättande av Eurojust för att stärka kampen mot grov brottslighet, EGT 2002 L 63, Europeiska unionens råd (2003), rådets beslut 2003/659/RIF av den 18 juni 2003 om ändring av beslut 2002/187/RIF om inrättande av Eurojust för att stärka kampen mot grov brottslighet, EUT 2003 L 44; Europeiska unionens råd (2009), rådets beslut 2009/426/RIF av den 16 december 2008 om förstärkning av Eurojust och om ändring av beslut 2002/187/RIF om inrättande av Eurojust för att stärka kampen mot grov brottslighet, EUT 2009 L 138 (*besluten om Eurojust*).

271 Konsoliderad version av rådets beslut 2002/187/RIF ändrad genom rådets beslut 2003/659/RIF och rådets beslut 2009/426/RIF, artikel. 15.2.

-organ och -kontor och utbyta personuppgifter med dem. Eurojust kan även samarbeta med och utbyta personuppgifter med tredjeländer och organisationer.

När det gäller skydd av personuppgifter måste Eurojust garantera en skyddsnivå som minst är densamma som principerna från Europarådets konvention 108 och dess senare ändringar. Vid utbyte av uppgifter måste specifika regler och begränsningar efterlevas, som införs antingen i samarbetsavtal eller i arbetsöverenskommelser i enlighet med Eurojust rådsbeslut och Eurojusts regler för skydd av personuppgifter.[272]

En oberoende gemensam tillsynsmyndighet har inrättats vid Eurojust med uppgift att övervaka behandlingen av personuppgifter som utförs av Eurojust. Enskilda kan överklaga till den gemensamma tillsynsmyndigheten om de inte är nöjda med Eurojusts svar på en begäran om tillgång, korrigering, blockering eller radering av personuppgifter. Om Eurojust behandlar personuppgifter otillåtet ska Eurojust vara ansvarigt i enlighet med nationell lag i den medlemsstat där huvudkontoret är beläget, dvs. Nederländerna, för eventuell skada som drabbat den registrerade.

7.2.4. Skydd av personuppgifter i de gemensamma informationssystemen på EU-nivå

Utöver utbyte av uppgifter mellan medlemsstater och inrättande av specialiserade EU-myndigheter för att bekämpa gränsöverskridande brott har flera gemensamma informationssystem inrättats på EU-nivå för att fungera som plattform för utbyte av uppgifter mellan behöriga nationella myndigheter och EU-myndigheter för specificerade syften inom brottsbekämpning, inbegripet invandrings- och tullagstiftning. Vissa av dessa system har utvecklats utifrån multilaterala avtal som sedan fått tillägg av EU:s juridiska instrument och system, såsom Schengens informationssystem, informationssystemet för viseringar, Eurodac, Eurosur eller tullinformationssystemet.

Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA)[273] inrättades 2012, och ansvarar för långsiktig operativ förvaltning av den andra generationen av Schengens informationssystem (SIS II), informationssystemet för viseringar (VIS) och Eurodac. Huvuduppgiften

272 Arbetsordning för behandling och skydd av personuppgifter vid Eurojust, EUT C 68, 19.3.2005, s. 1.

273 Europaparlamentets och rådets förordning (EU) nr 1077/2011 av den 25 oktober 2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa, EUT 2011 L 286.

för eu-LISA är att säkerställa en effektiv, säker och kontinuerlig drift av informationstekniksystemen. Byrån är också ansvarig för att anta nödvändiga åtgärder för att trygga säkerheten för systemen och personuppgifterna.

Schengens informationssystem

Under 1985 träffade flera medlemsstater i de tidigare Europeiska gemenskaperna ett avtal med staterna i Benelux, Tyskland och Frankrike om att gradvis avskaffa kontroller vid de gemensamma gränserna (*Schengenavtalet*), som syftar till att skapa ett område med fri rörlighet för personer, oberoende av gränskontroller inom Schengenområdet.[274] I syfte att uppväga hotet mot den allmänna säkerheten som skulle kunna uppstå genom öppna gränser, inrättades strängare gränskontroller vid Schengenområdets yttre gränser, liksom ett nära samarbete mellan nationell polis och rättsliga myndigheter.

Som en konsekvens av att ytterligare stater har anslutit sig till Schengenavtalet integrerades Schengensystemet slutligen i EU:s rättsliga ram genom Amsterdamfördraget .[275] Införlivandet av beslutet ägde rum 1999. Den senaste versionen av Schengens informationssystem, det så kallade SIS II, trädde i kraft den 9 april 2013. Det gäller nu för alla EU:s medlemsstater plus Island, Liechtenstein, Norge och Schweiz.[276] Europol och Eurojust har också tillgång till SIS II.

SIS II består av ett centralt syste (C-SIS), ett nationellt system (N-SIS) i respektive medlemsstat, och en kommunikationsinfrastruktur mellan det centrala systemet och de nationella systemen. C-SIS innehåller vissa uppgifter som medlemsstaterna lagt in om personer och föremål. C-SIS används av nationella gränskontroller, polisen, tullen, visummyndigheter och rättsliga myndigheter inom hela Schengenområdet. Samtliga medlemsstater driver en nationell kopia av C-SIS, kallad den nationella delen av Schengens informationssystem (N-SIS), som hela tiden uppdateras, och därmed uppdateras C-SIS. N-SIS konsulteras och utfärdar en varning om:

274 Överenskommelser mellan regeringarna i Beneluxstaterna, Tyskland och Frankrike om ett successivt avskaffande av kontroller vid deras gemensamma gränser, EGT 2000 L 239.

275 Europeiska gemenskaperna (1997), Amsterdamfördraget om ändring av fördraget om Europeiska unionen och Fördraget om upprättande av Europeiska gemenskaperna, och vissa därtill hörande handlingar, EGT 1997 C 340.

276 Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II), EUT 2006 L 381, och Europeiska unionens råd (2007), rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem, (SIS II), EUT 2007 L 205.

- en person inte har rätt att komma in i eller stanna i Schengenområdet; eller
- personen eller föremålet söks av rättsvårdande eller brottsbekämpande myndigheter; eller
- personen har rapporterats försvunnen; eller
- varor såsom sedlar, bilar, transportbilar, vapen och identitetshandlingar, har rapporterats som stuleneller försvunnen egendom.

Vid en varning ska uppföljningsaktiviteter initieras via den nationella delen av Schengens informationssystem.

SIS II har nya funktioner, såsom möjlighet att mata in biometriska uppgifter, exempelvis fingeravtryck och foton, eller nya kategorier av varningar, såsom stulna båtar, flygplan, containrar eller betalningssätt, och förbättrade varningar om personer och föremål, kopior av europeiska arresteringsorder om personer som söks för arrestering, överlämnande eller utlämning.

Rådets beslut 2007/533/RIF om inrättande, drift och användning av andra generationen av Schengens informationssystem (Schengen II-beslutet) införlivar konvention 108: ”Personuppgifter som behandlas med tillämpning av detta beslut skall skyddas i enlighet med Europarådets konvention av den 28 januari 1981”.[277] När nationella polismyndigheter använder personuppgifter genom tillämpning av Schengen II måste bestämmelserna i konvention 108, liksom i rekommendationen om användning av personuppgifter inom polissektorn, införlivas i nationell lag.

Behörig nationell tillsynsmyndighet i respektive medlemsstat övervakar den inhemska N-SIS. Den måste framför allt kontrollera kvaliteten på de uppgifter som medlemsstaterna lägger in i C-SIS via N-SIS. Den nationella tillsynsmyndigheten måste se till att behandlingen av uppgifter inom det inhemska N-SIS revideras minst vart fjärde år. De nationella tillsynsmyndigheterna och Europeiska datatillsynsmannen samarbetar och säkerställer samordnad tillsyn av SIS, medan datatillsynsmannen är ansvarig för tillsyn av C-SIS. För öppenhetens skull ska en gemensam rapport sändas till Europaparlamentet, rådet och eu-LISA vartannat år.

277 Europeiska unionens råd (2007), rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av den andra generationen av Schengens Informationssystem, EUT 2007 L 205, artikel 57.

Enskildas rätt till tillgång rörande SIS II kan utövas i alla medlemsstater eftersom samtliga N-SIS är en exakt kopia av C-SIS.

Exempel: I målet *Dalea mot Frankrike*[278] nekades den klagande visum till Frankrike eftersom de franska myndigheterna hade meddelat Schengens informationssystem att han skulle nekas tillträde. Den klagande begärde tillträde utan framgång och ändring eller radering av uppgifterna hos den franska dataskyddsmyndigheten, och till slut även hos franska högsta förvaltningsdomstolen. Europadomstolen ansåg att rapporteringen om den klagande till Schengens informationssystem hade skett i enlighet med lagen och följt det berättigade målet att skydda den nationella säkerheten. Eftersom den klagande inte visade hur han faktiskt hade lidit som ett resultat av att han nekades tillträde till Schengenområdet och eftersom tillräckliga åtgärder för att skydda honom från godtyckliga beslut fanns hade ingripandet i hans rätt till respekt för privatlivet varit proportionerligt. Den klagandes klagomål enligt artikel 8 förklarades därför otillåtligt.

Informationssystemet för viseringar

Informationssystemet för viseringar (VIS), som också hanteras av eu-LISA, utvecklades för att stödja införlivandet av en gemensam visumpolitik i EU.[279] Tack vare informationssystemet för viseringar kan Schengenstaterna utbyta visumuppgifter via ett system som förbinder konsulaten i Schengenstaterna i länder utanför EU med externa gränsövergångsställen i Schengens alla medlemsstater. Informationssystemet för viseringar hanterar uppgifter rörande ansökningar om korttidsvisum för att besöka eller resa igenom Schengenområdet. Systemet gör det möjligt för gränsmyndigheter att med hjälp av biometriska uppgifter kontrollera om en person med visum är rätt innehavare av det och identifiera personer utan handlingar eller med falska handlingar.

278 Europadomstolen, *Dalea mot Frankrike*, (dec.), no. 964/07, 2 februari 2010.

279 Europeiska unionens råd (2004), rådets beslut av den 8 juni 2004 om inrättande av informationssystemet för viseringar (VIS), EUT L 213, 15.6.2004; Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (*VIS-förordningen*), EUT 2008 L 218; Europeiska unionens råd (2008), rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott, EUT 2008 L 218.

Enligt Europaparlamentets och rådets förordning (EG) nr 767/2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (*VIS-förordningen*), får endast uppgifter om den klagande, hans eller hennes visum, fotografier, fingeravtryck, kopplingar till tidigare ansökningar och ansökningshandlingar för åtföljande personer registreras i VIS.[280] Tillträde till VIS i syfte att lägga in, ändra eller radera uppgifter är begränsat enbart till medlemsstaternas visummyndigheter, medan tillträde för att konsultera uppgifter ges till visummyndigheter och behöriga myndigheter för kontroller vid externa gränsövergångsställen, kontroll av invandring och asyl. Enligt vissa villkor kan nationell behörig polismyndighet och Europol begära tillgång till uppgifter som matats in i VIS i syfte att förhindra, upptäcka och utreda terroristbrott och andra brott.[281]

Eurodac

Eurodacs namn hänför sig till daktylogram eller fingeravtryck. Det är ett centraliserat system som innehåller fingeravtrycksuppgifter om tredjelandsmedborgare som ansöker om asyl i en av EU:s medlemsstater.[282] Systemet har funnits sedan januari 2003, och dess syfte är att bistå vid fastställande av vilken medlemsstat som är ansvarig för att granska en viss asylansökan enligt rådets förordning (EG) nr 343/2003 om kriterier och mekanismer för att avgöra vilken medlemsstat som har ansvaret för att pröva en asylansökan som en medborgare i ett tredje land har lämnat in i någon medlemsstat (*Dublin II-förordningen*).[283] Personuppgifter i Eurodac kan användas endast i syfte att underlätta tillämpningen av Dublin II-förordningen, medan all annan användning är förbjuden.

280 Artikel 5 i Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (*VIS-förordningen*), EUT 2008 L 218.

281 Europeiska unionens råd (2008), rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott, EUT 2008 L 218.

282 Rådets förordning (EG) nr 2725/2000 av den 11 december 2000 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av Dublinkonventionen, EUT 2000 L 316, rådets förordning (EG) nr 407/2002 av den 28 februari 2002 om vissa tillämpningsföreskrifter för förordning (EG) nr 2725/2000 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av Dublinkonventionen, EUT 2002 L 62 (*Eurodacförordningarna*).

283 Rådets förordning (EG) nr 343/2003 av den 18 februari 2003 om kriterier och mekanismer för att avgöra vilken medlemsstat som har ansvaret för att pröva en asylansökan som en medborgare i tredje land har gett in i någon medlemsstat, EUT 2003 L 50 (*Dublin II-förordningen*).

Eurodac består av en central enhet, som förvaltas av eu-LISA, för att lagra och jämföra fingeravtryck och ett system för elektronisk överföring av uppgifter mellan medlemsstaterna och den centrala databasen. Medlemsstaterna tar och vidarebefordrar fingeravtryck från alla medborgare från länder utanför EU eller statslösa personer som är minst 14 år och som ansöker om asyl på deras territorium, eller som grips för att olagligt ha passerat deras yttre gräns. Medlemsstaterna får också ta och vidarebefordra fingeravtryck från medborgare från länder utanför EU eller statslösa personer som uppehåller sig på deras territorium utan tillstånd.

Fingeravtrycksuppgifterna lagras i Eurodacs databas endast i pseudonymiserad form. Vid en eventuell matchning lämnas pseudonymen, tillsammans med namnet på den första medlemsstaten som överförde uppgifterna om fingeravtrycken, till den andra medlemsstaten. Denna andra medlemsstat kontaktar sedan den första medlemsstaten eftersom denna, enligt Dublin II-konventionen, är ansvarig för att behandla asylansökan.

Personuppgifter som lagras i Eurodac och som gäller asylsökande sparas i 10 år från och med den dag fingeravtrycken togs, om inte den registrerade blir medborgare i ett EU-land. I så fall måste uppgifterna omedelbart raderas. Uppgifter rörande utländska medborgare som grips för att olagligen ha passerat den yttre gränsen lagras i två år. Dessa uppgifter måste raderas omedelbart om den registrerade får uppehållstillstånd, lämnar EU:s territorium eller erhåller medborgarskap i en medlemsstat.

Utöver alla EU:s medlemsstater tillämpar även Island, Norge, Liechtenstein och Schweiz Eurodac på grundval av internationella överenskommelser.

Eurosur

Det europeiska gränsövervakningssystemet (*Eurosur*)[284] är utformat för att förbättra kontrollen av Schengens yttre gränser genom att upptäcka, förebygga och bekämpa illegal invandring och gränsöverskridande brottslighet. Det bidrar till att förbättra informationsutbytet och det operativa samarbetet mellan nationella centrum för

284 Europaparlamentets och rådets förordning (EU) nr 1052/2013 av den 22 oktober 2013 om inrättande av ett europeiskt gränsövervakningssystem (Eurosur), EUT 2013, L 295.

samordning och Frontex, det EU-organ som ansvarar för att utveckla och tillämpa det nya begreppet integrerad gränsförvaltning.[285] Dess allmänna målsättning är:

- att minska antalet illegala invandrare som kommer in i EU utan att upptäckas;
- att minska antalet döda eller illegala invandrare genom att rädda fler liv till havs;
- att öka EU:s inre säkerhet som helhet genom att bidra till att förebygga gränsöverskridande brottslighet.[286]

Eurosur inledde sitt arbete den 2 december 2013 i samtliga medlemsstater med yttre gränser, och kommer att börja den 1 december 2014 i de övriga. Förordningen kommer att gälla för övervakning av land, yttre gränser till havs och luftgränser i medlemsstaterna.

Tullinformationssystemet

Ett annat viktigt gemensamt informationssystem som inrättats på EU-nivå är tullinformationssystemet (TIS).[287] När den inre marknaden inrättades avskaffades alla kontroller och formalia när det gäller varor som flyttas inom EU:s territorium, vilket ledde till en ökad risk för bedrägeri. Risken uppvägdes av ett intensifierat samarbete mellan medlemsstaternas tullmyndigheter. Syftet med TIS är att bistå medlemsstaterna i att förebygga, utreda och åtala allvarliga brott mot tull- och jordbrukslagstiftning, såväl nationellt som på EU-nivå.

285 Europaparlamentets och rådets förordning (EU) nr 1168/2011 av den 25 oktober 2011 om ändring av rådets förordning (EG) nr 2007/2004 om inrättande av en europeisk byrå för förvaltningen av det operativa samarbetet vid Europeiska unionens medlemsstaters yttre gränser, EUT 2011 L 394 (*Frontexförordningen*).

286 Se även: Europeiska kommissionen (2008), meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och regionkommittén: Undersökning av möjligheterna att inrätta ett europeiskt gränsövervakningssystem (Eurosur), KOM(2008) 68 slutlig, Bryssel, 13 februari 2008, Europeiska kommissionen (2011), konsekvensbedömning som åtföljer Europaparlamentets och rådets förslag till förordning om inrättande av det europeiska gränsövervakningssystemet (Eurosur), arbetsdokument SEC(2011) 1536 slutlig, Bryssel, 12 december 2011, s. 18.

287 Europeiska unionens råd (1995), rådets akt av den 26 juli 1995 om utarbetandet av konventionen om användning av informationsteknologi för tulländamål, EUT 1995 C 316, ändrad av Europeiska unionens råd (2009), förordning nr 515/97 av den 13 mars 1997 om ömsesidigt bistånd mellan medlemsstaternas administrativa myndigheter och om samarbete mellan dessa och kommissionen för att säkerställa en korrekt tillämpning av tull- och jordbrukslagstiftningen, 2009/917/RIF av den 30 november 2009 om användning av informationsteknik för tulländamål, EUT 2009 L 323 (*TIS-beslutet*).

Informationen i TIS innefattar personuppgifter rörande varor, transportmedel, företag, personer, gods och kontanter som lagrats, beslagtagits eller konfiskerats. Informationen får endast användas i syfte att upptäcka, rapportera eller genomföra särskilda inspektioner eller för strategiska eller operativa analyser rörande personer som misstänks för att ha brutit mot tullagstiftningen.

Tillträde till TIS beviljas för nationella myndigheter inom tull, beskattning, jordbruk, folkhälsa och polis, samt till Europol och Eurojust.

Behandlingen av personuppgifter måste överensstämma med de specifika regler som inrättats genom förordning 515/97 och TIS-konventionen,[288] liksom bestämmelserna i dataskyddsdirektivet, dataskyddsförordningen, konvention 108 och rekommendationen om användning av personuppgifter inom polissektorn. Europeiska datatillsynsmannen är ansvarig för att se till att TIS följer förordning (EG) nr 45/2001 och kallar därför till ett möte minst en gång per år med samtliga nationella tillsynsmyndigheter inom skydd av personuppgifter som är behöriga för TIS-relaterade tillsynsfrågor.

288 *Ibid.*

8

Annan specifik europeisk lagstiftning om skydd av personuppgifter

EU	Frågor som täcks	Europarådet
Dataskyddsdirektivet Direktivet om sekretess och elektronisk kommunikation	Elektronisk kommunikation	Konvention 108 Rekommendation om telekommunikationstjänster
Dataskyddsdirektivet, artikel 8.2 b	Anställningsförhållanden	Konvention 108 Rekommendation om sysselsättning
		Europadomstolen, *Copland mot Förenade kungariket*, nr 62617/00, 3 april 2007
Dataskyddsdirektivet, artikel 8.3	Medicinska uppgifter	Konvention 108 Rekommendation om medicinska uppgifter
		Europadomstolen, *Z. mot Finland*, nr 22009/93, 25 februari 1997
Direktiv om kliniska försök	Kliniska försök	
Dataskyddsdirektivet, artikel 6.1 b och 6.1 e, artikel 13.2	Statistik	Konvention 108 Rekommendation om statistiska uppgifter
Förordning (EG) nr 223/2009 om europeisk statistik EU-domstolen, C-524/06, *Huber mot Bundesrepublik Deutschland*, 16 december 2008	Officiell statistik	Konvention 108 Rekommendation om statistiska uppgifter

EU	Frågor som täcks	Europarådet
Direktiv 2004/39/EG om marknader för finansiella instrument Förordning (EU) nr 648/2012 om OTC-derivat, centrala motparter och transaktionsregister Förordning (EG) nr 1060/2009 om kreditvärderingsinstitut Direktiv 2007/64/EG om betaltjänster på den inre marknaden	**Finansiella uppgifter**	Konvention 108 Rekommendation 90(19) som används för betalningar och andra liknande åtgärder Europadomstolen, *Michaud mot Frankrike*, nr 12323/11, 6 december 2012

I flera instanser har särskilda rättsliga instrument antagits på europeisk nivå som tillämpar de allmänna reglerna i konvention 108 eller i dataskyddsdirektivet mer i detalj på specifika situationer.

8.1. Elektronisk kommunikation

Viktiga punkter

- Specifika regler om skydd av personuppgifter inom området telekommunikation, med särskild hänvisning till telefontjänster, ingår i Europarådets rekommendation från 1995.
- Behandlingen av personuppgifter rörande tillhandahållande av kommunikationstjänster på EU-nivå regleras i direktivet om integritet och elektronisk kommunikation.
- Integritet när det gäller elektronisk kommunikation gäller inte enbart innehållet i ett meddelande utan även trafikuppgifter, såsom information om vem som kommunicerade med vem, när och hur länge, samt uppgifter om plats varifrån uppgifterna kommunicerades.

Kommunikationsnätverk riskerar att i allt större omfattning ingripa på ett omotiverat sätt i användarnas personliga sfär, eftersom de tillhandahåller ytterligare tekniska möjligheter för att lyssna på och övervaka kommunikation via sådana nätverk. Särskilda förordningar för skydd av personuppgifter bedömdes därför som nödvändiga för att bemöta de särskilda riskerna för användare av kommunikationstjänster.

1995 utfärdade Europarådet en rekommendation på telekommunikationsområdet, med särskild hänvisning till telefontjänster.[289] Enligt rekommendationen bör syftet med att samla in och behandla personuppgifter i samband med telekommunikationer begränsas till att ansluta en användare till nätverket, göra de särskilda telekommunikationstjänsterna tillgängliga, fakturera, kontrollera och säkerställa optimal teknisk drift samt utveckla nätverk och tjänster.

Särskild uppmärksamhet ägnades också åt användningen av kommunikationsnätverk för att sända direktmarknadsföringsmeddelanden. Som en generell regel får direktmarknadsföringsmeddelanden inte riktas till någon abonnent som uttryckligen har frånsagt sig att erhålla reklammeddelanden. Automatisk uppringningsutrustning för att överföra förinspelade reklammeddelanden kan användas endast om en abonnent uttryckligen har givit sitt samtycke. Inhemsk lag ska innehålla detaljerade regler på området.

När det gäller **EU:s rättsliga ram** antogs efter ett första försök 1997 direktivet om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (*direktivet om integritet och elektronisk kommunikation*) 2002 och det ändrades 2009, i syfte att komplettera och specificera bestämmelserna i dataskyddsdirektivet för telekommunikationssektorn.[290] Tillämpningen av direktivet om integritet och elektronisk kommunikation är begränsad till kommunikationstjänster i offentliga elektroniska nätverk.

I direktivet om integritet och elektronisk kommunikation urskiljs tre huvudkategorier av uppgifter som genereras vid kommunikation:

- uppgifter som utgör innehållet i de meddelanden som sänds vid kommunikation, dessa uppgifter är strikt konfidentiella;

289 Europarådet, ministerkommittén (1995), rekommendation Rec(95)4 till medlemsstaterna om skydd av personuppgifter på området telekommunikationstjänster, med särskild hänvisning till telefontjänster, 7 februari 1995.

290 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (*direktiv om integritet och elektronisk kommunikation*), EGT L 201, 31.7.2002, ändrat genom Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbete mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen, EUT L 337, 18.12.2009.

- de uppgifter som krävs för att upprätta och upprätthålla kommunikationen, så kallade trafikuppgifter, såsom information om kommunikationspartner, tid och kommunikationens varaktighet;

- inom trafikuppgifterna finns uppgifter som specifikt rör placeringen av kommunikationsutrustningen, så kallade lokaliseringsuppgifter och dessa uppgifter utgör samtidigt uppgifter om lokaliseringen *av användarna* av kommunikationsutrustningen och är särskilt relevant rörande användare av mobilkommunikationsutrustning.

Trafikuppgifter kan användas av tjänsteleverantören endast för fakturering och för att tekniskt tillhandahålla tjänsten. Efter samtycke från den registrerade kan emellertid dessa uppgifter lämnas till andra registeransvariga som erbjuder mervärdestjänster, exempelvis att lämna information i förhållande till var användaren befinner sig, var närmaste tunnelbanestation eller apotek finns eller väderprognos för platsen.

Annan tillgång till uppgifter om kommunikationer inom elektroniska nätverk, såsom tillgång för att undersöka brott, måste i enlighet med artikel 15 i direktivet om integritet och elektronisk kommunikation uppfylla kraven på berättigat ingripande i rätten till skydd av personuppgifter i enlighet med artikel 8.2 i Europakonventionen och bekräftat av stadgan i dess artikel 8 och 52.

Genom ändringarna från 2009 i direktivet om integritet och elektronisk kommunikation[291] infördes följande:

- Restriktionerna när det gäller att skicka ut e-post som direktmarknadsföring har utvidgats till sms-tjänster, tjänster för multimediameddelanden och andra slag av liknande tillämpningar. Marknadsföring via epost är förbjudet om inte samtycke lämnats i förväg. Utan detta samtycke får endast tidigare kunder kontaktas med marknadsföring via e-post om de har lämnat ut sin e-postadress och inte invänder.

291 Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbete mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen, EUT 2009 L 337.

- Medlemsstaterna är skyldiga att se till att rättsliga åtgärder kan vidtas vid överträdelser av förbudet mot icke begärd kommunikation.[292]

- Införande av cookies, programvara som övervakar och registrerar en datoranvändares åtgärder, är inte längre tillåtet utan användarens samtycke. Nationell lag bör mer i detalj reglera hur samtycke ska uttryckas och erhållas för att erbjuda tillräckligt skydd.[293]

Om överträdelse av uppgifter uppstår som ett resultat av otillåtet tillträde, förlust eller förstörelse av uppgifter måste den behöriga tillsynsmyndigheten omedelbart informeras. Abonnenterna måste informeras om en eventuell skada för dem är en konsekvens av överträdelse av uppgifter.[294]

Direktivet om lagring av uppgifter[295] (upphävt den 8 april 2014) tvingade leverantörer av kommunikationstjänster att hålla trafikuppgifter tillgängliga, särskilt i syfte att bekämpa allvarliga brott, under en period av minst sex och högst 24 månader, oavsett om leverantören fortfarande behövde uppgifterna för fakturering eller för att tekniskt tillhandahålla tjänsten.

EU:s medlemsstater ska utse oberoende offentliga myndigheter som är ansvariga för att övervaka säkerheten för lagrade uppgifter.

Lagring av telekommunikationsuppgifter är ett tydligt intrång i rätten till skydd av personuppgifter.[296] Huruvida detta intrång är motiverat har ifrågasatts i flera domstolsförfaranden i EU:s medlemsstater.[297]

---

292 Se det ändrade direktivet, artikel 13.

293 Se *Ibid.,* artikel 5, se även artikel 29-gruppen (2012), *Yttrande 04/2012 om undantag från krav på samtycke till kakor (cookies)*, WP 194, Bryssel, 7 juni 2012.

294 Se även artikel 29-gruppen (2011), *arbetsdokument 01/2011 om den aktuella ramen för EU:s överträdelse av personuppgifter och rekommendationer inför framtida policyutveckling*, WP 184, Bryssel, 5 april 2011.

295 Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, EUT 2006 L 105.

296 Europeiska datatillsynsmannen (2011), *Yttrande om utvärderingsrapporten från kommissionen till rådet och Europaparlamentet om datalagringsdirektivet (direktiv 2006/24/EG)*, 31 maj 2011.

297 Tyskland, förbundsförfattningsdomstolen (*Bundesverfassungsgericht*), *1 BvR 256/08*, 2 mars 2010, Rumänien, den federala författningsdomstolen (*Curtea Constituțională a României*), *nr 1258*, 8 oktober 2009, Tjeckien, författningsdomstolen (*Ústavní soud České republiky*), *94/2011 Coll.*, 22 mars 2011.

Exempel: I målet *Digital Rights Ireland och Seitlinger m.fl.* [298] förklarade EU-domstolen att datalagringsdirektivet var ogiltigt. Enligt domstolen är ”direktivets omfattande och särskilt allvarliga intrång i de grundläggande rättigheterna i frågan inte tillräckligt begränsade för att säkerställa att intrånget faktiskt är begränsat till det strikt nödvändiga.”

En avgörande fråga i samband med elektronisk kommunikation är de offentliga myndigheternas ingripande. Att övervaka eller avlyssna kommunikation, exempelvis med avlyssningsutrustning, är tillåtet endast om detta är tillåtet enligt lag och om det utgör en nödvändig åtgärd i ett demokratiskt samhälle för att skydda statens säkerhet, allmän säkerhet eller statens valutaintressen, eller förbjuda brott eller skydda den registrerade eller andra personers rättigheter och friheter.

Exempel: I målet *Malone mot Förenade kungariket*[299] hade den klagande anklagats för en rad brott rörande oärlig hantering av stulna varor. Under rättegången framkom det att en av den klagandes telefonkonversationer hade avlyssnats med hjälp av en fullmakt utfärdad av Secretary of State for the Home Department. Även om det sätt på vilket den klagandes kommunikation hade avlyssnats var tillåten enligt inhemsk lag ansåg Europadomstolen att det inte hade funnits några rättsliga regler rörande omfattning och sätt att utöva den bestämmanderätt som de offentliga myndigheterna åtnjöt på området, och att avlyssningen, som var ett resultat av förekomsten av praxisen i fråga, därför inte hade skett ”i enlighet med lagen”. Domstolen ansåg därför att artikel 8 i Europakonventionen hade överträtts.

8.2. Anställningsuppgifter

Viktiga punkter

- Särskilda regler för skydd av personuppgifter i relationen mellan arbetstagare och arbetsgivare ingår i Europarådets rekommendation om skydd för personuppgifter som används för ändamål som rör anställning.
- I dataskyddsdirektivet hänvisas särskilt till anställningsförhållanden endast i samband med behandling av känsliga uppgifter.

298 EU-domstolen, förenade målen C-293/12 och C-594/12, *Digital Rights Irland och Seitling m.fl.*, 8 april 2014, punkt 65.

299 Europadomstolen, *Malone mot Förenade kungariket*, nr 8691/79, 26 april 1985.

- Giltigheten i ett fritt samtycke som en rättslig grund för att behandla uppgifter om anställda kan vara tveksamt med tanke på den ekonomiska obalansen mellan arbetsgivare och anställd. Omständigheterna kring samtycket måste bedömas noggrant.

Det finns ingen specifik rättslig ram inom EU som styr behandling av personuppgifter i samband med anställning. I dataskyddsdirektivet hänvisas särskilt till anställningsförhållanden endast i artikel 8.2 i direktivet som handlar om behandling av känsliga uppgifter. Vad gäller Europarådet utfärdades rekommendationen om skydd för personuppgifter som används för ändamål som rör anställning 1989 och den uppdateras för närvarande.[300]

En undersökning av de vanligaste dataskyddsproblemen som är specifika för anställningar finns i ett arbetsdokument från artikel 29-gruppen.[301] Arbetsgruppen analyserade betydelsen av samtycke som rättslig grund för att behandla anställningsuppgifter.[302] Arbetsgruppen fann att den ekonomiska obalansen mellan arbetsgivaren som ber om samtycke och den anställda som ger sitt samtycke ofta reser tvivel om huruvida samtycket lämnades frivilligt eller ej. De omständigheter under vilka samtycke begärs bör därför övervägas noggrant vid bedömning av giltigheten av samtycke i samband med anställningar.

Ett vanligt problem med dataskydd i dagens representativa arbetsmiljö är den berättigade utvidgningen av övervakning av de anställdas elektroniska kommunikation på arbetsplatsen. Det hävdas ofta att problemet enkelt kan lösas genom att förbjuda privat användning av kommunikationsutrustning på arbetet. Ett sådant allmänt förbud kan emellertid bli oproportionerlig och orealistisk. Följande dom från Europadomstolen är särskilt intressant i detta sammanhang:

300 Europarådet, ministerkommittén (1989), *Recommendation R (89) 2 on the protection of personal data used for employment purposes*, 18 januari 1989. Se dessutom den rådgivande kommittén till 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 (undersökning av rekommendation nr R (89) 2 om skydd av personuppgifter som användas i anställningssyfte och för att lämna förslag till revidering av ovannämnda rekommendation), 9 september 2011.

301 Artikel 29-arbetsgruppen (2001), Opinion 8/2001 on the processing of personal data in the employment context, , WP 48, Bryssel, 13 september 2001.

302 Artikel 29-arbetsgruppen (2005), *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, WP 114, Bryssel, 25 november 2005.

Exempel: I målet *Coplant mot Förenade kungariket*[303] övervakades i hemlighet en högskoleanställds telefon-, epost- och internetanvändning för att ta reda på om hon i alltför stor utsträckning använde högskolans lokaler/utrustning i personligt syfte. Europadomstolen hävdade att telefonsamtal från affärslokaler omfattades av begreppen privatliv och korrespondens. Dessa samtal och e-postmeddelanden från arbetet, liksom information från övervakning av personlig internetanvändning, skyddades av artikel 8 i Europakonventionen. I den klagandes fall fanns inga bestämmelser som reglerade omständigheterna enligt vilka arbetsgivare kunde övervaka anställdas användning av telefon, e-post och internet. Ingripandet var därför inte i enlighet med lagen. Domstolen drog slutsatsen att artikel 8 i Europakonventionen hade överträtts.

Enligt Europarådets rekommendation om sysselsättning bör personuppgifter som samlas in om anställda erhållas direkt från den enskilda anställda.

Personuppgifter som samlas in för rekrytering måste begränsas till information som krävs för att utvärdera de klagandes lämplighet och deras möjligheter till karriär.

I rekommendationen nämns också specifikt uppgifter om domar rörande enskilda anställdas prestation eller potential. Uppgifter om domar måste baseras på korrekta och ärliga utvärderingar och får inte formuleras på ett förolämpande sätt. Detta framgår av principerna om rättvis behandling av uppgifter och korrekta uppgifter.

En specifik aspekt av dataskyddslagstiftningen i relationen mellan arbetsgivare och anställd är den roll den anställdas representant har. Dessa representanter kan få personuppgifter från anställda endast om det är nödvändigt för att de ska kunna representera de anställdas intressen.

Känsliga personuppgifter som samlas in i anställningssyfte får endast behandlas i särskilda fall och enligt de garantier som fastställts i inhemsk lag. Arbetsgivare kan fråga anställda eller arbetssökande om deras hälsostatus eller låta dem läkarundersökas endast om det är nödvändigt för att fastställa deras lämplighet för anställningen, uppfylla kraven på förebyggande vård eller göra det möjligt att bevilja sociala förmåner. Hälsouppgifter får inte samlas in från andra källor än den berörda anställda utom om uttryckligt och informerat samtycke erhållits eller om det föreskrivs i nationell lag.

303 Europadomstolen, *Copland mot Förenade kungariket*, nr 62617/00, 3 april 2007.

Enligt rekommendationen om anställning ska anställda informeras om syftet med behandlingen av deras personuppgifter, typen av personuppgifter som lagras, de enheter till vilka uppgifterna regelbundet skickas och syfte och den rättsliga grunden för denna kommunikation. Arbetsgivarna ska också informera sina anställda i förväg om införande eller anpassning av automatiska system för behandling av anställdas personuppgifter eller för övervakning av de anställdas förflyttningar eller produktivitet.

De anställda måste ha rätt att få tillgång till sina anställningsuppgifter liksom rätt att ändra eller radera dem. Om uppgifter om domar behandlas måste de anställda dessutom ha rätt att bestrida domen. Dessa rättigheter kan emellertid begränsas tillfälligt vid interna utredningar. Om en anställd nekas tillträde, ändring eller radering av personuppgifter om anställningen måste nationell lag tillhandahålla lämpliga förfaranden för att bestrida nekandet.

8.3. Medicinska uppgifter

Viktig punkt

- Medicinska uppgifter är känsliga uppgifter och omfattas därför av särskilt skydd.

Personuppgifter rörande den registrerades hälsotillstånd räknas som känsliga uppgifter enligt artikel 8.1 i dataskyddsdirektivet och enligt artikel 6 i konvention 108. Medicinska uppgifter omfattas i sin tur av striktare regler för behandling av uppgifter än icke känsliga uppgifter.

Exempel: I målet *Z. mot Finland*[304] hade den klagandes ex-make, som var smittad med hiv, begått ett antal sexualbrott. Han dömdes sedan för dråp eftersom han medvetet hade utsatt sina offer för risken att infekteras av hiv. Den nationella domstolen krävde att den fullständiga domen och handlingarna i målet skulle vara sekretessbelagda i tio år trots krav från den klagande om en längre sekretessperiod. Dessa krav avvisades av appellationsdomstolen, och domen

304 Europadomstolen, *Z. mot Finland*, nr 22009/93, 25 februari 1997, punkterna 94 och 112, se även Europadomstolen, *M.S. mot Sverige*, nr 20837/92, 27 augusti 1997; Europadomstolen, *L.L. mot Frankrike*, nr 7508/02, 10 oktober 2006, Europadomstolen, *I. mot Finland*, nr 20511/03, 17 juli 2008, Europadomstolen, *K.H. m.fl. mot Slovakien*, nr 32881/04, 28 april 2009, Europadomstolen, *Szuluk mot Förenade kungariket*, nr 36936/05, 2 juni 2009.

innehöll både den klagandes och hennes ex-makes fullständiga namn. Europadomstolen ansåg att ingripandet inte betraktades som nödvändigt i ett demokratiskt samhälle, eftersom skyddet av medicinska uppgifter var av grundläggande betydelse för rätten till respekt för privat- och familjeliv, särskilt när det gäller information om hiv-infektioner, med tanke på det stigma som är förbundet med sjukdomen i många samhällen. Domstolen drog därför slutsatsen att tillgång till den klagandes identitet och medicinska tillstånd, såsom det beskrevs i appellationsdomstolens dom efter en period om endast tio år efter domen, skulle innebära en överträdelse av artikel 8 i Europakonventionen.

Artikel 8.3 i dataskyddsdirektivet medger behandling av medicinska uppgifter när detta krävs för förebyggande vård, medicinsk diagnos, tillhandahållande av vård eller behandling eller hantering av hälsovårdstjänster. Behandling är emellertid endast tillåten när den utförs av vårdpersonal som omfattas av skyldigheten till tystnadsplikt, eller av en person som omfattas av en liknande skyldighet.[305]

Europarådets rekommendation om medicinska uppgifter från 1997 tillämpar principerna i konvention 108 på behandling av uppgifter på det medicinska området mer i detalj.[306] De föreslagna reglerna är i linje med dem i dataskyddsdirektivet när det gäller berättigade syften för att behandla medicinska uppgifter, de nödvändiga skyldigheterna till tystnadsplikt för personer som använder hälsouppgifter och de registrerades rätt till öppenhet och tillgång, ändring och radering. Medicinska uppgifter som får hanteras av vårdpersonal får inte överföras till rättsvårdande myndigheter om inte tillräckliga garantier för att förebygga spridning som inte överensstämmer med respekten för privatlivet som garanteras enligt artikel 8 i Europakonventionen tillhandahålls.[307]

Rekommendationen om medicinska uppgifter innehåller dessutom särskilda bestämmelser om medicinska uppgifter om ofödda barn och funktionshindrade personer, och om behandling av genetiska uppgifter. Vetenskaplig forskning erkänns uttryckligen som ett skäl för att bevara uppgifter längre än de egentligen behövs, även om detta vanligtvis kräver anonymisering. I artikel 12 i rekommendationen om medicinska uppgifter föreslås detaljerade regler för situationer där forskare behöver personuppgifter och anonymiserade uppgifter inte är tillräckliga.

305 Se även Europadomstolen, *Biriuk mot Litauen*, nr 23373/03, 25 november 2008.

306 Europarådet, ministerkommittén (1997), rekommendation Rec (97)5 till medlemsstaterna om skydd av medicinska uppgifter, 13 februari 1997.

307 Europadomstolen, nr 1585/09, *Avilkina m.fl. mot Ryssland*, nr 1585/09, 6 juni 2013, punkt 53 (ej slutlig).

Pseudonymisering kan vara ett lämpligt sätt att uppfylla vetenskapliga behov och samtidigt skydda de berörda patienternas intressen. Begreppet pseudonymisering i samband med skydd av personuppgifter förklaras mer i detalj i avsnitt 2.1.3.

På nationell och europeisk nivå har intensiva diskussioner ägt rum om initiativ för att lagra uppgifter om medicinsk behandling av en patient i en elektronisk journal.[308] En särskild aspekt av nationsomfattande system för elektroniska journaler är deras tillgänglighet över gränserna – ett ämne av särskilt intresse inom EU när det gäller gränsöverskridande hälsovård.[309]

Ett annat område som diskuteras rörande nya bestämmelser är kliniska försök, med andra ord utprovning av nya läkemedel på patienter i en dokumenterad forskningsmiljö, även detta ämne har avsevärd inverkan på skyddet av personuppgifter. Kliniska prövningar av humanläkemedel regleras genom Europaparlamentets och rådets direktiv 2001/20/EG av den 4 april 2001 om tillnärmning av medlemsstaternas lagar och andra författningar rörande tillämpning av god klinisk sed vid kliniska prövningar av humanläkemedel (*direktivet om kliniska prövningar*).[310] I december 2012 föreslog Europeiska kommissionen en förordning som skulle ersätta direktivet om kliniska försök i syfte att göra prövningar mer enhetliga och effektiva.[311]

Ytterligare lagstiftningsinitiativ och andra initiativ pågår på EU-nivå rörande personuppgifter inom hälsovårdssektorn.[312]

308 Artikel 29-gruppen (2007), *arbetsdokument om behandling av personuppgifter om hälsa i elektroniska journaler (EHR)*, WP 131, Bryssel, 15 februari 2007.

309 Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpning av patienters rättigheter vid gränsöverskridande hälsovård, EUT 2011 L 88.

310 Europaparlamentets och rådets direktiv 2001/20/EG av den 4 april 2001 om tillnärmning av medlemsstaternas lagar och andra författningar rörande tillämpning av god klinisk sed vid kliniska prövningar av humanläkemedel, EGT 2001 L 121.

311 Europeiska kommissionen (2012), *Europaparlamentets och rådets förslag till förordning om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG*, COM(2012) 369 final, Bryssel, 17 juli 2012.

312 Europeiska datatillsynsmannen (2013), *Europeiska datatillsynsmannens yttrande om meddelandet från kommissionen om "handlingsplan för e-hälsa 2012–2020 – Innovativ hälsovård för det 21:a århundradet"*, Bryssel, 27 mars 2013.

8.4. Behandling av uppgifter i statistiskt syfte

Viktiga punkter

- Uppgifter som samlas in i statistiksyfte får inte användas i något annat syfte.
- Uppgifter som samlats in på ett korrekt sätt, oavsett syfte, får användas även för statistiska ändamål, under förutsättning att nationell lag föreskriver lämpliga garantier som användarna tillämpar. För detta syfte bör framför allt anonymisering och pseudonymisering före överföring till tredje part planeras.

I dataskyddsdirektivet nämns behandling av uppgifter för statistiska syften i samband med möjliga undantag från dataskyddsprinciperna. I artikel 6.1 b i direktivet kan principen om begränsning av syftet undvikas i nationell lag till förmån för ytterligare användning av uppgifterna för statistiska syften, även om alla nödvändiga garantier också måste ingå i nationell lag. Enligt artikel 13.2 i direktivet medges begränsningar av tillträdesrätten i nationell lag om uppgifterna behandlas enbart för statistiska syften, men även då måste garantier finnas enligt nationell lag. I detta sammanhang innehåller dataskyddsdirektivet ett specifikt krav på att inga av de uppgifter som förvärvas eller skapas under statistisk forskning får användas för konkreta beslut om de registrerade.

Även om uppgifter som samlats in lagenligt av en registeransvarig, oavsett syfte, kan återanvändas av denna registeransvarigas för egna statistiska syften – så kallad sekundär statistik – skulle uppgifterna behöva anonymiseras eller pseudonymiseras, beroende på sammanhanget, innan de överförs till en tredje part för statistiska syften, om inte den registrerade har samtyckt till det eller det särskilt föreskrivs i nationell lag. Detta följer av kravet på lämpliga garantier enligt artikel 6.1 b i dataskyddsdirektivet.

De viktigaste fallen med användning av uppgifter för statistiska syften är officiell statistik, som utförs av nationella statistikbyråer eller EU:s statistikbyrå, baserat på nationell lagstiftning och EU-lagstiftning om officiell statistik. Enligt dessa lagar är medborgare och företag vanligtvis skyldiga att lämna uppgifter till statistikmyndigheterna. Tjänstemän vid statistikbyråer omfattas av särskilda skyldigheter när det gäller tystnadsplikt som noggrant följs, eftersom de är avgörande för den höga nivå av tillit från medborgarna som krävs om uppgifter ska göras tillgängliga för statistikmyndigheterna.

Förordning (EG) nr 223/2009 om europeisk statistik (nedan kallad *EU:s statistikförordning*) innehåller grundläggande regler för skydd av personuppgifter i officiell statistik och kan därför även anses relevant för bestämmelser om officiell statistik på nationell nivå.[313] I förordningen bibehålls principen att officiell statistikverksamhet behöver en tillräckligt exakt rättslig grund.[314]

> Exempel: I målet *Huber mot Bundesrepublik Deutschland*[315] ansåg EU-domstolen att en myndighets insamling och lagring av personuppgifter för statistiska syften inte var tillräckliga skäl i sig för att behandlingen skulle vara tillåten. Lagen som möjliggör behandling av personuppgifter behövde också uppfylla kravet på nödvändighet vilket inte var fallet i det aktuella sammanhanget.

Inom Europarådet omfattar rekommendationen om statistiska uppgifter som utfärdades 1997 utförande av statistik inom den offentliga och privata sektorn.[316] Genom rekommendationen infördes principer som sammanfaller med huvudreglerna i dataskyddsdirektivet som beskrivs ovan. Mer detaljerade regler ges rörande följande frågor.

Uppgifter som samlats in av en registeransvarig i statistiksyfte får inte användas för andra syften, medan uppgifter som samlats in för icke-statistiska syften ska vara tillgängliga för ytterligare statistisk användning. Rekommendation om statistiska uppgifter tillåter till och med vidarebefordran av uppgifter till tredje part om det endast är för statistiska syften. I dessa fall bör parterna komma överens och skriva ned omfattningen av den berättigade ytterligare användningen för statistik. Eftersom detta inte kan ersätta den registrerades samtycke får det antas att det måste finna ytterligare lämpliga garantier i nationell lag för att minimera riskerna för missbruk av personuppgifter, såsom en skyldighet att anonymisera eller pseudonymisera uppgifterna före överföring.

313 Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program, EUT 2009 L 87.

314 Principen ska anges mer i detalj i Eurostats uppförandekod, som i enlighet med artikel 11 i förordningen om europeisk statistik innehåller etiska riktlinjer för hur officiell statistik ska utföras, inbegripet hänsynsfull användning av personuppgifter, tillgänglig på: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 EU-domstolen, C-524/06, *Huber mot Bundesrepublik Deutschland*, 16 december 2008, se särskilt punkt 68.

316 Europarådet, ministerkommittén (1997), rekommendation Rec (97)18 till medlemsstaterna om skydd av personuppgifter som samlas in och bearbetas i statistiksyfte, 30 september 1997.

Människor som yrkesmässigt hanterar statistisk forskning bör omfattas av särskilda skyldigheter när det gäller tystnadsplikt – som är representativ för officiell statistik – enligt nationell statistik. Detta bör utvidgas även till intervjuare, om de arbetar med att samla in uppgifter från registrerade eller andra personer.

Om en statistisk undersökning som använder personuppgifter inte föreskrivs i lagen skulle de registrerade behöva samtycka till användning av deras uppgifter för att berättiga det, eller skulle åtminstone få möjlighet att invända. Om personuppgifter samlas in för statistiksyften genom intervjuer med personer måste dessa personer tydligt informeras om huruvida det är obligatoriskt att lämna uppgifter enligt nationell lag. Känsliga uppgifter bör aldrig samlas in på ett sådant sätt att en individ kan identifieras om det inte uttryckligen är tillåtet enligt nationell lag.

Om en statistisk undersökning inte kan utföras utan anonyma uppgifter, och personuppgifter är absolut nödvändiga, bör de uppgifter som samlas in i detta syfte anonymiseras så snart det är möjligt. Resultatet av den statistiska undersökningen får åtminstone inte möjliggöra identifiering av de registrerade, om det inte är uppenbart att det inte utgör någon risk.

Efter att den statistiska analysen har avslutats ska de personuppgifter som använts antingen raderas eller göras anonyma. I detta fall föreslås i rekommendationen om statistiska uppgifter att uppgifter som kan identifiera en person ska lagras separat från andra personuppgifter. Det innebär exempelvis att uppgifterna bör pseudonymiseras och antingen krypteringsnyckeln eller förteckningen över identifierande synonymer bör förvaras separat från de pseudonymiserade uppgifterna.

8.5. Finansiella uppgifter

Viktiga punkter

- Även om finansiella uppgifter inte är känsliga uppgifter i den mening som avses i konvention 108 eller i dataskyddsdirektivet krävs särskilda garantier vid behandling av uppgifter för att trygga korrekthet och datasäkerhet.
- Elektroniska betalningssystem behöver ha inbyggt dataskydd, så kallat inbyggt integritetsskydd.
- Särskilda dataskyddsproblem uppstår genom behovet av att inrätta lämpliga mekanismer för autentisering.

Exempel: I målet *Michaud mot Frankrike*[317] ifrågasatte den klagande, en fransk advokat, skyldigheten att rapportera misstankar om att hans klienter eventuellt bedrev penningtvätt. Europadomstolen noterade att kravet på att advokater till de administrativa myndigheterna ska vidarebefordra information om en annan person som de fått kännedom om genom utbyte med den personen utgör ett intrång i advokaternas rätt till respekt för sin korrespondens och sitt privatliv enligt artikel 8 i Europakonventionen, eftersom begreppet omfattade yrkesmässig verksamhet eller affärsverksamhet. Ingripandet var emellertid i enlighet med lagen och hade ett berättigat syfte, nämligen att förhindra oordning och brott. Eftersom advokater var skyldiga att rapportera misstankar endast under mycket begränsade förhållanden ansåg Europadomstolen att skyldigheten var proportionerlig och drog slutsatsen att artikel 8 inte hade överträtts.

En tillämpning av den allmänna rättsliga ramen för dataskydd på betalningar, enligt konvention 108, utarbetades av Europarådet i rekommendation Rec (90)19 från 1990.[318] I rekommendationen klargörs användning av tillåten insamling och användning av uppgifter när det gäller betalningar, särskilt med hjälp av betalkort. Där föreslås dessutom för de inhemska lagstiftarna detaljerade förordningar om begränsning när det gäller att lämna betalningsuppgifter till tredje part, om tidsgränser för bevarande av uppgifter, öppenhet, dataskydd och gränsöverskridande flöde av uppgifter och slutligen om tillsyn och prövning. De föreslagna lösningarna motsvarar vad som senare tillhandahölls som EU:s allmänna ram för skyddet av personuppgifter i dataskyddsdirektivet.

Ett antal rättsliga instrument skapas för att reglera marknader för finansiella instrument och verksamheten vid kreditinstitut och investeringsföretag.[319] Andra rättsliga

317 Europadomstolen, *Michaud mot Frankrike*, nr 12323/11, 6 december 2012; se även Europadomstolen, *Niemietz mot Tyskland*, nr 13710/88, 16 december 1992, punkt 29, och Europadomstolen, *Halford mot Förenade kungariket*, nr 20605/92, 25 juni 1997, punkt 42.

318 Europarådet, ministerkommittén (1990), rekommendation nr R (90)19 om skydd av personuppgifter som används vid betalningar och andra tillhörande åtgärder, 13 september 1990.

319 Europeiska kommissionen (2011), *Europaparlamentets och rådets förslag om marknader för finansiella instrument och om upphävande av Europaparlamentets och rådets direktiv 2004/39/EG*, KOM(2011) 656 slutlig, Bryssel, 20 oktober 2011; Europeiska kommissionen (2011), *Europaparlamentets och rådets förslag till förordning om marknader för finansiella instrument och om ändring av förordning [EMIR] om OTC-derivat, centrala motparter och transaktionsregister*, KOM(2011) 652 slutlig, Bryssel, 20 oktober 2011; Europeiska kommissionen (2011), *Europaparlamentets och rådets förslag till direktiv om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag samt om ändring av Europaparlamentets och rådet direktiv 2002/87/EG om extra tillsyn över kreditinstitut, försäkringsföretag och värdepappersföretag i ett finansiellt konglomerat*, KOM(2011) 453 slutlig, Bryssel, 20 juli 2011.

instrument bistår i kampen mot insiderhandel och marknadsmanipulation.[320] De mest kritiska frågorna inom dessa områden som påverkar dataskyddet är följande:

- lagring av register över finansiella transaktioner;
- överföring av personuppgifter till tredjeländer;
- inspelning av telefonsamtal eller registrering av elektronisk kommunikation, inbegripet möjlighet för behöriga myndigheter att begära ut register över telefon- och datatrafik;
- spridning av personuppgifter, inbegripet offentliggörande av straff;
- behöriga myndigheters befogenhet när det gäller tillsyn och utredning, inklusive inspektioner på plats, samt tillträde till privata lokaler för att beslagta handlingar;
- mekanismer för att rapportera överträdelser, dvs. system för visselblåsning;
- samarbete mellan behöriga myndigheter i medlemsstaterna och Europeiska värdepappers- och marknadsmyndigheten (Esma).

Det finns också andra frågor inom dessa områden som särskilt tas upp, bland annat insamling av uppgifter om de registrerades ekonomiska ställning[321] eller gränsöverskridande betalning via banköverföring, vilket oundvikligen medför flöden av personuppgifter.[322]

320 Europeiska kommissionen (2011), *Europaparlamentets och rådets förordning om insiderhandel och marknadspåverkan (marknadsmissbruk),* KOM(2011) 651 slutlig, Bryssel, 20 oktober 2011; Europeiska kommissionen (2011), *förslag till Europaparlamentets och rådets direktiv om straffrättsliga påföljder för insiderhandel och otillbörlig marknadspåverkan,* KOM(2011) 654 slutlig, Bryssel, 20 oktober 2011.

321 Europaparlamentets och rådets förordning (EG) nr 1060/2009 av den 16 september 2009 om kreditvärderingsinstitut, EUT 2009 L 302, Europeiska kommissionen, *Europaparlamentets och rådets förslag till förordning om ändring av förordning (EG) nr 1060/2009 om kreditvärderingsinstitut*, KOM(2010) 289 slutlig, Bryssel, 2 juni 2010.

322 Europaparlamentets och rådets direktiv 2007/64/EG av den 13 november 2007 om betaltjänster på den inre marknaden och om ändring av direktiven 97/7/EG, 2002/65/EG, 2005/60/EG och 2006/48/EG samt upphävande av direktiv 97/5/EG, EUT 2007 L 319.

Ytterligare läsning

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*, Bryssel, tillgänglig på: http://www.edri.org/files/paper06_datap.pdf.

Frowein, J. och Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. och 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. och Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. och Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bryssel, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, nr 5, s. 281–288.

Warren, S. och Brandeis, L. (1890), "The right to privacy", *Harvard Law Review,* Vol. 4, nr 5, s. 193–220, tillgänglig på: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. och 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. och 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. och 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*, tillgänglig 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" in: Grabitz, E., Hilf, M. and 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*, Saarbrucken, Éditions universitaires européennes.

Dammann, U. och Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Europeiska unionens byrå för grundläggande rättigheter) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburg, Publications Office of the European Union (Publikationsbyrån).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Wien, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburg, Publikationsbyrån.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, tillgänglig 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. och Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, 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*, Luxemburg, Publikationsbyrån, tillgänglig 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, Eurojust.

Drewer, D. och 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. och De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. och 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, tillgängligt på: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Kapitel 8

Büllesbach, A., Gijrath, S., Poullet, Y. och Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. och Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. och De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. och 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. och Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Rättspraxis

Utvald rättspraxis från Europadomstolen

Tillgång till personuppgifter

Gaskin mot Förenade kungariket, nr 10454/83, 7 juli 1989
Godelli mot Italien, nr 33783/09, 25 september 2012
K.H. m.fl. mot Slovakien, nr 32881/04, 28 april 2009
Leander mot Sverige, nr 9248/81, 26 mars 1987
Odièvre mot Frankrike [GC], nr 42326/98, 13 februari 2003

Avvägning av skydd av personuppgifter mot yttrandefrihet

Axel Springer AG mot Tyskland [GC], nr 39954/08, 7 februari 2012
Von Hannover mot Tyskland, nr 59320/00, 24 juni 2004
Von Hannover mot Tyskland (nr 2) [GC], nr 40660/08 och 60641/08, 7 februari 2012

Utmaningar inom skydd av personuppgifter på nätet

K.U. mot Finland, nr 2872/02, 2 december 2008

Korrespondens

Amann mot Schweiz [GC], nr 27798/95, 16 februari 2000
Bernh Larsen Holding AS m.fl. mot Norge, nr 24117/08, 14 mars 2013
Cemalettin Canli mot Turkiet, nr 22427/04, 18 november 2008
Dalea mot Frankrike, nr 964/07, 2 februari 2010
Gaskin mot Förenade kungariket, nr 10454/83, 7 juli 1989

Haralambie mot Rumänien, nr 21737/03, 27 oktober 2009
Khelili mot Schweiz, nr 16188/07, 18 oktober 2011
Leander mot Sverige, nr 9248/81, 26 mars 1987
Malone mot Förenade kungariket, nr 8691/79, 2 augusti 1984
McMichael mot Förenade kungariket, nr 16424/90, 24 februari 1995
M.G. mot Förenade kungariket, nr 39393/98, 24 september 2002
Rotaru mot Rumänien [GC], nr 28341/95, 4 maj 2000
S. och Marper mot Förenade kungariket, nr 30562/04 och 30566/04, 4 december 2008
Shimolovos mot Ryssland, nr 30194/09, 21 juni 2011
Turek mot Slovakien, nr 57986/00, 14 februari 2006

Databaser över brottsregister

B.B. mot Frankrike, nr 5335/06, 17 december 2009
M.M. mot Förenade kungariket, nr 24029/07, 13 november 2012

DNA-databaser

S. och Marper mot Förenade kungariket, nr 30562/04 och 30566/04, 4 december 2008

GPS-uppgifter

Uzun mot Tyskland, nr 35623/05, 2 september 2010

Hälsouppgifter

Biriuk mot Litauen, nr 23373/03, 25 november 2008
I. mot Finland, nr 20511/03, 17 juli 2008ashby
L.L. mot Frankrike, nr 7508/02, 10 oktober 2006
M.S. mot Sverige, nr 20837/92, 27 augusti 1997
Szuluk mot Förenade kungariket, nr 36936/05, 2 juni 2009
Z. mot Finland, nr 22009/93, 25 februari 1997

Identitet

Ciubotaru mot Moldavien, nr 27138/04, 27 april 2010
Godelli mot Italien, nr 33783/09, 25 september 2012
Odièvre mot Frankrike [GC], nr 42326/98, 13 februari 2003

Information om anställningar

Michaud mot Frankrike, nr 12323/11, 6 december 2012
Niemietz mot Tyskland, nr 13710/88, 16 december 1992

Avlyssning av kommunikation

Amann mot Schweiz [GC], nr 27798/95, 16 februari 2000
Copland mot Förenade kungariket, nr 62617/00, 3 april 2007
Cotlet mot Rumänien, nr 38565/97, 3 juni 2003
Kruslin mot Frankrike, nr 11801/85, 24 april 1990
Lambert mot Frankrike, nr 23618/94, 24 augusti 1998
Liberty m.fl. mot Förenade kungariket, nr 58243/00, 1 juli 2008
Malone mot Förenade kungariket, nr 8691/79, 2 augusti 1984
Halford mot Förenade kungariket, nr 20605/92, 25 juni 1997
Szuluk mot Förenade kungariket, nr 36936/05, 2 juni 2009

Skyldigheter för ansvariga

B.B. mot Frankrike, nr 5335/06, 17 december 2009
I. mot Finland, nr 20511/03, 17 juli 2008
Mosley mot Förenade kungariket, nr 48009/08, 10 maj 2011

Foton

Sciacca mot Italien, nr 50774/99, 11 januari 2005
Von Hannover mot Tyskland, nr 59320/00, 24 juni 2004

Rätt att bli bortglömd

Segerstedt-Wiberg m.fl. mot Sverige, nr 62332/00, 6 juni 2006

Rätt till invändning

Leander mot Sverige, nr 9248/81, 26 mars 1987
Mosley mot Förenade kungariket, nr 48009/08, 10 maj 2011
M.S. mot Sverige, nr 20837/92, 27 augusti 1997
Rotaru mot Rumänien, [GC], nr 28341/95, 4 maj 2000

Känsliga kategorier uppgifter

I. mot Finland, nr 20511/03, 17 juli 2008

Michaud mot Frankrike, nr 12323/11, 6 december 2012
S. och Marper mot Förenade kungariket, nr 30562/04 och 30566/04, 4 december 2008

Tillsyn och genomförande (olika aktörers roll, inklusive dataskyddsmyndigheter)

I. mot Finland, nr 20511/03, 17 juli 2008
K.U. mot Finland, nr 2872/02, 2 december 2008
Von Hannover mot Tyskland, nr 59320/00, 24 juni 2004
Von Hannover mot Tyskland (nr 2) [GC], nr 40660/08 och 60641/08, 7 februari 2012

Metoder för tillsyn

Allan mot Förenade kungariket, nr 48539/99, 5 november 2002
Association "21 Décembre 1989" m.fl. mot Rumänien, nr 33810/07 och 18817/08, 24 maj 2011
Bykov mot Ryssland [GC], nr 4378/02, 10 mars 2009
Kennedy mot Förenade kungariket, nr 26839/05, 18 maj 2010
Klass m.fl. mot Tyskland, nr 5029/71, 6 september 1978
Rotaru mot Rumänien [GC], nr 28341/95, 4 maj 2000
Taylor-Sabori mot Förenade kungariket, nr 47114/99, 22 oktober 2002
Uzun mot Tyskland, nr 35623/05, 2 september 2010
Vetter mot Frankrike, nr 59842/00, 31 maj 2005

Videoövervakning

Köpke mot Tyskland, nr 420/07, 5 oktober 2010
Peck mot Förenade kungariket, nr 44647/98, 28 januari 2003

Röstprov

P.G. och J.H. mot Förenade kungariket, nr 44787/98, 25 september 2001
Wisse mot Frankrike, nr 71611/01, 20 december 2005

Utvald rättspraxis från EU-domstolen

Rättspraxis rörande dataskyddsdirektivet

C-73/07, *Tietosuojavaltuutettu mot Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 december 2008
[Begreppet ”journalistisk verksamhet” i den mening som avses i artikel 9 i dataskyddsdirektivet]

Förenade målen C-92/09 och C-93/09, *Volker och Markus Schecke GbR och Hartmut Eifert mot Land Hessen*, 9 november 2010
[Proportionalitet i den rättsliga skyldigheten att offentliggöra personuppgifter om mottagare av vissa av EU:s jordbruksfonder]

C-101/01, *Bodil Lindqvist*, 6 november 2003
[En privatpersons berättigade offentliggörande av uppgifter om andras privatliv på internet]

C-131/12, *Google Spain, S.L., Google Inc. mot Agencia Española de Protección de Datos, Mario Costeja González*, Hänskjutning för förhandsavgörande från *Audiencia Nacional* (Spanien) inlämnad den 9 mars 2012, 25 maj 2012, ej avgjord
[Sökmotorleverantörers skyldighet att på den registrerades begäran avstå från att visa personuppgifter i sökresultaten]

C-270/11, *Europeiska kommissionen mot Sverige*, 30 maj 2013
[Böter för att inte ha införlivat ett direktiv]

C-275/06, *Productores de Música de España (Promusicae) mot Telefónica de España SAU*, 29 januari 2008
[Internetleverantörers skyldighet att lämna ut identiteten på användare av fildelningsprogrammet KaZaA till förening för skydd av immaterialrätt]

C-288/12, *Europeiska kommissionen mot Ungern*, 8 april 2014
[Berättigad förflyttning av den nationella datatillsynsmannens kontor]

C-291/12, *Michael Schwarz mot Stadt Bochum*, Generaladvokatens yttrande, 13 June 2013
[Överträdelse av EU:s primärrätt genom förordning (EG) 2252/2004 som föreskriver att fingeravtryck måste lagras i pass]

Förenade målen C-293/12 och C-594/12, *Digital Rights Ireland and Seitling m.fl.*, 8 april 2014
[Datalagringsdirektivets överträdelse av EU:s primärrätt]

C-360/10, *SABAM mot Netlog N.V.,* 16 februari 2012
[Sociala nätverksleverantörers skyldighet att förhindra nätanvändares otillåtna användning av musik och audiovisuella verk]

Förenade målen C-465/00, C-138/01 och C-139/01, *Rechnungshof mot Österreichischer Rundfunk m.fl. och Neukomm och Lauermann mot Österreichischer Rundfunk*, 20 maj 2003
[Proportionaliteten i den rättsliga skyldigheten att offentliggöra uppgifter om löner för anställda inom vissa kategorier av institutioner kopplade till den offentliga sektorn]

Förenade målen C-468/10 och C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado,* 24 november 2011
[Korrekt införlivande av artikel 7 f i dataskyddsdirektivet – ”andras berättigade intressen” – i nationell lag]

C-518/07, *Europeiska kommissionen mot Förbundsrepubliken Tyskland*, 9 mars 2010
[En nationell tillsynsmyndighets oberoende]

C-524/06, *Huber mot Bundesrepublik Deutschland*, 16 december 2008
[Berättigad lagring av uppgifter om utländska medborgare i ett statistikregister]

C-543/09, *Deutsche Telekom AG mot Bundesrepublik Deutschland*, 5 maj 2011
[Behovet av förnyat samtycke]

C-553/07, *College van burgemeester en wethouders van Rotterdam mot M.E.E. Rijkeboer*, 7 maj 2009
[Den registrerades rätt till tillgång till uppgifter]

C-614/10, *Europeiska kommissionen mot Republiken Österrike*, 16 oktober 2012
[Nationell tillsynsmyndighets oberoende]

Rättspraxis rörande dataskyddsförordningen

C-28/08 P, *Europeiska kommissionen mot The Bavarian Lager Co. Ltd*, 29 juni 2010
[Tillgång till handlingar]

C-41/00 P, *Interporc Im- und Export GmbH mot Europeiska gemenskapernas kommission*, 6 mars 2003
[Tillgång till handlingar]

F-35/08, *Dimitrios Pachtitis mot Europeiska kommissionen*, 15 juni 2010
[Användning av personuppgifter i samband med anställning vid EU:s institutioner]

F-46/09, *V. mot parlamentet*, 5 juli 2011
[Användning av personuppgifter i samband med anställning vid EU:s institutioner]

Innehållsförteckning

Rättspraxis från EU-domstolen

Rättspraxis från Europadomstolen

Rättspraxis från nationella domstolar

Europeiska unionens byrå för grundläggande rättigheter
Europarådet – Europeiska domstolen för de mänskliga rättigheterna

Handbok om den europeiska lagstiftningen om skydd av personuppgifter

2015 — 201 s. — 14,8 × 21 cm

ISBN 978-92-871-9932-4 (Europarådet)
ISBN 978-92-9239-499-8 (FRA)
doi:10.2811/73936

På internet finns mycket information om Europeiska unionens byrå för grundläggande rättigheter. Den nås via FRA:s webbplats på fra.europa.eu.

Mer information om Europarådet finns på internet på hub.coe.int.

Ytterligare information om Europadomstolen finns på domstolens webbplats: http://echr.coe.int. På sökportalen HUDOC finns domar och beslut på engelska och/eller franska, översättningar till ytterligare språk, rättsliga sammanfattningar, pressmeddelanden och annan information om domstolens arbete.

Hur hittar man EU:s publikationer?

Gratispublikationer
- Ett enskilt exemplar genom EU Bookshop (http://bookshop.europa.eu),
- Flera exemplar/affischer/kartor
  hos Europeiska unionens representationer (http://ec.europa.eu/represent_sv.htm),
  hos delegationer i länder utanför EU (http://eeas.europa.eu/delegations/index_sv.htm),
  genom att kontakta nätverket Europe Direct (http://europa.eu/europedirect/index_sv.htm)
  eller ringa 00 800 6 7 8 9 10 11 (gratis inom hela EU) (*).

Avgiftsbelagda publikationer
- Genom EU Bookshop (http://bookshop.europa.eu).

(*) Varken informationen eller samtalen kostar i regel något (men vissa operatörer, telefonkiosker och hotell kan ta betalt för samtalen).

Så här får du tillgång till Europarådets publikationer

Europarådets publikationsavdelning tar fram arbeten inom organisationens alla områden, bland annat mänskliga rättigheter, juridisk vetenskap, hälsa, etik, sociala frågor, miljö, utbildning, kultur, sport, ungdomsfrågor och arkitektoniskt arv. Böcker och elektroniska publikationer från den omfattande katalogen kan beställas på nätet (http://book.coe.int/).

I ett virtuellt läsrum kan användarna konsultera utdrag från de viktigaste arbetena som publicerats eller den fullständiga texten av vissa officiella handlingar kostnadsfritt.

Information om, liksom den fullständiga texten till, Europarådets konventioner finns på fördragskontorets webbplats: http://conventions.coe.int/.

10.2811/73936 TK-01-13-772-SV-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 snabba utvecklingen av informations- och kommunikationstekniken visar på det växande behovet av ett ordentligt skydd av personuppgifter – en rättighet som garanteras av instrument från både Europeiska unionen (EU) och Europarådet. Tekniska framsteg vidgar gränserna för exempelvis övervakning, kommunikation, avlyssning och lagring av uppgifter, och allt detta skapar betydande utmaningar för rätten till skydd av personuppgifter. Handboken är utformad för att jurister som inte är specialiserade inom dataskyddsområdet ska få kännedom om detta område inom juridiken. Den innehåller en översikt över EU:s och Europarådets tillämpliga rättsliga ramar. Den förklarar viktig rättspraxis och sammanfattar viktiga domar från både Europadomstolen och EU-domstolen. Om det inte finns någon rättspraxis ges praktiska illustrationer med hypotetiska scenarier. I korthet syftar handboken till att bidra till att säkerställa att rätten till skydd av personuppgifter upprätthålls kraftfullt och beslutsamt.

EUROPEISKA UNIONENS BYRÅ FÖR GRUNDLÄGGANDE RÄTTIGHETER
Schwarzenbergplatz 11 – 1040 Wien - Österrike
Tel. +43 (1) 580 30-60 – Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

EUROPARÅDET
EUROPADOMSTOLEN
67075 Strasbourg Cedex – Frankrike
Tel. +33 (0) 3 88 41 20 00 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Publikationsbyrån

ISBN 978-92-871-9932-4 (Europarådet)
ISBN 978-92-9239-499-8 (FRA)