RI.
SE

Vägledning om dataskydd

God integritet vid digital tjänste- och affärsutveckling

Del 1: Inledning
Reviderad version

Om författaren

Jonas Ledendal är jur.dr. och forskar om dataskyddsjuridik vid Institutionen för handelsrätt, Ekonomihögskolan, Lunds universitet. Han har tidigare deltagit i tre VINNOVA-projekt om öppna datakällor och har författat en handbok om handlingsoffentlighet och integritet i det digitala samhället tillsammans med Stefan Larsson och Joakim Wernberg.

Förord

Projektet ”Sjyst data!” syftar till att främja digital tjänste- och affärsutveckling med vad vi betecknar som god integritet. Centralt för detta arbete är EU:s dataskyddsförordning (GDPR), som blev tillämplig i Sverige och alla andra medlemsstater den 25 maj 2018. Fram till dess låg mycket av fokus på traditionell regelefterlevnad (”compliance”), men drygt ett halvår senare står det klart att dataskydd handlar om betydligt mer än att uppdatera sin personuppgifts-policy och hämta in nya samtycken. Det är nu det verkliga arbetet börjar med att hitta lösningar som förenar dataskydd med affärsnytta. Här ser vi att det krävs ny kunskap, bl.a. om hur rättsliga krav på information och inhämtande av samtycke ska kunna förenas med en god användarupplevelse och skapa den tillit som behövs för att slutanvändare ska känna sig trygga med att dela med sig av sin data.

För att användare ska kunna göra informerade val krävs enkla standardiserade (gärna maskinläsbara) symboler som ersätter långa och krångliga slutanvändaravtal. Det kommer också behövas någon form av integritetsmärkning, uppförandekoder och certifiering som säkerställer att digitala tjänster lever upp till kravet på god integritet. För att ett sådant system ska vara väl förankrat hos olika intressenter, både tjänsteleverantörer och slutanvändare, bygger projektet på ett brett konsortium av forskare och företag med gedigen kompetens och erfarenhet inom ett flertal områden, såsom digitala media, dataskyddsjuridik, marknads-undersökningar, telekommunikations- och nätverksteknologi.

I projektet deltar RISE Research Institutes of Sweden AB, Södertörns högskola, Malmö universitet, Lunds universitet, Bumbee Labs AB, IAB Sverige, Kantar SIFO, Sandvine AB, Skandinaviska Enskilda Banken AB, TS Mediefakta AB, Urban ICT Arena och Öresundskraft AB. Projektet finansieras med 10 miljoner kronor av Vinnova inom programmet Utmanings-driven innovation som är en satsning för att lösa samhällsutmaningar som kräver bred samverkan.

Håkan Cavenius

projektledare

Stockholm den 1 februari 2019

Europeiska unionens dataskyddsreglering

Europeiska unionens dataskyddsrätt innehåller regler om skydd av enskilda individers grundläggande fri- och rättigheter i samband med behandling av personuppgifter, men även det fria flödet av personuppgifter inom unionen. Dataskyddsrätten regleras i första hand genom EU:s allmänna dataskyddsförordning (GDPR), som blev direkt tillämplig i Sverige och alla andra medlemsstater den 25 maj 2018.

Europeiska unionens dataskyddsrätt

Europeiska unionens dataskyddsrätt innehåller regler om skydd av enskilda individers grundläggande fri- och rättigheter i samband med behandling av personuppgifter, men även det fria flödet av personuppgifter inom unionen.[1] Reglerna på unionsnivå har alltså ett dubbelt syfte. I unionsrätten skyddas rätten till respekt för privatlivet och rätten till skydd av personuppgifter som grundläggande rättigheter enligt EU:s stadga om de grundläggande rättigheterna, som tillsammans med grundfördragen utgör en del av unionens primärrätt.[2] För att säkerställa att olikheter i medlemsstaternas dataskyddslagstiftning inte blir ett handelshinder på den inre marknaden har unionen fått befogenhet att anta regler om skydd av personuppgifter och det fria flödet av sådana uppgifter.[3]

I januari 2012 inleddes en dataskyddsreform, som under 2016 ledde till att EU antog det s.k. dataskyddspaketet.[4] Paketet utgör en del av EU:s strategi för den digitala inre marknaden och dess främsta syfte var att anpassa de tidigare reglerna till den pågående digitala transformationen, särskilt internet. Reformen syftade emellertid även till att göra dataskyddsreglerna mer enhetliga samt inrätta en mekanism för ökat samarbete mellan tillsynsmyndigheter vid gränsöverskridande behandling av personuppgifter. Med mer enhetliga regler är avsikten att det ska bli enklare för företag att bl.a. tillhandahålla digitala tjänster på den inre marknaden utan att dessa ska behöva anpassas till varje medlemsstat samtidigt som reglerna säkerställer en hög nivå av skydd för användare av dessa tjänster.

På samma sätt ska det bli enklare för myndigheter i olika medlemsstater att utbyta personuppgifter när de utför sina uppgifter. En enhetlig ram för dataskydd ska möjliggöra e-tjänster som företag och medborgare kan använda för att bl.a. enkelt ansöka om tillstånd eller lämna en skattedeklaration i en annan medlemsstat.

EU:s allmänna dataskyddsförordning

Europeiska unionens dataskyddsrätt regleras i första hand genom EU:s allmänna dataskyddsförordning (GDPR)[5], som antogs den 27 april 2016 och numera har ersatt EU:s dataskyddsdirektiv från 1995[6]. Förordningen blev direkt tillämplig i Sverige och alla andra medlemsstater den 25 maj 2018.[7] Det innebär att dataskyddsförordningen automatiskt blir gällande eftersom den i motsats till ett EU-direktiv inte behöver införlivas i nationell rätt. Samtidigt ger förordningen medlemsstaterna vissa möjligheter att införa nationella undantag, men också nationella kompletterande bestämmelser som krävs för att denna i praktiken ska fungera på nationell nivå.

I Sverige har sådana bestämmelser bl.a. införts genom lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen), som trädde i kraft samtidigt som förordningen blev tillämplig.[8] Lagen kompletteras i sin tur med tillämpningsföreskrifter som finns i den svenska förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning.[9] Det finns också en omfattande speciallagstiftning om hur personuppgifter får behandlas inom olika områden, såsom hälso- och sjukvården. I det följande behandlas viss sådan speciallagstiftning.

Polisiär och annan brottsbekämpande verksamhet

EU:s dataskyddsförordning gäller inte när behöriga myndigheter behandlar personuppgifter i samband med polisiär och annan brottsbekämpande verksamhet.[10] Sådan behandling regleras i stället av ett särskilt EU-direktiv som antogs 2016 i samband med EU:s dataskyddsreform.[11] Direktivet, som senast ska vara införlivat i medlemsstaternas nationella rätt den 6 maj 2018, ersätter och upphäver EU:s dataskyddsrambeslut från 2008 om polisiärt och straffrättsligt samarbete.[12] Direktivet har i första hand införlivats i svensk rätt genom brottsdatalagen, som trädde i kraft den 1 augusti 2018.[13]

Elektronisk kommunikation

EU:s dataskyddsförordning gäller även inom sektorn för elektronisk kommunikation, men för organisationer som är verksamma inom detta område gäller även viss speciallagstiftning om behandling av personuppgifter och integritetsskydd vid elektronisk kommunikation. Sådana bestämmelser finns i första hand i EU:s direktiv om integritet och elektronisk kommunikation (det s.k. e-integritets-direktivet) från 2002 och som har ändrats 2009.[14] Direktivet har i första hand införlivats i svensk rätt genom vissa bestämmelser i lagen om elektronisk kommunikation (LEK)[15] och marknadsföringslagen (MFL)[16].

Direktivet gäller vid behandling av personuppgifter vid tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät, exempelvis sådana kommunikationstjänster som tillhandahålls av tele- och bredbandsoperatörer.[17] Dess bestämmelser preciserar och kompletterar EU:s dataskyddsförordning. Direktivet ställer bl.a. krav på säkerhetsåtgärder och konfidentialitet vid kommunikation samt att abonnenter informeras om behandling av trafikuppgifter och risker för brott mot nätsäkerheten.[18]

Det innebär att kommunikation och relaterade trafikuppgifter inte utan samtycke får fångas upp eller lagras av andra personer än användarna.[19] Medlemsstaterna får dock införa undantag från detta förbud, om det är nödvändigt för att skydda den nationella säkerheten, bekämpa brott och vissa andra liknande samhällsintressen.[20] Trafikuppgifter om abonnenter och användare ska dock normalt raderas eller anonymiseras så snart de inte längre behövs för att överföra kommunikation.[21] Det är alltså som huvudregel inte tillåtet att lagra sådana uppgifter för andra ändamål än fakturering av abonnemangsavgifter.[22] För marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av mervärdestjänster krävs abonnentens eller användarens samtycke.[23]

Behandlingen ska dessutom begränsas till sådana personer som getts i uppdrag att sköta fakturering, trafikstyrning, kundförfrågningar, spårning av bedrägerier, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av en mervärdestjänst. Den får heller inte omfatta mer än sådant som är nödvändigt för att utföra dessa uppgifter.[24]

Direktivet innehåller också bestämmelser om s.k. webbkakor (”cookies”) som innebär att användaren ska ha informerats om och samtyckt till att sådana uppgifter lagras eller görs tillgängliga.[25] Det finns dock vissa undantag från kravet på användarens samtycke, bl.a. när kakor används för att lagra användarens inloggning eller språkinställningar under en pågående session. Det finns även ett förbud mot s.k. skräppost och annan icke begärd kommunikation, som i svensk rätt har införlivats i marknadsföringslagen.[26]

Svensk tillsynsmyndighet för verksamhet som faller under lagen om elektronisk kommunikation är Post- och telestyrelsen (PTS). För mer information se myndighetens webbplats:

pts.se

EU-kommissionen har som en del av unionens dataskyddsreform i januari 2017 lagt fram ett förslag till en ny förordning om integritet och elektronisk kommunikation (den s.k. ”ePrivacy-förordningen”) samt om upphävande av 2002 års direktiv.[27] Ett av syftena med förslaget är att samordna de sektorspecifika reglerna med 2016 års allmänna dataskyddsförordning. Den nya förordningen skulle ha blivit tillämplig i maj 2018 samtidigt som dataskyddsförordningen, men förslaget har mött starkt motstånd och det är oklart när nya regler kan komma att antas av EU:s lagstiftare.

Datalagringsdirektivet

I EU:s datalagringsdirektiv från 2006 fanns tidigare bestämmelser som inskränkte e-integritetsdirektivet och tvingade tele- och bredbandsoperatörer att lagra vissa trafikuppgifter.[28] Direktivet har dock ogiltigförklarats av EU-domstolen den 8 april 2014 eftersom detta kränkte rätten till respekt för privatliv och rätten till skydd för personuppgifter enligt EU:s stadga om grundläggande rättigheter.[29] Domstolen har i ett senare avgörande även slagit fast att de svenska bestämmelser i lagen om elektronisk kommunikation som genomför datalagringsdirektivet strider mot unionsrätten.[30] EU-domstolen har dock inte befogenhet att ogiltigförklara nationell rätt, vilket innebär att de svenska bestämmelserna formellt gäller fram tills den svenska riksdagen upphäver dessa. Regeringen tillsatte i januari 2017 en utredning som lämnat förslag på hur de svenska reglerna ska göras förenliga med unionsrätten.[31] Det är oklart när dessa nya regler kan komma att träda i kraft.

Datainspektionen och andra tillsynsmyndigheter

EU:s dataskyddsförordning anger att det ska finnas oberoende nationella tillsynsmyndigheter som ska övervaka dataskyddsreglernas efterlevnad. Datainspektionen är svensk tillsynsmyndighet för företag, myndigheter och andra organisationer som är etablerade i Sverige, men kan även fungera som ansvarig eller berörd tillsynsmyndighet vid gränsöverskridande behandling av personuppgifter. Förordningen innebär även ett förstärkt samarbete mellan nationella tillsynsmyndigheter inom unionen. Mer information finns på inspektionens webbplats:

www.datainspektionen.se

För att övervaka unionens institutioner, organ och byråers efterlevnad finns sedan 2014 dessutom Europeiska datatillsynsmannen, som bedriver tillsyn enligt en särskild EU-förordning om institutionernas, organens och byråernas behandling av personuppgifter. En ny förordning som samordnar reglerna med GDPR antogs den 23 oktober 2018.[32] Mer information finns på tillsynsmannens webbplats:

edps.europa.eu

Europeiska dataskyddsstyrelsen

Genom EU:s dataskyddsförordning inrättades Europeiska dataskyddsstyrelsen, som ersätter den s.k. Artikel 29-gruppen. Dataskyddsstyrelsen består av cheferna för medlemsstaternas tillsynsmyndigheter och den Europeiska datatillsynsmannen. Dess främsta uppgift är att verka för en enhetlig tillämpning av dataskyddsreglerna, vilket bl.a. innefattar att utfärda riktlinjer, rekommendationer och bästa praxis (se bilaga om vilka riktlinjer styrelsen hittills har antagit). Styrelsens riktlinjer är icke bindande, men kan vara vägledande vid tolkning och tillämpning av dataskyddsförordningen.

Förordningen inrättar även en mekanism för enhetlighet som ger styrelsen befogenhet att fatta beslut i en tvist mellan medlemsstaternas tillsynsmyndigheter. Genom förordningen skapas ett system med en ansvarig tillsynsmyndighet och berörda tillsynsmyndigheter, som ska samarbeta i samband med gränsöverskridande behandling av personuppgifter. Om tillsynsmyndigheterna har olika uppfattning kan styrelsen med kvalificerad majoritet fatta ett rättsligt bindande beslut (se avsnittet om gränsöverskridande behandling av personuppgifter angående vilken medlemsstat som ska vara ansvarig tillsynsmyndighet).

Mer information finns på dataskyddsstyrelsens webbplats:

edpb.europa.eu

Noter

[1] Artikel 1 i förordning (EU) 2016/679. Se även artikel 1.1 i fördrag 2002/58/EG, som förutom personuppgifter även talar om fri rörlighet för utrustning och tjänster avseende elektronisk kommunikation.

[2] Artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (EUT C 326, 26.10.2012, s. 391–407).

[3] Artikel 16.2 i Fördraget om Europeiska unionens funktionssätt (konsoliderad version) (EUT C 326, 26.10.2012, s. 47–390).

[4] Dataskyddspaketet består av förordning (EU) 2016/679 och direktiv (EU) 2016/680. Se EU-kommissionens meddelande Skydd av den personliga integriteten i en uppkopplad värld - En europeisk ram för personuppgiftsskydd för tjugohundratalet, COM(2012) 9 slutlig.

[5] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1–88). Den svenska språkversionen har rättats den 23 maj 2018 (EUT L 119, 4.5.2016).

[6] 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 (EGT L 281, 23.11.1995, s. 31–50). Direktivet har upphört genom artikel 94 i förordning (EU) 2016/679, som även innehåller övergångsbestämmelser.

[7] Artikel 99 i förordning (EU) 2016/679.

[8] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

[9] Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

[10] Artikel 2.1 d i förordning (EU) 2016/679.

[11] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89–131). Den svenska språkversionen har rättats den 23 maj 2018 (EUT L 127, 23.5.2018, s. 16–21).

[12] Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.

[13] Brottsdatalag (2018:1177).

[14] 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, s. 37–47). Direktivet har ändrats genom direktiv 2009/136/EG.

[15] Lag (2003:389) om elektronisk kommunikation.

[16] Marknadsföringslag (2008:486).

[17] Artikel 3 i direktiv 2002/58/EG.

[18] Artiklarna 4 och 5 i direktiv 2002/58/EG.

[19] Artiklarna 2, 5 och 6 i direktiv 2002/58/EG.

[20] Artikel 15 i direktiv 2002/58/EG.

[21] Artikel 6.1 i direktiv 2002/58/EG.

[22] Artikel 6.2 i direktiv 2002/58/EG.

[23] Artikel 6.3 i direktiv 2002/58/EG.

[24] Artikel 6.5 i direktiv 2002/58/EG.

[25] Artikel 5.3 i direktiv 2002/58/EG.

[26] Artikel 13 i direktiv 2002/58/EG. 19–21 §§ Marknadsföringslagen (2008:486).

[27] EU-kommissionens förslag till Europaparlamentet och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation), COM(2017) 10 slutlig.

[28] 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 L 105, 13.4.2006, s. 54–63).

[29] EU-domstolens dom av den 8 april 2014 i förenade målen C-293/12 och C-594/12 Digital Rights Ireland (ECLI:EU:C:2014:238).

[30] EU-domstolens dom av den 21 december 2016 i förenade målen C-203/15 och C-698/15 Tele2 Sverige (ECLI:EU:C:2016:970).

[31] Delbetänkande av Utredningen om datalagring och EU-rätten SOU 2017:75 Datalagring – brottsbekämpning och integritet. Se även utredningens slutbetänkande SOU 2018:61 Rättssäkerhetsgarantier och hemliga tvångsmedel.

[32] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39–98).

Dataskyddsförordningens tillämpningsområde

EU:s dataskyddsförordning (GDPR) gäller som huvudregel vid all behandling av personuppgifter. Det innebär att alla organisationer i normalfallet måste följa förordningens regler så snart de behandlar personuppgifter. Vad som räknas som behandling av personuppgifter blir alltså avgörande för att fastställa om dataskyddsreglerna blir tillämpliga.

Vem skyddas av dataskyddsreglerna?

Den vars personuppgifter behandlas kallas för den registrerade och det är hans eller hennes grundläggande fri- och rättigheter som skyddas genom EU:s dataskyddsreglering.[1] Endast nu levande människor (i lagtexten används den juridiska termen fysisk person) omfattas av detta skydd.[2] Att avlidnas personuppgifter inte omfattas av unionsrätten innebär dock inte att det är helt fritt fram att behandla sådana uppgifter i Sverige. Det finns särskild svensk lagstiftning som reglerar uppgifter om avlidna.[3] EU:s dataskyddsförordning omfattar heller inte uppgifter som avser juridiska personer, såsom bolag, föreningar och stiftelser.[4] Exempelvis ett bolags firmanamn och kontaktuppgifter. Däremot skyddas människors personuppgifter inte bara i rent privata sammanhang, utan även i yrkeslivet.[5]

Vad räknas som personuppgifter?

Med personuppgifter avses all information som kan hänföras till en identifierad eller identifierbar människa.[6] Ett första krav är alltså att det ska finnas ett tillräckligt samband mellan uppgifterna och en människa.

Exempel: Uppgifter som beskriver en människas egenskaper såsom hennes namn, ögonfärg, längd och vikt kan vara personuppgifter, men även t.ex. uppgifter om någons elkonsumtion eller surfvanor.

En uppgift som inte alls kan hänföras till någon människa kan däremot inte vara en personuppgift. Det kan dock ibland vara svårt att avgöra om ett sådant samband föreligger.

Exempel: Uppgiften att avståndet mellan jorden och månen är 384 400 km är i sig ingen personuppgift, men om uppgiften lämnats av en elev på ett prov är det inte längre lika självklart att uppgiften inte avser en människa.

Om något är en personuppgift beror alltså normalt på i vilket sammanhang uppgiften förekommer. Det är dock inte tillräckligt att uppgiften avser en människa, hon eller han måste även vara identifierad eller identifierbar. Det är därför dataskyddsreglerna inte är tillämpliga på anonym information (se nedan om anonymisering och pseudonymisering).

En person är identifierad om han eller hon kan särskiljas från alla andra individer i en grupp. Förordningen kräver dock inte att en person faktiska ska ha blivit identifierad, det är tillräckligt att han eller hon potentiellt kan identifieras. Det är heller inget krav att personen ska vara direkt identifierbar, det är tillräckligt att han eller hon indirekt kan identifieras med hjälp av uppgifterna. Det vanliga är att någon blir identifierbar genom uteslutning eller genom att en uppgift kompletteras med andra uppgifter.

Exempel: För att en maskin som ansluts till internet ska kunna identifieras får den ett unikt nummer – ett IP-nummer (även kallat IP-adress). Ett IP-nummer i sig själv är inte en personuppgift eftersom det inte är direkt kopplat till en människa, men kan genom att kombineras med andra uppgifter, t.ex. ett internetabonnemang, användas för att identifiera en människa. Många IP-nummer, oavsett om dessa är statiska eller dynamiska, ska därför räknas som personuppgifter enligt dataskyddsförordningen.[7]

För att avgöra om någon ska räknas som identifierbar i förordningens mening ska man beakta alla hjälpmedel som rimligen kan komma att användas för att identifiera en person. Detta

innefattar samtliga objektiva faktorer, såsom kostnader och tidsåtgång, med hänsyn taget både till befintlig teknik såväl som den tekniska utvecklingen. Det är heller inte nödvändigt att den personuppgiftsansvarige själv förfogar över de uppgifter och andra hjälpmedel som krävs för att identifiera den registrerade. Det räcker att dessa finns att tillgå hos någon tredje part.[8]

Vad menas med pseudonymisering och anonymisering av personuppgifter?

Pseudonymisering

Med pseudonymisering enligt EU:s dataskyddsförordning avses behandling av personuppgifter på ett sådant sätt att uppgifterna inte längre kan hänföras till en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte kan hänföras till en identifierad eller identifierbar människa.[9]

Pseudonymisering är en av flera tekniska skyddsåtgärder som en personuppgiftsansvarig kan behöva vidta enligt förordningen, men det framgår också av förordningen att det inte räcker med pseudonymisering för att uppgifterna ska räknas som avidentifierade.[10] Pseudonymiserade uppgifter räknas fortfarande som personuppgifter och omfattas därför fullt ut av EU:s dataskyddsförordning.

Anonymisering

Eftersom en uppgift, som framgår ovan, måste kunna identifiera en människa omfattas anonym information över huvud taget inte av dataskyddsreglerna.[11] Med anonym information avses information som inte hänför sig till någon identifierad eller identifierbar person eller personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte längre är identifierbar.[12] Det får alltså inte gå att avanonymisera uppgifterna. När man bedömer om det föreligger en sådan risk gäller vad som sägs ovan om när en person ska räknas som identifierbar (se även ovan om pseudonymisering).

Vad menas med känsliga personuppgifter?

Med känsliga personuppgifter avses normalt det som i EU:s dataskyddsförordning benämns ”särskilda kategorier av personuppgifter”.[13] Det är även så begreppet bl.a. används i den svenska dataskyddslagen. Följande kategorier av personuppgifter räknas som särskilt känsliga till sin natur:

- ras eller etniskt ursprung
- politiska åsikter, religiös eller filosofisk övertygelse
- medlemskap i fackförening
- genetiska uppgifter
- biometriska uppgifter
- uppgifter om hälsa
- sexualliv eller sexuell läggning

För behandling av dessa kategorier av uppgifter gäller särskilt strikta krav enligt unionens dataskyddsreglering eftersom de på grund av sin natur anses medföra särskilda risker för den registrerades grundläggande fri- och rättigheter. Exempelvis att denne utsätts för diskriminering. Särskilda krav gäller även för behandling av person- och samordningsnummer samt fällande domar i brottmål och överträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder.[14]

Vad räknas som behandling av personuppgifter?

Med behandling av personuppgifter avses i princip alla åtgärder som vidtas med sådana uppgifter.[15] Förordningen omfattar både automatiserad och manuell behandling, men för att behandling som uteslutande sker på manuell väg ska omfattas krävs att uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av sådana uppgifter som gör dem sökbara på särskilda kriterier (ett register med personuppgifter).[16]

Exempel: Personuppgifter som förekommer i löpande text i en pappershandling eller i en tryckt bok omfattas inte av dataskyddsreglerna. Vid manuell behandling måste uppgifterna ingå i ett sökbart register.

För att behandlingen ska omfattas är det dock tillräckligt att uppgifterna helt eller delvis behandlas i en dator eller överförs i ett nätverk. Det måste heller inte röra sig om en aktiv åtgärd,

det räcker att uppgifterna passivt lagras i ett dataminne.

Exempel: Personuppgifter som lagras på ett USB-minne i en skrivbordslåda räknas som behandling av personuppgifter även om inga andra åtgärder vidtas med den lagrade informationen.

Exempel: Personuppgifter, såsom namn eller telefonnummer, som publiceras på en webbplats på internet utgör behandling av personuppgifter.[17]

Det har varit EU-lagstiftarens avsikt att dataskyddsreglerna ska gälla under hela datalivscykeln, det vill säga från att uppgifterna samlas in till att de raderas.

Missbruksregeln

Tidigare omfattades inte personuppgifter i ostrukturerat material fullt ut av de svenska reglerna om skydd av personuppgifter (den s.k. missbruksregeln).[18] Något motsvarande undantag finns inte i EU:s dataskyddsförordning. Den svenska missbruksregeln upphörde att gälla den 25 maj 2018 i samband med att förordningen blev direkt tillämplig i Sverige. Det finns alltså numera inget krav på att personuppgifter som behandlas digitalt ska lagras i en databas eller någon liknande strukturerad samling. Även personuppgifter i ostrukturerat material, såsom ett ordbehandlingsdokument eller e-postmeddelande, omfattas alltså numera fullt ut av dataskyddsregleringen.

Vad gäller vid privatpersoners behandling av personuppgifter?

EU:s dataskyddsförordning omfattar över huvud taget inte privatpersoners behandling av personuppgifter så länge denna är av rent privat natur.[19]

Exempel: En privatpersons inlägg på sociala media, såsom Facebook, Twitter eller Instagram, omfattas inte av EU:s dataskyddsförordning. Däremot omfattas ett inlägg som en person gör i sin närings- eller yrkesverksamhet.

Vad gäller vid myndighets behandling i brottsbekämpande verksamhet?

EU:s dataskyddsförordning gäller inte vid behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, vilket innefattar att förebygga och förhindra hot mot den allmänna säkerheten.[20] För sådan behandling gäller i stället ett särskilt EU-direktiv från 2016 om behandling av personuppgifter i behöriga myndigheters brottsbekämpande verksamhet[21], som bl.a. har införlivats i svensk rätt genom brottsdatalagen.[22] Det rör sig bl.a. om sådan behandling som sker hos polis- och åklagarmyndigheten för att förebygga och utreda brott.

Vilken annan behandling omfattas inte av EU:s dataskyddsförordning?

EU:s dataskyddsförordning gäller inte behandling som sker i verksamhet som inte omfattas av unionsrätten, såsom medlemsstaternas nationella säkerhet.[23] Detsamma gäller medlemsstaternas behandling av personuppgifter inom ramen för den gemensamma utrikes- och säkerhetspolitiken.[24] Dataskyddslagen utsträcker dock – med vissa undantag – dataskyddsförordningens tillämpningsområde även till dessa verksamhetsområden.[25] I Sverige ska alltså förordningens bestämmelser även gälla vid behandling som inte omfattas av unionsrätten och när svenska myndigheter behandlar personuppgifter inom ramen för den gemensamma utrikes- och säkerhetspolitiken.

Noter

[1] Artikel 4.1 i förordning (EU) 2016/679 definierar vad som avses med ”en registrerad”.

[2] Skäl 27 i förordning (EU) 2016/679. Medlemsstaterna får i sin nationella rätt utsträcka skyddet även till avlidna personer.

[3] I 5 kap. 4 § brottsbalken straffbeläggs förtal av avliden och enligt rättspraxis har sekretess enligt offentlighets- och sekretesslagen (2009:400) även ansetts kunna gälla till förmån för avliden.

[4] Skäl 14 i förordning (EU) 2016/679.

[5] EU-domstolens dom av den 9 november 2010 i de förenade målen C-92/09 och C-93/09 *Volker und Markus Schecke och Eifert*, punkten 59.

[6] Artikel 4.1 i förordning (EU) 2016/679 innehåller en definition av vad som avses med ”personuppgifter”.

[7] EU-domstolens dom av den 19 oktober 2016 i mål C-582/14 *Breyer* (ECLI:EU:C:2016:779).

[8] Skäl 26 i förordning (EU) 2016/679.

[9] Artikel 4.5 i förordning (EU) 2016/679.

[10] Skäl 26 i förordning (EU) 2016/679.

[11] Skäl 26 i förordning (EU) 2016/679.

[12] Skäl 26 i förordning (EU) 2016/679.

[13] Artikel 9 i förordning (EU) 2016/679.

[14] 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Artikel 10 i förordning (EU) 2016/679.

[15] Artikel 4.2 i förordning (EU) 2016/679 innehåller en definition av vad som avses med ”behandling” av personuppgifter.

[16] Artikel 2.1 i förordning (EU) 2016/679. I artikel 4.6 anges att med ett ”register” avses ”en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden”. Se även EU-domstolens dom av den 10 juli 2018 i mål C-25/17 *Jehovan todistajat* (ECLI:EU:C:2018:551).

[17] EU-domstolens dom av den 6 november 2003 i mål C-101/01 *Lindqvist* (ECLI:EU:C:2003:596).

[18] Personuppgifter i ostrukturerat material omfattades på grund av en svensk nationell särregel i 5 a § personuppgiftslagen (den s.k. missbruksregeln) tidigare inte fullt av dessa regler. Denna undantagsregel har upphört att gälla den 25 maj 2018 genom lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

[19] Artikel 2.2 c i förordning (EU) 2016/679.

[20] Artikel 2.2 d i förordning (EU) 2016/679.

[21] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89–131).

[22] Brottsdatalagen (2018:1177), som trädde i kraft den 1 augusti 2018.

[23] Artikel 2.2 a i förordning (EU) 2016/679.

[24] Artikel 2.2 b i förordning (EU) 2016/679.

[25] 1 kap. 2 och 3 §§ lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Ansvar för personuppgifter

Det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för behandling av personuppgifter. Den personuppgiftsansvarige är bl.a. skyldig att vidta tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd av personuppgifter. Den personuppgiftsansvarige är också skyldig att visa att denne uppfyller alla de grundläggande krav på behandling av personuppgifter som ställs upp i förordningen. Även den som endast utför behandling av personuppgifter för någon annans räkning (personuppgiftsbiträde) har vissa egna skyldigheter enligt dataskyddsförordningen. Den som överträder förordningen kan drabbas av stränga sanktioner.

Vad menas med principen om ansvarsskyldighet?

Principen om ansvarsskyldighet (”accountability”) innebär att det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för att all behandling av personuppgifter som utförs under dennes överinseende eller för dennes räkning uppfyller alla de grundläggande krav (principer om dataskydd) som ställs upp i dataskyddsförordningen.[1] Den personuppgiftsansvarige är bl.a. skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd av personuppgifter.

I ansvarsskyldigheten ligger även ett krav på att den personuppgiftsansvarige ska kunna bevisa att denne lever upp till ovanstående krav. Principen innebär en omvänd bevisbörda.[2] Det räcker alltså inte att den personuppgiftsansvarige i och för sig gjort korrekta bedömningar och faktiskt vidtagit tekniska och organisatoriska åtgärder. I praktiken måste bedömningar och åtgärder även dokumenteras på ett sådant sätt att det i efterhand går att visa att den personuppgiftsansvarige uppfyller förordningens krav. Brister i dokumentationen kan göra att den personuppgiftsansvarige inte förmår uppfylla sin bevisbörda, vilket kan innebära att denne drabbas av sanktioner. En organisation behöver därför ett ledningssystem för dataskydd. Även anslutning till godkända uppförandekoder och certifieringar för dataskydd kan användas som bevismedel.[3]

Vem är personuppgiftsansvarig?

Personuppgiftsansvarig är den organisation som bestämmer ändamålen och medlen för behandling av personuppgifter.[4] Det är denna organisation som har det huvudsakliga ansvaret för behandling av personuppgifter som utförs under dennas överinseende eller för dennas räkning. Det avgörande är vem som beslutar om förutsättningarna för behandlingen, inte vem som rent faktiskt utför denna (se nedan om personuppgiftsbiträde).

Även organisationens storlek, såsom antalet anställda eller dess omsättning, saknar i princip betydelse för frågan om ett företag är skyldigt att följa EU:s dataskyddsförordning. Det finns dock vissa lättnader för små- och medelstora företag, såsom undantag från skyldigheten att föra register över behandlingen.[5]

Den personuppgiftsansvarige är normalt ett företag, en myndighet eller någon annan organisation. Den personuppgiftsansvarige måste dock inte vara en juridisk person, även en fysisk person kan räknas som personuppgiftsansvarig. Exempelvis en person som driver näringsverksamhet i form av en enskild firma eller ett enkelt bolag. Den som är anställd räknas dock inte som personuppgiftsansvarig (se nedan om ansvar för anställdas behandling av personuppgifter).

Vem räknas som personuppgiftsbiträde?

Ett företag, en myndighet eller annan organisation som endast behandlar personuppgifter för någon annans räkning, utan att själv bestämma ändamålen eller medlen för behandlingen är ett personuppgiftsbiträde.[6] Även ett personuppgiftsbiträde har vissa egna skyldigheter enligt EU:s dataskyddsförordning. För att räknas som biträde ska det röra sig om ett separat organ, inte endast en avdelning inom den personuppgiftsansvariges organisation. Det är också värt att lägga märke till att ett biträde i sin tur kan anlita ett s.k. underbiträde. När ett biträde eller underbiträde anlitas ställs särskilda krav på vilka tekniska och organisatoriska åtgärder som ska vidtas, bl.a. tecknande av personuppgiftsbiträdesavtal.[7]

Det avgörande för om någon ska räknas som ett biträde är graden av självständighet. Ett biträde behandlar osjälvständigt personuppgifter för den personuppgiftsansvariges räkning. Om ett biträde bestämmer ändamålen eller medlen för behandlingen tillsammans med uppdragsgivaren räknas de i stället som gemensamt personuppgiftsansvariga (se nedan om vad som gäller vid gemensamt ansvar), medan en leverantör som helt på egen hand bestämmer ändamålen och medlen för behandlingen räknas som en fristående personuppgiftsansvarig. Alla leverantörer räknas alltså inte som personuppgiftsbiträden.

Vad gäller vid gemensamt personuppgiftsansvar?

Om två eller flera personuppgiftsansvariga gemensamt fastställer ändamålen och medlen för behandlingen ska de räknas som gemensamt personuppgiftsansvariga.[8] Dessa ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning genom ett inbördes arrangemang. Arrangemanget ska på lämpligt sätt återspegla de gemensamt ansvarigas respektive roller och förhållanden gentemot registrerade. Det inbördes arrangemanget påverkar inte den registrerades möjligheter att göra sina rättigheter enligt förordningen gällande mot någon av de personuppgiftsansvariga.

Exempel: En organisation som lagt upp och driver en sida (”fanpage”) på det sociala nätverket Facebook har tillsammans med Facebook ansetts gemensamt personuppgiftsansvarig för behandling av besökarnas personuppgifter även om den förra för egen del endast tog emot besöksstatistik i anonymiserad form. Däremot ska någon som enbart använder ett socialt nätverk, t.ex. gillar eller kommenterar ett inlägg, inte anses vara medansvarig för nätverkets behandling av personuppgifter.[9]

Vem ansvarar för anställdas behandling av personuppgifter?

Den personuppgiftsansvarige eller ett personuppgiftsbiträde ansvarar för alla som behandlar personuppgifter under dennes överinseende. Det är alltså normalt arbetsgivaren som ansvarar för sina anställdas behandling av personuppgifter. Den som är anställd får endast utföra behandling av personuppgifter som denne får tillgång till i tjänsten enligt arbetsgivarens instruktioner.[10] Det är arbetsgivarens ansvar att se till att det finns lämpliga tekniska och organisatoriska skyddsåtgärder som hindrar att anställda får obehörig tillgång till personuppgifter.[11]

Vad händer vid en överträdelse av dataskyddsförordningen?

Sanktionsavgifter

Den som överträder dataskyddsförordningens bestämmelser kan drabbas av stränga sanktioner. Om ett företag överträder förordningen kan tillsynsmyndigheten besluta om en sanktionsavgift som uppgår till 20 miljoner euro eller 4 % av företagets totala globala årsomsättning. För vissa till sin art mindre allvarliga överträdelser är den högsta sanktionsavgiften i stället 10 miljoner euro eller 2 % av företagets totala globala årsomsättning.[12]

Förordningen ger en medlemsstat möjlighet att själv bestämma i vilken utsträckning dessa sanktionsavgifter även ska gälla för myndigheter eller andra offentliga organ. Sverige har valt att begränsa avgiften för svenska myndigheter till som högst 10 miljoner kronor eller 5 miljoner kronor i mindre allvarliga fall.[13]

En sanktionsavgift tillfaller staten och ska betalas till Kammarkollegiet inom 30 dagar.[14]

Förbudsföreläggande m.m.

Förutom administrativa sanktionsavgifter har tillsynsmyndigheten även möjlighet att använda åtgärder vid överträdelse av dataskyddsregleringen såsom att utfärda en varning eller reprimand eller att förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta vissa åtgärder.[15] Tillsynsmyndigheten får även genom föreläggande utfärda ett förbud mot eller begränsning av behandling av personuppgifter. Om en personuppgiftsansvarige eller ett personuppgiftsbiträde inte rättar sig efter tillsynsmyndighetens föreläggande kan denna påföra en administrativ sanktionsavgift (se ovan om sanktionsavgifter).[16] Dataskyddsförordningen tillåter även att medlemsstaterna inför andra sanktioner. Den svenska lagstiftaren har dock avstått från att behålla de straffrättsliga sanktioner (böter och fängelse) som fanns enligt den numera upphävda personuppgiftslagen.

Skadeståndsansvar

Den registrerade har även rätt till skadestånd enligt dataskyddsförordningen. Den personuppgiftsansvarige ska ersätta både ekonomisk och icke-ekonomisk skada som uppkommit på grund av överträdelsen.[17] Om personuppgifter som läckt ut i strid med dataskyddsförordningen används för att begå kontokortsbedrägerier kan den personuppgiftsansvarige exempelvis bli skyldig att ersätta den registrerades förlust i pengar. Med icke-ekonomisk skada avses ersättning för den kränkning som intrånget har inneburit.

Exempel: I svensk rättspraxis har domstolarna normalt dömt ut ett belopp mellan 3 000 – 5 000 kronor i kränkningsersättning vid överträdelse av den numera upphävda personuppgiftslagen.

Även ett personuppgiftsbiträde kan bli skadeståndsskyldig, men det förutsätter att biträdet inte har fullgjort någon av sina egna skyldigheter eller behandlat uppgifterna i strid med den personuppgiftsansvariges anvisningar. Om mer än en personuppgiftsansvarig har orsakat skadan ansvarar de solidariskt för hela skadan. Detsamma gäller om skadan orsakats av ett personuppgiftsbiträde som medverkat vid behandlingen.

Den personuppgiftsansvarige eller ett personuppgiftsbiträde kan endast undgå ansvar genom att bevisa att denne inte på något sätt är ansvarig för den händelse som orsakade skadan. Regeln innebär att bevisbördan placeras på den personuppgiftsansvarige eller personuppgiftsbiträdet som ska visa att det inte finns något orsakssamband mellan den rättsstridiga behandlingen och den uppkomna skadan.

Noter

[1] Artikel 5.2 i förordning (EU) 2016/679.

[2] Artikel 5.2 i förordning (EU) 2016/679.

[3] Artiklarna 24.3, 25.3 och 32.3 förordning (EU) 2016/679.

[4] Artikel 4.7 i förordning (EU) 2016/679 innehåller en definition av vad som avses med ”personuppgiftsansvarig”.

[5] Artikel 30.5 i förordning (EU) 2016/679. Se även skäl 13 som uppmanar medlemsstaterna och deras tillsynsmyndigheter att vid tillämpningen av förordningen ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda behov.

[6] Artikel 4.8 i förordning (EU) 2016/679 innehåller en definition av vad som avses med ”personuppgiftsbiträde”.

[7] Artikel 28 i förordning (EU) 2016/679.

[8] Artikel 26 i förordning (EU) 2016/679.

[9] EU-domstolens dom av den av den 5 juni 2018 i mål C-210/16 *Wirtschaftsakademie Schleswig-Holstein* (ECLI:EU:C:2018:388).

[10] Artikel 29 i förordning (EU) 2016/679.

[11] Artikel 32.4 i förordning (EU) 2016/679.

[12] Artikel 83 i förordning (EU) 2016/679.

[13] 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

[14] 6 kap. 5–6 §§ lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning samt 9 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

[15] Artikel 58.2 i förordning (EU) 2016/679 innehåller en uppräkning av tillsynsmyndighetens korrigerande befogenheter.

[16] Artikel 83 i förordning (EU) 2016/679.

[17] Artikel 82 i förordning (EU) 2016/679.

Krav vid behandling av personuppgifter

All behandling av personuppgifter ska uppfylla vissa grundläggande krav (principer för dataskydd) som ställs upp i EU:s dataskyddsförordning. Särskilt strikta krav gäller för känsliga personuppgifter, såsom uppgifter om hälsa, samt vid behandling av barns personuppgifter. Den registrerade har dessutom ett antal rättigheter mot den personuppgiftsansvarige. Dessa rättigheter ska bl.a. ge den registrerade ökad insyn i och kontroll över behandlingen av hans eller hennes personuppgifter.

Vilka grundläggande krav ställs på behandling av personuppgifter?

All behandling av personuppgifter ska uppfylla ett antal grundläggande krav (principer för dataskydd).[1] Dessa principer har preciserats i dataskyddsförordningen, men överensstämmer i huvudsak med vad som redan gäller enligt dataskyddsdirektivet och personuppgiftslagen.

Laglighet, korrekthet och öppenhet: Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

Ändamålsbegränsning: Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Uppgiftsminimering: Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Riktighet: Personuppgifter ska vara riktiga och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Lagringsminimering: Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Integritet och konfidentialitet: Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

För vissa områden, bl.a. arkiv, vetenskaplig forskning och statistik görs vissa undantag från dessa principer.[2]

Vilken information måste den personuppgiftsansvarige lämna till registrerade?

Behandling av personuppgifter ska ske på ett öppet sätt i förhållande till den registrerade. Den personuppgiftsansvarige är därför skyldig att lämna viss obligatorisk information när personuppgifter samlas in från den registrerade, men även när uppgifter om honom eller henne tas emot från en annan källa.[3] Informationen ska lämnas på den personuppgiftsansvariges eget initiativ samt vara klar och tydlig.[4] En viss grundläggande information måste dessutom lämnas i samband med att samtycke inhämtas för att detta över huvud taget ska vara giltigt.

När krävs samtycke för behandling av personuppgifter?

Den registrerades samtycke krävs alltid vid behandling av hans eller hennes personuppgifter, om den personuppgiftsansvarige inte kan stödja sig på en annan rättslig grund.[5] Om samtycke saknas kan behandlingen i stället bl.a. grundas på den s.k. intresseavvägningsregeln. Regeln innebär att det kan vara tillåtet att behandla någons personuppgifter om det är nödvändigt för att uppnå ett ändamål som rör den personuppgiftsansvarige eller tredje parts berättigade intressen. Detta förutsätter dock att skyddet av den registrerades intressen eller grundläggande fri- och rättigheter inte väger tyngre.[6]

En nyhet i dataskyddsförordningen är att myndigheter inte kan stödja sig på denna intresseavvägningsregel när de fullgör sina uppgifter.[7] Förordningen förutsätter i stället att grunden för myndigheters behandling av personuppgifter regleras i nationell lagstiftning. En myndighet har normalt rätt att behandla personuppgifter när det är nödvändigt för att fullgöra en uppgift av allmänt intresse eller vid myndighetsutövning.[8] För att utföra behandling som är nödvändig för att fullgöra sådana uppgifter krävs alltså normalt inget samtycke från den registrerade. Det är heller inte säkert att ett sådant samtycke hade varit giltigt eftersom det är tveksamt om det uppfyller det nya striktare kravet på frivillighet (se nedan om vad som krävs för giltigt samtycke).

Det finns även andra rättsliga grunder för behandling av personuppgifter i förordningen och i nationell lagstiftning. För känsliga personuppgifter (t.ex. uppgifter om hälsa) gäller andra striktare krav för att behandlingen ska vara laglig. Huvudregeln är att sådan behandling är förbjuden om inte den personuppgiftsansvarige kan stödja sig på något av de undantag som räknas upp i förordningen.

Vad räknas som giltigt samtycke till behandling av personuppgifter?

Ett samtycke ska vara frivilligt, specifikt, informerat och otvetydigt.[9] Det är den personuppgiftsansvarige som ska bevisa att alla dessa krav är uppfyllda.[10] Att ett samtycke är specifikt innebär bl.a. att det inte går att lämna ett generellt samtycke. För att samtycket ska räknas som informerat måste den personuppgiftsansvarige även ha lämnat viss grundläggande information, bl.a. om behandlingens ändamål. Arbetsgivare och myndigheter kan dessutom normalt ha svårt att visa att ett samtycke är frivilligt eftersom detta kräver att den registrerade hade en äkta valmöjlighet. För samtycke till behandling av känsliga personuppgifter krävs dessutom att samtycket är uttryckligt.[11]

När kan ett barn själv samtycka till behandling av sina personuppgifter?

I svensk rätt gäller som huvudregel att den som är omyndig (under 18 år) inte kan åta sig förpliktelser utan vårdnadshavares samtycke.[12] I EU:s dataskyddsförordningen finns en särskild bestämmelse om barns samtycke till behandling av sina egna personuppgifter.[13] Huvudregeln är att sådan behandling kräver samtycke eller godkännande från den person som har föräldraansvar för barnet. Bestämmelsen gäller endast vid erbjudande av informationssamhällets tjänster direkt till ett barn. Med informationssamhällets tjänster avses ungefär tjänster på internet såsom sociala media och sökmotorer. Det är alltså oklart vad unionsrätten kräver när samtycket inte avser en sådan tjänst. Vem som räknas som barn ska dessutom fastställas i nationell rätt. I svensk rätt föreskrivs att den som bor i Sverige och är under 13 år ska räknas som barn i det ovan nämnda sammanhanget.[14]

Exempel: Ida som har fyllt 13 år kan själv samtycka till behandling av sina personuppgifter när hon skapar ett konto på det sociala nätverket Snapchat.

Vad som gäller för barns samtycke till behandling av personuppgifter i andra situationer framgår inte av svensk lag.

Vilka rättigheter har den registrerade?

Dataskyddsförordningen innebär en viss förstärkning av de rättigheter som den registrerade redan hade enligt dataskyddsdirektivet och personuppgiftslagen. Syftet med dessa rättigheter är att ge den registrerade ökad insyn i och kontroll över behandlingen av hans eller hennes personuppgifter. Förordningen ger därför den registrerade nedanstående rättigheter mot den personuppgiftsansvarige. Det är viktigt att den personuppgiftsansvarige vidtar tekniska och organisatoriska åtgärder för att inom de tidsramar som föreskrivs i förordningen kunna hantera en begäran från den registrerade beträffande hans eller hennes rättigheter.

Rätt till information

Behandling av personuppgifter ska vara transparent. Den personuppgiftsansvarige är därför skyldig att lämna viss obligatorisk information när personuppgifter samlas in från den registrerade, men även när uppgifterna erhålls från en annan källa (se ovan om vilken information som måste lämnas till den registrerade).[15]

Rätt till tillgång

Den registrerade har på begäran rätt att få en bekräftelse på om personuppgifter som rör honom eller henne behandlas och i så fall även rätt att få viss obligatorisk information om behandlingen.[16] Dessutom har den registrerade rätt att utan kostnad få en kopia av sina personuppgifter. Syftet med bestämmelsen är att den registrerade ska få ökad insyn i behandlingen av sina personuppgifter, vilket är en förutsättning för att kunna utöva andra rättigheter. Avsikten är inte att den ska vara ett alternativ till rätten att få tillgång till allmänna handlingar. Det som ska lämnas ut är den registrerades personuppgifter och inget annat.

Rätt till rättelse och radering

Den registrerade har rätt att få felaktiga personuppgifter rättade samt få ofullständiga personuppgifter kompletterade.[17] Den registrerade har även rätt att få sina personuppgifter raderade ("rätten att bli bortglömd") förutsatt att vissa villkor är uppfyllda.[18] Det är alltså inte fritt fram att få sina uppgifter raderade, men den personuppgiftsansvarige får räkna med att uppgifter på den registrerades begäran kan behöva tas bort. Vid rättelse och radering måste även mottagare av uppgifterna underrättas.[19]

Rätt till begränsning av behandling

Den registrerade har rätt att kräva att behandlingen begränsas om vissa villkor är uppfyllda.[20] Sådana uppgifter ska markeras och åtgärden innebär att dessa endast får behandlas med samtycke eller för vissa särskilda ändamål. Begränsning av behandling används normalt provisoriskt som ett mindre ingripande alternativ till rättelse eller radering. Även vid begränsning av behandling måste mottagare av uppgifterna underrättas.[21]

Rätt till dataportabilitet

Den registrerade har rätt att få sina personuppgifter överförda till en annan personuppgiftsansvarig i ett strukturerat, allmänt använt och maskinläsbart format.[22] Rätten omfattar endast uppgifter som den registrerade har tillhandahållit och förutsätter att behandlingen grundar sig på samtycke eller avtal samt sker på automatisk väg. Rätt till portabilitet gäller heller inte myndighets verksamhet. Syftet är att ge den registrerade ökad kontroll över sina personuppgifter, men också främja konkurrens mellan leverantörer av digitala tjänster. Det ska inte gå att låsa in användarens personuppgifter.

Rätt att invända mot behandling

Den registrerade kan alltid motsätta sig att hans eller hennes personuppgifter används för direkt marknadsföring. Den registrerade kan även motsätta sig annan behandling som sker med stöd av intresseavvägningsregeln eller för att utföra en uppgift av allmänt intresse eller vid myndighetsutövning.[23] När det gäller annan behandling än direkt marknadsföring kan fortsatt behandling dock bl.a. vara tillåten om den personuppgiftsansvarige kan visa att denne har ett tvingande berättigat intresse som väger tyngre än den registrerades intressen.

Exempel: En skola kan normalt bevara en elevs slutbetyg även om denne motsätter sig detta eftersom det finns motstående berättigade intressen. Efter att eleven slutat på skolan saknas dock normalt skäl att bevara ett flertal andra uppgifter om eleven, t.ex. dennes skåpnummer. Det räcker inte att uppgifterna kan vara bra att ha, om den registrerade motsätter sig behandlingen krävs tungt vägande skäl för att den ska få fortsätta.

Profilering och annat automatiserat beslutsfattande

Den registrerade har rätt att slippa att bli föremål för ett beslut som uteslutande grundar sig på automatiserad behandling.[24] Detta innefattar att bli föremål för profilering. En förutsättning för att behandlingen ska vara förbjuden är att denna har rättsliga följder för den registrerade eller på liknande sätt i betydande grad påverkar honom eller henne. Förbudet omgärdas dessutom av ett flertal undantag. Det är t.ex. tillåtet att använda profilering och annat automatiserat beslutsfattande med den registrerades uttryckliga samtycke. Det är också möjligt att tillåta sådan behandling i särskild lagstiftning. Det har blivit allt vanligare att s.k. artificiell intelligens (algoritmiskt beslutsfattande) används vid myndighetsutövning. Profilering används bl.a. för att utreda skatteflykt och skatteundandragande.[25] Det är oklart i vilken utsträckning sådana metoder överensstämmer med EU:s dataskyddsförordning.

Noter

[1] Artikel 5 i förordning (EU) 2016/679.

[2] Undantagen framgår dels direkt av bestämmelser i förordning (EU) 2016/679, dels av bestämmelser i svensk nationell rätt. Förordningen föreskriver att särskilda undantag får göras för behandling som avser arkivändamål av allmänt intresse, vetenskapliga och historiska forskningsändamål eller statistiska ändamål. Dessa områden är inte helt undantagna från förordningens tillämpningsområde, men det är bl.a. möjligt att lagra personuppgifter under längre tid än vad som annars hade varit tillåtet.

[3] Artiklarna 13 och 14 i förordning (EU) 2016/679.

[4] Artikel 12 i förordning (EU) 2016/679.

[5] Artikel 6 i förordning (EU) 2016/679.

[6] Artikel 6.1 f i förordning (EU) 2016/679.

[7] Artikel 6.1 andra stycket i förordning (EU) 2016/679.

[8] Artikel 6.1 e i förordning (EU) 2016/679.

[9] Artikel 4.11 i förordning (EU) 2016/679 innehåller en definition av ”samtycke av den registrerade”.

[10] Artikel 7 i förordning (EU) 2016/679.

[11] Artikel 9.2 a i förordning (EU) 2016/679.

[12] 9 kap. 1 § föräldrabalken. Det finns dock vissa undantag som föreskrivs i lag. Det finns bl.a. undantag för den som fyllt 16 år.

[13] Artikel 8 i förordning (EU) 2016/679.

[14] 2 kap. 4 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

[15] Artiklarna 13 och 14 i förordning (EU) 2016/679.

[16] Artikel 15 i förordning (EU) 2016/679.

[17] Artikel 16 i förordning (EU) 2016/679.

[18] Artikel 17 i förordning (EU) 2016/679.

[19] Artikel 19 i förordning (EU) 2016/679.

[20] Artikel 18 i förordning (EU) 2016/679.

[21] Artikel 19 i förordning (EU) 2016/679.

[22] Artikel 20 i förordning (EU) 2016/679.

[23] Artikel 21 i förordning (EU) 2016/679.

[24] Artikel 22 i förordning (EU) 2016/679.

[25] Papis-Alamansa, Marta, *A ’STIR’ing example of the use of new technologies in ensuring VAT compliance in Poland: what are the legal challenges?,* (kommande) i EC Tax Law.

Tekniska och organisatoriska åtgärder

EU:s dataskyddsförordning reglerar i första hand hur organisationer hanterar personuppgifter, särskilt hur organisationen hanterar de risker som är förknippade med dess behandling av personuppgifter. För att efterleva dataskyddsförordningen måste den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder. Hur långtgående åtgärder som måste vidtas beror i första hand på vilka risker som uppkommer i samband med dennes behandling av personuppgifter. För styrning och kontroll av efterlevnad behöver större organisationer normalt även införa strategier och ledningssystem för dataskydd. Dessa åtgärder, strategier och system för dataskydd måste dessutom ständigt utvärderas och vid behov revideras.

När måste den personuppgiftsansvarige utse ett dataskyddsombud?

En myndighet måste alltid utse ett dataskyddsombud.[1] Flera myndigheter kan dela på ett och samma ombud under förutsättning att ombudet ändå kan utföra sina uppgifter. Andra organisationer ska utse ett ombud om dess kärnverksamhet antingen består av regelbunden och systematisk övervakning i stor omfattning eller behandling av känsliga personuppgifter i stor omfattning.[2] Dataskyddsombudets kontaktuppgifter ska offentliggöras (t.ex. på organisationens webbplats) samt meddelas till behörig tillsynsmyndighet.

Ett ombud ska ha tillräcklig kompetens samt ha en oberoende ställning. Ombudet fungerar som tillsynsmyndighetens förlängda arm och ska bl.a. granska att den personuppgiftsansvarige efterlever reglerna om dataskydd. Ombudet ska också ge råd och information samt vara en kontaktperson för registrerade.[3]

Artikel 29-gruppen har utfärdat riktlinjer om dataskyddsombud (WP 243).[4]

Tekniska och organisatoriska åtgärder

För att efterleva dataskyddsförordningen måste den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder.[5] Vissa av dessa åtgärder anges direkt i förordningen, men uppräkningen är inte uttömmande. Den personuppgiftsansvarige måste även vidta alla andra lämpliga åtgärder som med hänsyn till omständigheterna behövs för att skydda den registrerades personuppgifter. Hur långt denna skyldighet sträcker sig beror i första hand på vilka risker som uppkommer för den registrerades fri- och rättigheter. Om det uppkommer en hög risk krävs mer långtgående åtgärder än vid en låg risk. Dataskyddsförordningen bygger alltså på en riskbaserad modell.

Inbyggt dataskydd och dataskydd som standard

Dataskyddsförordningen kräver att vissa skyddsåtgärder integreras i de system som används för behandling av personuppgifter (”inbyggt dataskydd”).[6] Ett exempel på sådana skyddsåtgärder som nämns i förordningen är pseudonymisering. Förordningen ställer också krav på åtgärder som innebär att behandling i standardfallet endast sker i den omfattning som är nödvändigt för varje ändamål med behandlingen (”dataskydd som standard”).[7] Dessa bestämmelser har sin grund i ”privacy by design”, en designprincip som innebär att integritetskrav ska beaktas redan under utvecklingen av ett IT-system.[8] Det är dock fortfarande oklart vad som närmare avses med kravet på ”inbyggt dataskydd” och ”dataskydd som standard” i dataskyddsförordningens mening. Kravets närmare

innebörd behöver klargöras och preciseras genom riktlinjer, tekniska standarder eller godkända uppförandekoder.

Register över behandling av personuppgifter

Dataskyddsförordningen kräver att den personuppgiftsansvarige för ett register över behandling av personuppgifter som utförs under dennes ansvar.[9] Vad som ska antecknas i ett sådant register specificeras i förordningen. Det ska bl.a. innehålla en beskrivning av kategorier av registrerade och kategorier av personuppgifter. Det rör sig däremot inte om en löpande förteckning över varje enskild behandlingsåtgärd eller varje enskild registrerad eller dennes personuppgifter. En organisation som har under 250 anställda kan dock vara undantagen från detta krav på att föra ett register över behandling.

Konsekvensbedömningar avseende dataskydd och förhandssamråd

Om en viss typ av behandling sannolikt leder till en hög risk för enskildas fri- och rättigheter ska den personuppgiftsansvarige utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.[10] Om den personuppgiftsansvarige har utsett ett dataskyddsombud ska detta rådfrågas. Vad bedömningen ska innefatta anges i förordningen. När det är lämpligt ska de registrerades synpunkter inhämtas, vilket kan ske genom en organisation som företräder dessa. Om bedömningen visar att behandlingen skulle leda till en hög risk ska den personuppgiftsansvarige samråda med tillsynsmyndigheten (förhandssamråd).[11]

Artikel 29-gruppen har utfärdat riktlinjer om konsekvensbedömningar avseende dataskydd (WP 248).[12]

Säkerhet för personuppgifter

Dataskyddsförordningen kräver att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig nivå av informationssäkerhet i samband med behandling av personuppgifter.[13] Syftet med dessa säkerhetsåtgärder är att garantera systemens konfidentialitet, integritet, tillgänglighet och motståndskraft. Även dessa åtgärder ska baseras på en bedömning av vilka risker behandlingen innebär för den registrerades fri- och rättigheter. Det kan t.ex. vara lämpligt att skydda personuppgifter genom kryptering och pseudonymisering. Den ansvarige måste också regelbundet testa, undersöka och utvärdera skyddsåtgärdernas verkningsfullhet.

ISO/IEC 27000-serien innehåller en samling standarder för informationssäkerhet som en organisation kan använda för att genomföra dataskyddsförordningens krav på säkerhet för personuppgifter.

Anmälan av personuppgiftsincident

Vid en personuppgiftsincident (t.ex. ett dataintrång) ska den personuppgiftsansvarige utan onödigt dröjsmål eller senast inom 72 timmar anmäla incidenten till behörig tillsynsmyndighet.[14] Vad en sådan anmälan ska innehålla anges i förordningen. Den personuppgiftsansvarige är också skyldig att dokumentera alla personuppgiftsincidenter. Om det finns en hög risk för de registrerades fri- och rättigheter ska den personuppgiftsansvarige dessutom utan onödigt dröjsmål informera dessa om incidenten.[15]

Uppförandekoder och certifiering

Dataskyddsförordningens allmänna regler kan vara svåra att omedelbart tillämpa på de specifika förhållandena inom en industri, bransch eller något annat livsområde. Förordningen gör det därför möjligt att genom viss självreglering specificera hur dess bestämmelser ska tillämpas. En sådan uppförandekod får utarbetas av en branschorganisation eller liknande sammanslutning. För att koden ska få den rättsliga status som avses i förordningen ska den ges in till och godkännas av behörig tillsynsmyndighet. Efterlevnaden av koden ska övervakas av ett organ som ackrediterats av behörig tillsynsmyndighet. En kod som godkänns genom ett särskilt förfarande kan få allmän giltighet i unionen.[16]

Den personuppgiftsansvarige kan även genom certifiering, som utförts enligt en godkänd certifieringsmekanism, visa att dess behandling av personuppgifter är förenlig med förordningen. Certifiering utförs av en behörig tillsynsmyndighet eller ett ackrediterat certifierings-

organ.[17] Det är för närvarande oklart hur sådan certifiering kommer att vara organiserad i Sverige.

[1] Artikel 37.1 a i förordning (EU) 2016/679. Skyldigheten gäller behandling som domstolar utför som en del av domstolens dömande verksamhet.

[2] Artikel 37.1 b och c i förordning (EU) 2016/679.

[3] Artikel 38–39 i förordning (EU) 2016/679.

[4] Artikel 29-gruppens riktlinjer om dataskyddsombud (WP 243), antagen den 13 december 2016 och senast ändrad den 5 april 2017. [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048].

[5] Artikel 24 i förordning (EU) 2016/679.

[6] Artikel 25.1 i förordning (EU) 2016/679.

[7] Artikel 25.2 i förordning (EU) 2016/679.

[8] European Union Agency for Network and Information Security. [www.enisa.europa.eu/topics/data-protection/privacy-by-design].

[9] Artikel 30 i förordning (EU) 2016/679.

[10] Artikel 35 i förordning (EU) 2016/679.

[11] Artikel 36 i förordning (EU) 2016/679.

[12] Artikel 29-gruppens riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen sannolikt leder till en hög risk i den mening som avses i förordning 2016/679 (WP 248), antagen 4 april 2017 och senast ändrad den 4 oktober 2017 [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236].

[13] Artikel 32 i förordning (EU) 2016/679. Se även Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (”NIS-direktivet”) (EUT L 194, 19.7.2016, s. 1–30), som ska vara genomfört i svensk rätt senast den 10 maj 2018. Förslag till svensk nationell lagstiftning har lämnats i betänkandet SOU 2017:36 Informationssäkerhet för samhällsviktiga och digitala tjänster.

[14] Artikel 33 i förordning (EU) 2016/679.

[15] Artikel 34 i förordning (EU) 2016/679.

[16] Artikel 40–41 i förordning (EU) 2016/679.

[17] Artikel 42–43 i förordning (EU) 2016/679.

Gränsöverskridande behandling av personuppgifter

EU:s dataskyddsförordning gäller som huvudregel för personer eller organisationer som antingen är etablerade i Europeiska unionen (EU) eller Europeiska ekonomiska samarbetsområdet (EES). Den gäller dock även för företag som är etablerade utanför unionen när dessa riktar erbjudanden till personer som befinner sig i unionen eller övervakar deras beteende. Det saknar också betydelse var behandlingen utförs.

Var gäller dataskyddsförordningen?

Dataskyddsförordningen gäller för företag, myndigheter och andra organisationer som är etablerade i något av Europeiska unionens medlemsstater eller i en stat som är medlem i Europeiska ekonomiska samarbetsområdet (EES).[1] Förutom EU:s 28 medlemsstater gäller förordningen alltså även Island, Norge och Lichtenstein.[2] Schweiz är medlem i EFTA, men inte EES och räknas därför som tredje land.

Ett företag i tredje land (t.ex. Schweiz, USA eller Kina) som riktar erbjudanden om varor eller tjänster till personer som befinner sig i unionen eller som övervakar deras beteende i unionen ska också följa EU:s dataskyddsregler.[3] Om en person eller organisation omfattas av förordningen spelar det heller ingen roll var behandlingen utförs.[4] Om ett svenskt företag eller en svensk myndighet anlitar ett företag i tredje land för att t.ex. utföra dess löneutbetalningar omfattas denna behandling av de anställdas personuppgifter fortfarande av dataskyddsförordningen.

När är det tillåtet att överföra personuppgifter till tredje land

Ett av dataskyddsförordningens syften är att säkerställa en fri rörlighet av personuppgifter inom unionen. Det är däremot som huvudregel förbjudet att överföra personuppgifter till ett land utanför unionen eller EES. För att det ska vara tillåtet att överföra personuppgifter till tredje land krävs som huvudregel att det finns ett beslut om adekvat skyddsnivå.[5]

Om ett svenskt företag eller en svensk myndighet anlitar en tjänsteleverantör i tredje land är det viktigt att kontrollera att denne omfattas av ett sådant beslut eller att det finns någon annan rättslig grund för överföring av personuppgifter. Detsamma gäller om ett svenskt företag eller en svensk myndighet överför personuppgifter till en myndighet eller ett lärosäte i tredje land eller en internationell organisation.

Ett beslut om adekvat skyddsnivå ska fattas av Europeiska kommissionen. Det finns ett sådant beslut som gör det möjligt att överföra personuppgifter till USA (”EU-US Privacy Shield”).[6] Beslutet gäller dock endast för amerikanska företag som har anslutit sig till detta arrangemang genom amerikanska handelsministeriet. Endast företag som finns med på handelsministeriets lista omfattas av beslutet.

www.privacyshield.gov/list

Beslut som antagits enligt 1995 års dataskyddsdirektiv gäller tills vidare.[7]

Om ett företag eller en organisation i tredje land inte omfattas av ett sådant beslut är det endast tillåtet att överföra personuppgifter förutsatt att en adekvat skyddsnivå kan garanteras på något annat sätt. En multinationell företagskoncern kan t.ex. använda sig av bindande företagsbestämmelser (”binding corporate rules”).[8] Bestämmelserna ska godkännas av behörig tillsynsmyndighet och fungerar som en intern uppförandekod. Det går även att använda standardavtalsklausuler som har godkänts av kommissionen.[9] Den registrerade kan också lämna ett uttryckligt samtycke till en överföring av hans eller hennes personuppgifter.[10] Det finns även vissa andra undantag.[11]

Noter

[1] Artikel 3 i förordning (EU) 2016/679 anger dess territoriella tillämpningsområde. Vad som avses med ”etablerad” i unionen definieras inte i förordningen, men det framgår av skäl 22 att det som avses är ”det faktiska och reella utförandet av verksamhet med hjälp av en stabil struktur” samt att den rättsliga formen inte är avgörande. Se även EU-domstolens dom av den 28 juli 2016 i mål C-191/15 *Verein für Konsumenteninformation mot Amazon EU Sàrl* (ECLI:EU:C:2016:612), dom av den 1 oktober 2015 i mål C-230/14 *Weltimmo s.r.o. mot Nemzeti Adatvédelmi és Információszabadság Hatóság* (ECLI:EU:C:2015:639) samt dom av den 13 maj 2014 i mål C‑131/12 *Google Spain SL och Google Inc. mot Agencia Española de Protección de Datos (AEPD) och Mario Costeja González* (ECLI:EU:C:2014:317).

[2] Förordning (EU) 2016/679 blir inte omedelbart tillämplig i Norge, Island och Lichtenstein, utan måste först införlivas i Avtalet om Europeiska ekonomiska samarbetsområdet. Se Europeiska kommissionens meddelande ”Starkare skydd, nya möjligheter - riktlinjer från kommissionen om den direkta tillämpningen av den allmänna dataskyddsförordningen från och med den 25 maj 2018”, COM(2018) 43 slutlig. För mer information se [http://www.efta.int/eea-lex/32016R0679].

[3] Artikel 3.2 i förordning (EU) 2016/679. Bestämmelsen innebär en utvidgning av Europeiska unionens dataskyddsregler i jämförelse med vad som gäller enligt direktiv 95/46/EG, som endast var tillämpligt på organisationer som var etablerade i unionen.

[4] Artikel 3.1 i förordning (EU) 2016/679 anger uttryckligen att behandling inom ramen för verksamhet som bedrivs av en organisation som är etablerad i unionen omfattas av förordningen ”oavsett om behandlingen utförs i unionen eller inte”. Det är värt att lägga märke till att överföring av personuppgifter till en tjänsteleverantör i tredje land dessutom omfattas av de särskilda bestämmelserna om överföring till tredje land.

[5] Artikel 44–50 i förordning (EU) 2016/679.

[6] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna (EUT L 207, 1.8.2016, s. 1–112).

[7] Artikel 45.9 i förordning (EU) 2016/679. Beslut enligt direktiv 95/46/EG gäller tills de ändrats, ersatts eller upphävts genom kommissionsbeslut.

[8] Artikel 47 i förordning (EU) 2016/679. Bindande företagsbestämmelser ska godkännas av behörig tillsynsmyndighet. Se även [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_sv].

[9] Artikel 46.2 c i förordning (EU) 2016/679. Se även [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en].

[10] Artikel 49.2 a i förordning (EU) 2016/679. Ett samtycke ska vara uttryckligt, vilket innebär ett strängare krav än vad som gäller för den registrerades samtycke till behandling av personuppgifter i allmänhet.

[11] Artikel 49 i förordning (EU) 2016/679 innehåller undantag i särskilda situationer när det inte föreligger ett beslut om adekvat skyddsnivå enligt artikel 45 eller om lämpliga skyddsåtgärder enligt artikel 46, vilket innefattar bindande företagsbestämmelser.

Sjyst data! – Ett forsknings- och innovationsprojekt kring dataskydd och integritet

Användardata är hårdvaluta på den digitala marknaden och används i många sammanhang; allt från olika tillämpningar, media, reklam och marknadsundersökningar till samhällsfunktioner som trafikövervakning samt säkerhet och trygghet. Här finns stora affärsmöjligheter för företag som använder data på rätt sätt. 2016 antog EU en ny dataskyddsförordning, GDPR, som träder i kraft 2018 och ersätter nuvarande personuppgiftslagstiftning i medlemsländerna. Projektets hypotes är att användardata ska kunna utnyttjas bättre, ur flera parters perspektiv, även med ny lagstiftning på plats. En möjlighet som projektet ska utreda är om det finns förutsättningar för att skapa en integritetscertifiering för digitala tjänster.

Projektet avser att bidra till en konstruktiv affärsutveckling för avsändare av olika digitala tjänster baserade på användardata som främjar tillit utifrån juridiska, etiska och affärsmässiga krav. Detta kommer förhoppningsvis även att skapa ett ökat förtroende hos konsumenter gentemot avsändaren av en tjänst.

Läs mer på **sjystdata.se**

RI.SE VINNOVA bumbee labs KANTAR SIFO MALMÖ UNIVERSITET iab. ÖRESUNDS KRAFT

LUND UNIVERSITY Urban ICT Arena SANDVINE SEB