Vägledning om dataskydd

God integritet vid digital tjänste- och affärsutveckling

2019:2

Vägledning om dataskydd

God integritet vid digital tjänste- och affärsutveckling

Jonas Ledendal

Revision
2019:2

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 år senare står det klart att dataskydd handlar om betydligt mer än att bara uppdatera sin integritetspolicy 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 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, marknadsundersökningar, 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, Kantar Audit (f.d. TS Mediefakta AB), Sandvine AB, Skandinaviska Enskilda Banken AB, Urban ICT Arena och Öresundskraft AB. Projektet finansieras med 10 miljoner kronor av Vinnova inom programmet Utmanings-driven innovation (UDI) som är en satsning för att lösa samhällsutmaningar som kräver bred samverkan.

Håkan Cavenius

projektledare

Stockholm den 4 november 2019

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. 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. 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. 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.

I januari 2012 inleddes en dataskyddsreform, som under 2016 ledde till att EU antog det s.k. dataskyddspaketet. 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.

Grundläggande fri- och rättigheter

Syftet med dataskyddsrätten är att skydda enskilda individers grundläggande fri- och rättigheter i samband med behandling av personuppgifter. Rätten till respekt för privatlivet är en grundläggande fri- och rättighet som i flera folkrättsliga instrument erkänts som en mänsklig rättighet. Ett sådant erkännande finns exempelvis både i FN:s allmänna förklaring om de mänskliga rättigheterna[1] och den internationella konventionen om medborgerliga och politiska rättigheter[2]. Ett motsvarande erkännande finns i Europarådets konvention om de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen).[3] Sverige har genom att ansluta sig till dessa konventioner åtagit sig att skydda rätten till privatliv. Detta gäller även människors rätt till privatliv i den digitala miljön. I den svenska grundlagen föreskrivs också att var och en ska vara skyddad mot intrång i den personliga integriteten. Dessutom gäller Europakonventionen som lag i Sverige, vilket innebär att dess bestämmelser direkt kan åberopas i en svensk domstol.[4]

En rätt till respekt för privatlivet föreskrivs även i Europeiska unionens stadga om de grundläggande rättigheterna.[5] Stadgas bestämmelser speglar i stor utsträckning vad som redan gäller enligt Europakonventionen. I unionsrätten erkänns dock härutöver även en rätt till skydd av personuppgifter som en separat grundläggande rättighet.[6] Sverige är genom sitt EU-medlemskap även bundet att skydda dessa grundläggande rättigheter. Stadgan, som utgör primärrätt, har företräde framför nationell rätt och är direkt tillämplig i medlemsstaterna, men gäller endast inom unionsrättens område.[7] Den ersätter alltså inte helt och hållet motsvarande konstitutionella bestämmelser i medlemsstaterna. Det senare har dock på grund av en långtgående harmonisering begränsad relevans på dataskyddsrättens område.

Rätten till skydd av personuppgifter är emellertid, liksom andra grundläggande fri- och rättigheter, inte en absolut rättighet. Det framgår av uttalanden i ingressen till EU:s dataskyddsförordning att denna rätt måste förstås utifrån sin uppgift i samhället och måste vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen.[8] Rätten till skydd av personuppgifter måste exempelvis sammanjämkas med yttrande- och informationsfriheten. Stadgan tillåter att dessa rättigheter begränsas förutsatt att en sådan inskränkning är föreskriven i lag och förenlig med det väsentliga innehållet i de fri- och rättigheter som föreskrivs i stadgan. En begränsning ska också i enlighet med proportionalitetsprincipen vara nödvändig och faktiskt svara mot ett mål av allmänt samhällsintresse som erkänns av unionen eller behovet av att skydda andra människors fri- och rättigheter.[9] Dataskyddsförordningen och andra sekundärrättsliga bestämmelser ska betraktas som en sådan avvägning mellan olika intressen.[10]

Fri rörlighet för data

Europeiska unionens dataskyddsrätt, särskilt EU:s dataskyddsförordning, utgör ett led i att förverkliga den digitala inre marknaden. En målsättning med EU:s dataskyddsreform var att säkerställa en enhetlig skyddsnivå för att undanröja hinder för det fria flödet av personuppgifter inom unionen. Ett av förordningens syften var att motverka den fragmentering som uppkommit sedan antagandet av 1995 års dataskyddsdirektiv. Sådana skillnader kan annars bli ett hinder för tillhandahållande av gränsöverskridande digitala tjänster, men också varor vilka idag tenderar allt bli allt mer uppkopplade. Unionens dataskyddsrätt har således två ändamål, dels att skydda enskilda individers fri- och rättigheter, men också att säkerställa det fria flödet av personuppgifter inom unionen. För att en inre digital marknad ska fungera krävs emellertid också att användarna har tillit till digitala tjänster. De nya regler som tillkom genom dataskyddsreformen var också ett svar på att undersökningar som gjorts av kommissionen visade på en stor oro bland EU-medborgare för hur deras personuppgifter används på internet.[11] Detta motiverade en förstärkning av skyddet, bl.a. genom att ge registrerade ökad insyn och kontroll. Ett starkt och enhetligt skydd av personuppgifter utgör alltså även ett medel för att säkerställa att den inre digitala marknaden fungerar.

I en datadriven ekonomi är det allt viktigare att data, precis som varor och tjänster, kan röra sig fritt över gränser. Lagstiftning som begränsar fri rörlighet för data kan bli ett handelshinder, dels för att data i sig har blivit en handelsvara, men också därför att dataflöden utgör en nödvändig beståndsdel vid tillhandahållandet av varor och tjänster. Detta gäller särskilt nya uppkopplade produkter som sakernas internet (”internet of things”), men även exempelvis vid tillhandahållande av finansiella tjänster. Det talas numera därför om en femte frihet vid sidan av den fria rörligheten för varor, tjänster, kapital och personer (de fyra friheterna). En sådan fri rörlighet för data säkerställs, som nämns ovan, genom EU:s dataskyddsrätt, men även av en parallell förordning om en ram för det fria flödet av andra data än personuppgifter.[12] Förordningen syftar till att säkerställa ett sådant fritt flöde genom att fastställa gemensamma regler avseende datalokaliseringskrav, tillgång till data för behöriga myndigheter och dataportering för professionella användare. Det finns ingen motsvarande regim på internationell nivå, vilket är ett ökande problem vid internationell handel.

EU:s rättsliga ram för dataskydd

Bestämmelser på sekundärrättslig nivå finns numera i första hand i EU:s allmänna dataskyddsförordning, men också i ett flertal sektorsspecifika rättsakter. Exempelvis finns särskilda bestämmelser om myndigheters brottsbekämpande verksamhet och elektronisk kommunikation.

EU:s allmänna dataskyddsförordning

Europeiska unionens dataskyddsrätt regleras i första hand genom EU:s allmänna dataskyddsförordning (GDPR)[13], som antogs den 27 april 2016 och numera har ersatt EU:s dataskyddsdirektiv från 1995[14]. Förordningen blev direkt tillämplig i Sverige och alla andra medlemsstater den 25 maj 2018. 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.[15] Lagen kompletteras i sin tur med tillämpningsföreskrifter som finns i den svenska förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning.[16] 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.

Brottsbekämpande verksamhet

EU:s dataskyddsförordning gäller inte när behöriga myndigheter behandlar personuppgifter i samband med polisiär och annan brottsbekämpande verksamhet. Sådan behandling regleras i stället av ett särskilt EU-direktiv som antogs 2016 i samband med EU:s dataskyddsreform.[17] 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. Direktivet har i första hand införlivats i svensk rätt genom brottsdatalagen, som trädde i kraft den 1 augusti 2018.[18]

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-integritetsdirektivet) från 2002 och som har ändrats 2009.[19] Direktivet har i första hand införlivats i svensk rätt genom vissa bestämmelser i lagen om elektronisk kommunikation (LEK)[20] och marknadsföringslagen (MFL)[21].

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. 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.

Det innebär att kommunikation och relaterade trafikuppgifter inte utan samtycke får fångas upp eller lagras av andra personer än användarna. 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. Trafikuppgifter om abonnenter och användare ska dock normalt raderas eller anonymiseras så snart de inte längre behövs för att överföra kommunikation. Det är alltså som huvudregel inte tillåtet att lagra sådana uppgifter för andra ändamål än fakturering av abonnemangsavgifter. För marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av mervärdestjänster krävs abonnentens eller användarens samtycke.

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.

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. 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.

Svensk tillsynsmyndighet för verksamhet som faller under lagen om elektronisk kommunikation är Post- och telestyrelsen (PTS).

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. ”e-Privacy-förordningen”) samt om upphävande av 2002 års direktiv.[22] 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.[23] 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.[24] Domstolen har i ett senare avgörande även slagit fast att de svenska bestämmelser i lagen om elektronisk kommunikation som genomför datalagringsdirektivet strider mot unionsrätten.[25] 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 skulle göras förenliga med unionsrätten och ny lagstiftning baserad på detta förslag trädde i kraft den 1 oktober 2019.[26] Genom den nya lagen införs åter ett krav på att operatörer lagrar trafikuppgifter som ska kunna användas vid brottsbekämpning. De nya reglerna överensstämmer i huvudsak med tidigare regler, men innehåller vissa inskränkningar som är avsedda att tillgodose EU-rättens krav på skydd av grundläggande fri- och rättigheter.

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. För att övervaka unionens institutioners, organs 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 dessa regler med GDPR antogs den 23 oktober 2018.[27]

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.

EU:s dataskyddsförordning

EU:s dataskyddsförordning innehåller bestämmelser om skydd av enskilda individers fri och rättigheter i samband med behandling av personuppgifter. Dessa gäller i princip för all verksamhet som innefattar behandling av sådana uppgifter, oberoende av om den som utför behandlingen är ett företag eller en myndighet. Alla organisationer måste därför se till att de följer dataskyddsförordningen, vilket bl.a. innebär att de måste vidta lämpliga tekniska och organisatoriska åtgärder för att minska de risker som kan uppkomma för registrerade.

Dataskyddsförordningens syfte

Dataskyddsförordningens har två parallella syften: dels att skydda människors fri och rättigheter i samband med behandling av deras personuppgifter, men också att säkerställa ett fritt flöde av personuppgifter i unionen.[28] EU-domstolen har konstaterat att syftet med unionens dataskyddsrätt är att säkerställa en hög skyddsnivå för enskilda individers fri och rättigheter, särskilt deras rätt till privatliv. Dataskyddsbestämmelserna ska därför normalt tolkas på ett sätt som säkerställer ett effektivt och fullständigt skydd av dessa rättigheter. Domstolen har således till förmån för den registrerade gett många centrala dataskyddsrättliga begrepp, såsom person-uppgifter och personuppgiftsansvarig, en vidsträckt innebörd. Det ska helt enkelt inte vara möjligt att kringgå ansvar genom att luta sig mot teknikaliteter.

Materiellt tillämpningsområde

Dataskyddsförordningen omfattar i princip all verksamhet som innefattar behandling av personuppgifter. Vad som menas med ”personuppgifter” och ”behandling” av sådana uppgifter blir alltså ytterst bestämmande för vad som omfattas av unionens dataskyddsbestämmelser (det materiella tillämpningsområdet).

Vad räknas som personuppgifter?

Vad som räknas som ”personuppgifter” definieras i dataskyddsförordningen:

> **personuppgifter**: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

Begreppet omfattar all sorts information som avser en identifierad eller identifierbar människa. Det avgörande för om en uppgift ska vara att anse som en personuppgift är alltså om uppgiften avser en människa (”fysisk person” med en juridisk term) samt om han eller hon kan identifieras med hjälp av denna. Om uppgiften inte avser en fysisk person omfattas dess behandling alltså inte av dataskyddsreglerna. Exempelvis omfattas inte uppgifter som avser juridiska personer, såsom bolag, föreningar eller stiftelser. Förordningen omfattar dessutom endast nu levande människor. Det är dock inte helt klart vad som gäller beträffande ofödda barn, vilket bl.a. har praktisk relevans vid frysförvaring av embryon och foster-diagnostik.

Begreppet personuppgifter ska enligt EU-domstolens rättspraxis ges en vidsträckt tolkning. En uppgift kan ”avse” en människa även om den inte omedelbart beskriver hans eller hennes egenskaper, såsom dennes namn, längd eller vikt. Det är också nödvändigt att beakta syftet med behandlingen och vilka konsekvenser denna kan få för hans eller hennes intressen eller fri- och rättigheter. Exempelvis kan svar som någon lämnat på ett prov vara en personuppgift eftersom dessa samlats in i syfte att göra en bedömning av honom eller henne. Uppgifterna som sådana måste inte handla om personen i fråga.

För att räknas som en personuppgift måste denna även kunna användas för att identifiera en viss fysisk person. Anonym information omfattas inte av dataskyddsförordningen. Det är inte nödvändigt att någon är direkt identifierbar, det är tillräckligt att han eller hon indirekt kan identifieras med hjälp av uppgiften. Exempelvis kan ett IP-nummer inte direkt kopplas till en specifik person, men många IP-nummer räknas ändå som personuppgifter eftersom de indirekt kan kopplas till en människa genom att kombineras med andra uppgifter, t.ex. genom ett abonnemang eller vem som äger en apparat.

Lagstöd: Artikel 4.1 i GDPR. Läs mer: Artikel 29-arbetsgruppens yttrande 4/2007 om begreppet personuppgifter, antagen den 20 juni 2007 (WP 136). Rättspraxis: EU-domstolens dom av den 19 oktober 2016 i mål C-582/14 *Breyer*; dom av den 20 december 2017 i mål C-434/16 *Nowak*.

Vad räknas som behandling av personuppgifter?

Vad som räknas som ”behandling” av personuppgifter definieras i dataskyddsförordningen:

> **behandling**: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

Begreppet omfattar i princip varje åtgärd som vidtas beträffande personuppgifter, men det finns vissa verksamheter som är undantagna. Begreppet ska tolkas vidsträckt. Utgångspunkten är att dataskyddsrätten reglerar hela datalivscykeln från insamling till radering av personuppgifter. Bestämmelserna omfattar i första hand automatiserad behandling, det vill säga behandling som helt eller delvis sker med hjälp av datorteknik, men regleringen är i princip teknikneutral. För att förordningen ska bli tillämplig på fullständigt manuell behandling krävs dock att personuppgifterna antingen ingår i eller kommer att ingå i ett register. Med register avses en strukturerad samling av personuppgifter som gjorts sökbara enligt särskilda kriterier. Exempelvis ett kortregister. Däremot omfattas inte ostrukturerade handskrivna anteckningar som inte är avsedda att ingå i ett sådant register.

Lagstöd: Artikel 2 och 4.2 i GDPR.

> **Missbruksregeln har upphört**
>
> Tidigare omfattades inte personuppgifter i ostrukturerat material fullt ut av de svenska reglerna om skydd av personuppgifter (den s.k. missbruksregeln). 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. Även personuppgifter i ostrukturerat material, såsom ett ordbehandlingsdokument eller e-postmeddelande, omfattas alltså numera fullt ut av dataskyddsregleringen.

Verksamhet som är undantagen

EU:s dataskyddsförordning är i princip tillämplig på all verksamhet som innefattar behandling av personuppgifter, men det finns vissa undantag som föreskrivs i förordningen eller kompletterande lagstiftning. Det är dock värt att nämna att sådan verksamhet inte sällan i stället omfattas av sektorsspecifik reglering. Syftet med dessa undantag är att undvika en överlappning mellan förordningens allmänna bestämmelser och sådan speciallagstiftning. I dataskyddsförordningen föreskrivs att denna inte ska vara tillämplig på följande verksamheter:

- Privatpersoners behandling av rent privat natur eller som har samband med hans eller hennes hushåll. Det är trots rättspraxis från EU-domstolen inte helt klart var gränsen ska dras, men behandlingen får inte ha samband med yrkesmässig verksamhet.
- Behandling som faller inom ramen för den gemensamma utrikes och säkerhetspolitiken eller rör verksamhet som inte omfattas av unionsrätten. I enlighet med svensk nationell rätt ska dataskyddsförordningen dock även tillämpas på dessa områden med undantag för viss militär och polisiär underrättelseverksamhet som regleras i annan lagstiftning.
- Behandling som behöriga myndigheter utför i samband med brottsbekämpande verksamhet. För denna behandling gäller i stället ett direktiv om dataskydd vid brottsbekämpande verksamhet, som i svensk rätt i huvudsak har införlivats genom brottsdatalagen.
- Behandling som sker i Europeiska unionens institutioner, organs och byråers verksamhet. För denna behandling gäller i stället en särskild förordning om dataskydd.

För verksamhet som faller utanför undantagen gäller dataskyddsförordningens allmänna bestämmelser. Exempelvis gäller förordningen som vanligt när polis- eller åklagarmyndigheten i sin personaladministrativa verksamhet behandlar anställdas personuppgifter för att betala ut löner. Bortsett från EU:s institutioner, organ och byråer omfattas alltså endast vissa verksamhetsområden av undantagen, inte hela organisationen.

Lagstöd: Artikel 2.2–3 i GDPR.

Personuppgiftsansvar

Det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för behandlingen, vilket innebär att det är denne som ska vidta de tekniska och organisatoriska åtgärder som krävs för att behandlingen ska överensstämma med dataskyddsregleringen. Det är också den personuppgiftsansvarige som kan drabbas av sanktioner om behandlingen inte uppfyller dessa krav.

Vem ansvarar för behandlingen?

Vad som räknas som ”personuppgiftsansvarig” definieras i dataskyddsförordningen:

> **personuppgiftsansvarig**: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter

Det är den personuppgiftsansvarige som fastställer ändamålet med behandlingen. Vem som ska vara personuppgiftsansvarig regleras normalt inte i lag, men när det finns sådana föreskrifter får beslutet endast fattas av det organ som anges i föreskrifterna. Om sådana föreskrifter saknas blir det i stället omvänt så att den som faktiskt fattat beslutet ensam eller tillsammans med andra blir ansvarig för behandlingen.

Den ansvarige är normalt en organisation, men även en fysisk person kan räknas som personuppgiftsansvarig. Exempelvis finns det inget hinder mot att någon som driver enskild firma eller är bolagsman i ett enkelt bolag är

ansvarig för verksamhetens personuppgiftsbehandling. Det finns heller inget krav på att den ansvarige ska vara en egen juridisk person. Begreppet omfattar privaträttsliga subjekt såsom bolag, föreningar och stiftelser, men också myndigheter och andra offentliga organ. Den rättsliga formen är alltså inte avgörande för om någon ska räknas som ansvarig för behandling av personuppgifter.

Lagstöd: Artikel 4.7 i GDPR. Läs mer: Artikel 29-gruppens yttrande 1/2010 om begreppen registeransvarig och registerförare (WP 169), antaget den 16 februari 2010.

Vem räknas som personuppgiftsbiträde?

Vad som räknas som ”personuppgiftsbiträde” definieras i dataskyddsförordningen:

> **personuppgiftsbiträde**: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

Den som endast utför behandling av personuppgifter för någon annans räkning, utan att själv vara personuppgiftsansvarig, kallas för personuppgiftsbiträde. Ett biträde får endast behandla personuppgifter enligt den personuppgiftsansvariges instruktioner, men har också ett visst eget ansvar för att behandlingen.

Lagstöd: Artikel 4.8 i GDPR. Läs mer: Artikel 29-gruppens yttrande 1/2010 om begreppen registeransvarig och registerförare (WP 169), antaget den 16 februari 2010.

Territoriellt tillämpningsområde

EU:s dataskyddsförordning är i första hand tillämplig på verksamhet som bedrivs i unionen, men till skillnad från tidigare regler omfattas även vissa organisationer i tredje land. Förordningens bestämmelser gäller förutom i EU:s medlemsstater i enlighet med EES-avtalet dessutom även i Norge, Lichtenstein och Island. För organisationer som är etablerade i Europeiska ekonomiska samarbetsområdet gäller förordningen all behandling, men för andra organisationer blir den endast tillämplig på vissa verksamhetsområden och beträffande registrerade som befinner sig i unionen.

För en organisation som är etablerad i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet gäller EU:s dataskyddsförordning fullt ut. Det avgörande är den personuppgiftsansvariges eller biträdets verksamhetsort, inte den registrerades nationalitet eller bosättningsort. Det har heller ingen betydelse var i världen själva behandlingen utförs. För en organisation som är etablerad i unionen gäller alltså EU:s dataskydds-förordning fullt ut även om behandlingen för dennes räkning utförs av en annan organisation i tredje land eller om behandlingen avser personer som är bosatta i tredje land. Med verksamhetsställe menas det faktiska och reella utförandet av verksamhet med hjälp av en stabil struktur. Den rättsliga form i vilken verksamheten bedrivs är inte avgörande. Förutsatt att denna har en stabil struktur så saknar det betydelse om verksamheten utgör en egen juridisk person. Behandlingen måste dock anses ske inom ramen för den verksamhet som bedrivs i unionen. Det är inte helt klart vad som gäller om delar av verksamheten bedrivs vid ett verksamhetsställe utanför unionen, men enligt tidigare praxis från EU-domstolen skulle denna ibland betraktas som en enhet på vilken unionsrätten blev tillämplig.

För en organisation som saknar verksamhetsställe i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet gäller EU:s dataskyddsförordning inte fullt ut. En nyhet i förhållande till tidigare dataskydds-bestämmelser är dock att unionens dataskyddsregler även kan bli tillämpliga på delar av den verk-samhet som bedrivs av sådana organisationer. Syftet med denna utvidgning är att anpassa dataskyddsrätten till den digitala utvecklingen. Det är numera i stor utsträckning möjligt att tillhandahålla varor och tjänster till personer som befinner sig i en medlemsstat utan att ha något verksamhetsställe i unionen. För att registrerade genom denna utveckling inte ska fråntas det skydd som förordningen ger dem måste även ett företag som är etablerat i tredje land följa EU:s dataskyddsförordning när detta riktar erbjudanden om varor och tjänster till fysiska personer som befinner sig i unionen eller övervakar sådana personers beteende i unionen. Detta gäller även om de marknadsförda varorna eller tjänsterna är kostnadsfria. Förordningen ska dessutom tillämpas på verksamhet som bedrivs utanför unionen när en medlemsstats nationella rätt enligt folkrätten gäller på den platsen. Exempelvis en medlemsstats diplomatiska beskickning eller konsulat i tredje land. Detsamma gäller på ett fartyg som är flaggat i en medlemsstat, oavsett var det befinner sig. Den som inte är etablerad i unionen ska också utse en företrädare i unionen.

Lagstöd: Artikel 3 och 27 i GDPR. Läs mer: Europeiska dataskyddsstyrelsens Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version for public consultation.

Grundläggande dataskyddsprinciper

All behandling av personuppgifter ska uppfylla ett antal grundläggande krav (principer för dataskydd). 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.

Lagstöd: Artikel 5 i GDPR.

Rättslig grund

För att behandlingen ska vara tillåten måste den ske enligt någon av följande rättsliga grunder

- den registrerades samtycke
- avtals ingående eller fullgörande
- fullgörande av en annan rättslig förpliktelse
- skydd av människors vitala intressen
- uppgift av allmänt intresse eller myndighetsutövning
- annat berättigat intresse

Den rättsliga grunden för behandlingen ska alltid fastställas innan behandlingen påbörjas så att denna information kan lämnas till de registrerade. Även om det inte är obligatoriskt så antecknas den rättsliga grunden vanligtvis också i det register över behandling som de flesta personuppgiftsansvariga är skyldiga att föra enligt dataskyddsförordningen.

Den registrerades samtycke

De flesta organisationer förlitar sig i första hand på samtycke som grund för behandling av personuppgifter. Detta beror inte sällan på en vanligt förekommande missuppfattning om att detta är ett krav enligt EU:s dataskyddsförordning. En annan vanlig förklaring är att samtycke påminner om ett avtal, en regleringsform som många företag redan känner sig bekanta med. Det är dock värt att lägga märke till att samtycke inte alltid är möjligt eller lämpligt som grund för behandling av personuppgifter. För att ett samtycke ska vara giltigt måste viljeförklaringen vara

1. frivillig
2. specifik
3. informerad
4. otvetydig

Det är den person-uppgiftsansvarige som ska bevisa att alla dessa krav är uppfyllda. Det är långt ifrån alla samtycken som uppfyller dessa fyra kumulativa villkor. När ett giltigt samtycke saknas måste behandlingen för att vara laglig i ställer grundas på någon av de andra rättsliga grunderna i dataskyddsförordningen. Det är också värt att påpeka att dessa alltid kan utgöra ett alternativ till den registrerades samtycke. Förordningen kräver alltså inte att den personuppgiftsansvarige först uttömt möjligheten att inhämta samtycke.

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.

I svensk rätt gäller som huvudregel att den som är omyndig (under 18 år) inte kan åta sig förpliktelser utan vårdnadshavares samtycke. I EU:s dataskyddsförordningen finns en särskild bestämmelse om barns samtycke till behandling av sina egna personuppgifter. 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.

> 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.

Lagstöd: Artikel 6.1 a, 4.11, 7 och 8 i GDPR. Läs mer: Artikel 29-arbetsgruppens riktlinjer om samtycke enligt förordning (EU) 2016/679 (WP 259), antagna 10 april 2018.

Avtals ingående eller fullgörande

Behandling av personuppgifter får ske utan de registrerades samtycke om detta är nödvändigt för att ingå eller fullgöra ett avtal. Grunden gäller endast ett avtalsförhållande mellan den registrerade och den personuppgiftsansvarige. Den kan därför inte åberopas vid kollektivavtal. Det finns dock inget hinder mot att behandlingen utförs av någon som den personuppgiftsansvarige anlitat som personuppgiftsbiträde. Det krävs heller inte att något avtal redan träffats, bara att den finns en sådan avsikt från den registrerades sida. Eftersom behandlingen ska vara nödvändig för att ingå ett avtal eller utföra en avtalsförpliktelse kan grunden inte användas för några andra ändamål. Det gäller inte bara utlämnande av uppgifterna till någon annan, utan även den personuppgiftsansvariges egen interna behandling. För sådan

behandling krävs den registrerades samtycke eller en annan rättslig grund.

Lagstöd: Artikel 6.1 b i GDPR.

Rättslig förpliktelse

Behandling av personuppgifter får ske utan de registrerades samtycke om detta är nödvändigt för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. En sådan förpliktelse ska följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Att förpliktelsen ska åvila den personuppgiftsansvarige hindrar inte att behandlingen utförs av någon som den personuppgiftsansvarige anlitat som personuppgiftsbiträde. Den ifrågavarande grunden blir i första hand aktuell när den personuppgiftsansvarige är ett privaträttsligt subjekt, såsom en enskild individ, ett bolag, en förening eller en stiftelse. Exempelvis kan grunden användas vid ett företags redovisning av mervärdesskatt. När den personuppgiftsansvarige är en myndighet och behandlingen avser en uppgift av allmänt intresse eller myndighetsutövning är artikel 6.1 e i GDPR normalt en lämpligare grund. Om det rör sig om en avtalsförpliktelse som inte följer av kollektivavtal gäller i stället artikel 6.1 b i GDPR.

Lagstöd: Artikel 6.1 c i GDPR; 2 kap. 1 § lagen med kompletterande bestämmer till EU:s dataskyddsförordning.

Skydd av människors vitala intressen

Behandling av personuppgifter får ske utan de registrerades samtycke om detta är nödvändigt för att skydda dennes eller andra människors vitala intressen. Det som åsyftas är att någon befinner sig i en nödsituation. Om det krävs för att rädda någons liv är det exempelvis inte nödvändigt att inhämta samtycke. Den aktuella grunden ska dock endast användas som en sista utväg. Om samtycke eller någon annan grund kan användas ska den användas i första hand.

Lagstöd: Artikel 6.1 d i GDPR.

Allmänt intresse och myndighetsutövning

En nyhet i dataskyddsförordningen är att myndigheter inte kan stödja sig på denna intresseavvägningsregel när de fullgör sina uppgifter. 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. 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 ovan om vad som krävs för giltigt samtycke).

Lagstöd: Artikel 6.1 e i GDPR.

Intresseavvägningsregeln

Den registrerades samtycke krävs alltid vid behandling av hans eller hennes personuppgifter, om den personuppgiftsansvarige inte kan stödja sig på en annan rättslig grund. 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 personuppgifts-ansvarige eller tredje parts berättigade intressen. Detta förutsätter dock att skyddet av den registrerades intressen eller grundläggande fri- och rättigheter inte väger tyngre.

Lagstöd: Artikel 6.1 f i GDPR.

Känsliga personuppgifter

För känsliga personuppgifter 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. Med känsliga personuppgifter avses normalt det som i EU:s dataskyddsförordning benämns ”särskilda kategorier av personuppgifter”. 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.

Lagstöd: Artikel 9 och 10 i GDPR.

Tekniska och organisatoriska åtgärder

Principen om ansvarsskyldighet innebär att den personuppgiftsansvarige är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att minska de risker som kan uppkomma för registrerade i samband med behandling av personuppgifter. Det räcker inte att sådana åtgärder rent faktiskt vidtagits den ansvarige måste också kunna visa att behandlingen uppfyller de grundläggande krav som föreskrivs i dataskyddsförordningen. Detta kan bl.a. göras genom sådana godkända uppförandekoder eller certifieringsmekanismer som regleras i förordningen.

För att efterleva dataskyddsförordningen måste den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder. 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.

Lagstöd: Artikel 5.2 och 24 i GDPR.

Inbyggt dataskydd och dataskydd som standard

Dataskyddsförordningen kräver att vissa skydds-åtgärder integreras i de system som används för behandling av personuppgifter (”inbyggt dataskydd”). Ett exempel på sådana skydds-åtgärder 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”). Dessa bestämmelser har sin grund i ”privacy by design”, en designprincip som innebär att integritetskrav ska beaktas redan under utvecklingen av ett IT-system. 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.

Lagstöd: 25 i GDPR.

Automatiserat beslutsfattande

Den registrerade har rätt att slippa att bli föremål för ett beslut som uteslutande grundar sig på automatiserad behandling. 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 antal undantag. Det är t.ex. tillåtet att använda 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. Det är oklart i vilken utsträckning sådana metoder överens-stämmer med EU:s dataskyddsförordning.

Lagstöd: Artikel 22 i GDPR. Läs mer: Artikel 29arbetsgruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679 (WP 251), antagna den 6 februari 2018.

Register över behandling av personuppgifter

Dataskyddsförordningen kräver att den person-uppgiftsansvarige för ett register över behandling av personuppgifter som utförs under dennes ansvar. 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.

Lagstöd: artikel 30 i GDPR.

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. 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).

Lagstöd: artikel 35 och 36 i GDPR. Läs mer: Artikel 29-gruppens riktlinjer om konsekvensbedömningar avseende dataskydd (WP 248).

Säkerhet för personuppgifter

Dataskyddsförordningen kräver att den person-uppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig nivå av informationssäkerhet i samband med behandling av personuppgifter. 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.

Vid en personuppgiftsincident (t.ex. ett dataintrång) ska den personuppgiftsansvarige utan onödigt dröjsmål eller senast inom 72 timmar anmäla incidenten till behörig tillsyns-myndighet. Vad en sådan anmälan ska innehålla anges i förordningen. Den personuppgiftsansvarige är också skyldig att dokumentera alla personuppgifts-

incidenter. Om det finns en hög risk för de registrerades fri- och rättigheter ska den personuppgiftsansvarige dessutom utan onödigt dröjsmål informera dessa om incidenten.

Lagstöd: Artikel 32–34 i GDPR. Läs mer: Artikel 29-gruppens riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679 (WP 250).

Dataskyddsombud

En myndighet måste alltid utse ett dataskydds-ombud. 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 kärn-verksamhet antingen består av regelbunden och systematisk övervakning i stor omfattning eller behandling av känsliga personuppgifter i stor omfattning. Dataskyddsombudets kontakt-uppgifter 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.

Lagstöd: Artikel 37–39 i GDPR. Läs mer: Artikel 29-gruppens riktlinjer om dataskyddsombud (WP 243).

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 tillsyns-myndighet. En kod som godkänns genom ett särskilt förfarande kan få allmän giltighet i unionen.

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 tillsyns-myndighet eller ett ackrediterat certifieringsorgan. Det är för närvarande oklart hur sådan certifiering kommer att vara organiserad i Sverige.

Lagstöd: Artikel 40–43 i GDPR.

Den registrerades rättigheter

För att öka de registrerades kontroll över sina personuppgifter har deras rättigheter förstärkts genom EU:s dataskyddsförordning. Den registrerade har följande rättigheter:

- rätt till information
- rätt till tillgång
- rätt till dataportabilitet
- rätt till rättelse
- rätt till radering (”rätt att bli bortglömd”)
- rätt till begränsning av behandling
- rätt att invända mot behandling
- rätt att slippa automatiserat individuellt beslutsfattande

Att den registrerade har kännedom om sina rättigheter är en förutsättning för att han eller hon ska kunna utöva dessa. Den personuppgiftsansvarige är därför enligt principen om öppenhet skyldig att informera den registrerade om dennes rättigheter i samband med behandling av hans eller hennes personuppgifter. De rättigheter som föreskrivs i förordningen får under vissa förutsättningar begränsas genom annan unionsrättslig eller nationell lagstiftning. Sådana inskränkningar har i svensk rätt bl.a. gjorts beträffande rätten till information och tillgång till personuppgifter. Rätten att slippa bli föremål för automatiserat individuellt beslutsfattande har beskrivits ovan under avsnittet Tekniska och organisatoriska åtgärder.

Lagstöd: Artikel 12–23 i GDPR; 5 kap. lagen med kompletterande bestämmer till EU:s dataskyddsförordning.

Rätt till information

Behandling av personuppgifter ska ske på ett öppet sätt i förhållande till den registrerade. Att den registrerade har god insyn i behandlingen är en förutsättning för att han eller hon ska kunna kontrollera att denna överensstämmer med unionens dataskyddsbestämmelser och vid behov åberopa de andra rättigheter som han eller hon har enligt dataskyddsförordningen. Exempelvis rätten att få sina personuppgifter rättade eller raderade. Den personuppgiftsansvarige har därför en allmän skyldighet att lämna information till registrerade om behandling av deras personuppgifter. Denna information ska lämnas på den personuppgiftsansvariges eget initiativ. Det krävs inte att den registrerade själv efterfrågar informationen. Vilken information som ska lämnas och hur denna ska utformas framgår av dataskyddsförordningen. När informationen ska lämnas skiljer sig åt beroende på om uppgifterna samlas in direkt från den registrerade eller om dessa har hämtats från någon annan datakälla. Huvudregeln är dock att detta ska ske innan behandlingen av de aktuella personuppgifterna påbörjas.

Lagstöd: Artikel 12–14 i GDPR. Läs mer: Artikel 29arbetsgruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679, antagna den 11 april 2018 (WP 260).

Rätt till tillgång

För att öka den registrerades insyn i behandlingen har denne även rätt att få veta om någon behandlar hans eller hennes personuppgifter. Om så är fallet har han eller hon även rätt att få ett registerutdrag samt ytterligare information om behandlingen. Ett sådant utdrag är avgiftsfritt, men om den registrerade begär ytterligare kopior har den personuppgiftsansvarige rätt att ta ut en rimlig avgift. När den personuppgiftsansvarige är en svensk myndighet kompletterar rätten till tillgång enligt dataskyddsförordningen den rätt till partsinsyn som den registrerade kan ha enligt förvaltningslagen eller envars rätt att ta del av allmänna handlingar enligt tryckfrihetsförordningen. Den registrerades rätt till tillgång omfattar endast hans eller hennes personuppgifter, inte andra uppgifter som finns i samma handling. Rätten att få en kopia av uppgifterna får heller inte inverka menligt på andras fri och rättigheter.

Lagstöd: Artikel 15 i GDPR.

Rätt till dataportabilitet

Rätten till dataportabilitet är en nyhet som infördes genom dataskyddsförordningen. Syftet med denna är att öka den registrerades kontroll över sina personuppgifter, men främjar även konkurrens mellan företag som erbjuder digitala tjänster. När behandlingen sker digitalt (automatiserat) har den registrerade rätt att få en elektronisk kopia av sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format. Uppgifterna ska exempelvis kunna laddas ner som en JSON eller XMLfil. När det är tekniskt möjligt har den registrerade även rätt att få sina personuppgifter direkt överförda till en annan tjänsteleverantör. Rätten till dataportabilitet omfattar dock endast när behandlingen grundas på samtycke eller avtal. Den gäller inte vid myndighetsutövning eller liknande verksamhet. Rätten att få en kopia av eller att överföra uppgifterna får heller inte inverka menligt på andras fri och rättigheter.

Lagstöd: Artikel 20 i GDPR. Läs mer: Artikel 29arbetsgruppens riktlinjer om dataportabilitet, antagna den 5 april 2017 (WP 242).

Rätt till rättelse

Den personuppgiftsansvarige ska enligt principen om riktighet på eget initiativ bedriva registervård för att säkerställa att de personuppgifter som denne behandlar inte är felaktiga. Denna skyldighet kompletteras av en rätt för den registrerade att själv begära att en felaktig personuppgift utan onödigt dröjsmål rättas av den personuppgiftsansvarige. Den registrerade har även rätt att få en ofullständig uppgift kompletterad. Vad som räknas som felaktig eller ofullständig får bedömas med hänsyn till syftet med behandlingen. Under handläggningen av ett sådan begäran har den registrerade även rätt att kräva att behandlingen av uppgifterna ska begränsas i väntan på att den personuppgiftsansvarige haft möjlighet att kontrollera deras riktighet (se nedan om rätt till begränsning av behandlingen). Om det inte är omöjligt eller innebär en oproportionerlig ansträngning ska den personuppgiftsansvarige underrätta alla eventuella mottagare av uppgifterna om att dessa har rättats.

Lagstöd: Artikel 16 och 19 i GDPR.

Rätt till radering (”rätt att bli bortglömd”)

En av de mer uppmärksammade rättigheterna är den s.k. ”rätten att bli bortglömd”. Att en sådan fanns redan enligt 1995 års dataskyddsdirektiv konstaterade EU-domstolen i målet *Google Spain och Google*, som gällde en sökmotorleverantörs skyldighet att ta bort länkar till externa webbplatser som visades i ett sökresultat. I EU:s dataskyddsförordning har denna rättighet förtydligats. Rätten att få sina personuppgifter raderade är dock inte villkorslös. Den som vill få sina uppgifter raderade måste visa att en sådan begäran kan motiveras enligt någon av de grunder som räknas upp i bestämmelsen. Även om något av dessa villkor skulle vara uppfyllda kan den personuppgiftsansvarige vägra att radera dessa förutsatt att något av de undantag som räknas upp i samma bestämmelse är tillämpliga. Exempelvis kan personuppgifter som förekommer i en nyhetsartikel på en tidskrifts webbplats sällan raderas med stöd av rätten att bli bortglömd. I det senare fallet väger normalt yttrande och informationsfriheten tyngre än den registrerades rätt till privatliv.

När den registrerade har rätt att bli bortglömd ska den personuppgiftsansvarige radera uppgifterna utan onödigt dröjsmål. Om den registrerade har begärt att uppgifterna ska överföras enligt bestämmelserna om dataportabilitet ska dessa dock först överföras innan de raderas. För att stärka rätten att bli bortglömd i en digital miljö ska den personuppgiftsansvarige dessutom vidta rimliga åtgärder för att informera dem som mottagit personuppgifterna att den registrerade har begärt att dessa ska raderas. Den som får en sådan underrättelse ska radera eventuella länkar till eller kopior av personuppgifterna. Om det inte är omöjligt eller innebär en oproportionerlig ansträngning ska den personuppgiftsansvarige även underrätta alla eventuella mottagare av uppgifterna om att dessa har raderats.

Lagstöd: Artikel 17 och 19 i GDPR. Rättspraxis: EU-domstolens dom av den 13 maj 2014 i mål C131/12 Google Spain och Google.

Rätt till begränsning av behandling

Den registrerade har under vissa villkor rätt att begära att behandlingen av hans eller hennes personuppgifter ska begränsas. Det senare innebär att uppgifterna ska markeras samt med undantag för lagring endast får behandlas för vissa särskilda ändamål som räknas upp i dataskyddsförordningen. Om det inte är omöjligt eller innebär en oproportionerlig ansträngning ska den personuppgiftsansvarige underrätta alla eventuella mottagare av uppgifterna om att behandlingen av dessa har begränsats. Begränsning av behandlingen kan bl.a. bli aktuellt under tiden en begäran om rättelse eller invändning mot behandlingen handläggs av den personuppgiftsansvarige. Att den registrerade har tillgång till en sådan provisorisk åtgärd är praktiskt viktigt eftersom handläggningen av en begäran när det finns skäl för det får ta upp till tre månader. Begränsning kan också

bli aktuell i vissa situationer när den registrerade motsätter sig att uppgifterna raderas. Den registrerade ska alltid underrättas om att begränsningen upphör innan detta beslut verkställs.

Lagstöd: Artikel 18 och 19 i GDPR.

Rätt att invända mot behandling

Den registrerade har när som helst rätt att motsätta sig fortsatt behandling av hans eller hennes personuppgifter även om behandlingen i och för sig är laglig. Denna rätt gäller endast när behandlingen grundas på allmänt intresse, myndighetsutövning eller intresseavvägnings-regeln. Om behandlingen grundas på samtycke kan samma resultat dock åstadkommas genom att samtycket återkallas. När personuppgifter behandlas för direkt marknadsföring är rätten att motsätta sig behandlingen villkorslös, men när det gäller annan behandling ska en avvägning göras mellan den personuppgiftsansvariges och den registrerades intressen. Om den personuppgifts-ansvarige kan visa att det finns avgörande berättigade skäl för behandlingen får denna fortsätta.

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.

Särskilda regler gäller när uppgifter behandlas för forskningsändamål eller statistiska ändamål. I dessa situationer får behandlingen alltid fortsätta om den är nödvändig för att utföra en uppgift av allmänt intresse. I väntan på att den personuppgiftsansvarige kontrollerar om behandlingen får fortsätta har den registrerade rätt att kräva att behandlingen ska begränsas (se ovan om rätt till begränsning av behandlingen).

Lagstöd: Artikel 21 i GDPR.

Överföring 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.

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”). 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. 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”). Bestämmelserna ska godkännas av behörig tillsynsmyndighet och fungerar som en intern uppförandekod. Det går även att använda standard-avtalsklausuler som har godkänts av kommissionen. Den registrerade kan också lämna ett uttryckligt samtycke till en överföring av hans eller hennes personuppgifter. Det finns även vissa andra undantag.

Lagstöd: Artikel 44–50 i GDPR.

Överträdelser och sanktioner

Administrativa 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. 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. En sanktionsavgift tillfaller staten och ska betalas till Kammarkollegiet inom 30 dagar.

Skadeståndsansvar

Den registrerade har även rätt till skadestånd enligt dataskyddsförordningen. Den person-uppgiftsansvarige ska ersätta både ekonomisk och icke-ekonomisk skada som uppkommit på grund av överträdelsen. Om person-uppgifter 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 kränknings-ersättning vid överträdelse av den numera upphävda person-uppgiftslagen.

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 person-uppgiftsbiträde som medverkat vid behandlingen.

Den personuppgiftsansvarige eller ett person-uppgifts-biträde 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 personuppgifts-biträdet som ska visa att det inte finns något orsaks-samband mellan den rättsstridiga behandlingen och den uppkomna skadan.

Förbudsföreläggande m.m.

Förutom administrativa sanktionsavgifter har tillsynsmyndigheten även möjlighet att använda åtgärder vid överträdelse av dataskydds-regleringen såsom att utfärda en varning eller reprimand eller att förelägga den person-uppgiftsansvarige eller personuppgiftsbiträdet att vidta vissa åtgärder. Tillsynsmyndigheten får även genom föreläggande utfärda ett förbud mot eller begränsning av behandling av personuppgifter. Om en personuppgifts-ansvarige eller ett personuppgiftsbiträde inte rättar sig efter tillsynsmyndighetens före-läggande kan denna påföra en administrativ sanktionsavgift (se ovan om sanktionsavgifter). 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.

Dataskyddslivscykeln

EU:s dataskyddsförordning gäller under hela datalivscykeln. Datalivscykelhantering ("data life cycle management") är ett sätt att betrakta hur data flödar genom ett informationssystem. Datalivscykeln delas normalt in i ett antal steg som beskriver informationens livscykel från att denna samlas in eller skapas till att den gallras ut och förstörs.

Insamling

I det här avsnittet beskrivs krav som är särskilt relevanta i samband med insamling av personuppgifter.

Användningsfall: Insamling av personuppgifter kan bl.a. omfatta följande generella användningsfall

- Personuppgifter samlas in av den personuppgiftsansvarige direkt från den registrerade. Exempelvis genom att han eller hon fyller i en enkät eller deltar i en intervju.
- Personuppgifter samlas in av den personuppgiftsansvarige genom att observera den registrerades beteende. Exempelvis kamerabevakning, webbhistorik, pulsmätare eller andra sensorer.

Den personuppgiftsansvarige kan bl.a. också få tillgång till personuppgifter genom att dessa överförs från en annan personuppgiftsansvarig, nya uppgifter kan också skapas genom en analys av befintliga uppgifter. Dessa fall behandlas under avsnitten **utlämnande** och **bearbetning**.

Materiellt tillämpningsområde

EU:s dataskyddsförordning gäller inte anonym information, men även om personuppgifter anonymiseras innan de senare används är de normalt inte anonyma vid insamlingsögonblicket. Dataskyddsreglerna gäller fram till att uppgifterna anonymiserats eller raderats. Även om uppgifterna samlas in manuellt (t.ex. på pappersenkäter eller handskrivna anteckningar) så gäller dataskyddsreglerna om avsikter är att dessa uppgifter senare ska föras in i en databas eller på annat sätt behandlas på automatisk väg. Det räcker att handskrivna anteckningar renskrivs i en ordbehandlare.

Personuppgiftsansvar

När en organisation inte själv utför själva insamlingen är det nödvändigt att fastställa om den som anlitas för att samla in uppgifterna ska räknas som personuppgiftsbiträde eller anses vara gemensamt personuppgiftsansvarig. En organisation kan vara ansvarig även om den inte har tillgång till personuppgifterna eller endast tar emot anonym statistik baserad på dessa.

Specificering av ändamålet

Den personuppgiftsansvariga organisationen bör så tidigt som möjligt och allra senast när insamlingen av personuppgifter påbörjas specificera ändamålet med behandlingen. Behandlingens ändamål bör specificeras så precist att beskrivningen ger registrerade tillräcklig insyn i behandlingen samtidigt som det inte i onödan begränsar den personuppgiftsansvariga organisationens möjligheter att vidareutnyttja de insamlade personuppgifterna för andra berättigade ändamål. Den personuppgiftsansvariga organisationen bör dokumentera ändamålet med behandlingen. För att uppfylla principen om ansvarsskyldighet bör dokumentationen vara skriftlig. Personuppgiftsansvariga som är skyldiga att föra ett register över behandling av personuppgifter bör använda detta register för att dokumentera behandlingens ändamål.

Uppgiftsminimering

Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Detta gäller redan beträffande insamling av personuppgifter. Det är alltså inte tillåtet att samla in fler uppgifter än vad som är nödvändigt med hänsyn till det ändamål som den personuppgiftsansvarige har fastställt. Det finns dock inget hinder mot att uppgifter vid ett och samma tillfälle samlas in för mer än ett specifikt ändamål. Det är inte alltid möjligt att helt förhindra insamling av irrelevant information, men sådan måste gallras ut så snart det är möjligt enligt principen om lagringsminimering (se avsnittet **bevarande**).

Rättslig grund

Insamling av personuppgifter måste ske i enlighet med någon av de rättsliga grunder som föreskrivs i EU:s dataskyddsförordning. Vilken grund som är lämplig beror på ändamålet med behandlingen och andra omständigheter i det enskilda fallet. Om insamlingen sker genom en enkät eller intervju är det normalt möjligt och lämpligt att inhämta ett samtycke. När det inte är praktiskt möjligt eller olämpligt får en annan rättslig grund användas. Det avgörande för valet av rättslig grund är vad uppgifterna ska användas till efter att de samlats in. Om en butik använder kamerabevakning för att förhindra stölder kan behandlingen normalt grundas på intresseavvägningsregeln.

Öppenhet

Behandling av personuppgifter ska vara transparent i förhållande till den registrerade. När personuppgifter samlas in direkt från honom eller henne ska den personuppgiftsansvarige i princip alltid lämna följande information innan uppgifterna samlas in:

- Den personuppgiftsansvariges identitet och kontaktuppgifter och i förekommande fall för dennes företrädare.
- Kontaktuppgifter för dataskyddsombudet, om organisationen har ett sådant.
- Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.
- Om behandlingen är baserad på intresseavvägningsregeln, den personuppgiftsansvariges eller en tredje parts berättigade intressen.
- Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna.
- Om uppgifterna ska överföras till tredje land eller en internationell organisation, att så är fallet samt om överföringen omfattas av ett beslut om adekvat skyddsnivå och när så inte är fallet vilka lämpliga skyddsåtgärder som vidtagits.
- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
- Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.
- Om behandlingen grundar sig på samtycke, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
- Rätten att inge klagomål till en tillsynsmyndighet.
- Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.
- Förekomsten av automatiserat beslutsfattande, inklusive profilering, och meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

Undantag görs bara om den registrerade redan har fått den aktuella informationen. Det är alltså inte tillåtet att underlåta att lämna ovanstående information med motiveringen att det skulle innebära en oproportionerlig ansträngning. Åtminstone viss information måste lämnas innan ett eventuellt samtycke avges för att detta ska räknas som informerat. Övrig information måste åtminstone finnas tillgänglig, t.ex. genom en länk till en webbplats, så att den registrerade kan ta del av denna om han eller hon så önskar.

Konsekvensbedömning

Eftersom en eventuell konsekvensbedömning avseende dataskydd ska göras innan behandlingen påbörjas är det alltid nödvändigt att avgöra om en sådan krävs innan personuppgifter samlas in. Det som ska bedömas är om behandlingen sannolikt kan medföra en hög risk för registrerades fri- och rättigheter. Det är först efter att ha konstaterat att så inte är fallet som behandlingen kan påbörjas utan en formell konsekvensbedömning och ett eventuellt förhandssamråd med tillsynsmyndigheten.

Säkerhet

Det är värt att lägga märke till att samma krav på informationssäkerhet gäller redan vid insamlingen av personuppgifter. Det kan bl.a. innebära att känsliga uppgifter omedelbart måste krypteras.

Bearbetning

I det här avsnittet beskrivs krav som är särskilt relevanta i samband med insamling av personuppgifter.

Användningsfall: Bearbetning av personuppgifter kan innefatta ett stort antal användningsfall som innebär att personuppgifter används utan att behandlingen omfattas av något av de andra användningsfall som räknas upp under övriga steg i datalivscykeln. Exempelvis att en anställd hämtar uppgifter om en kund i ett Customer Relations Management-system. Användningen kan innebära att befintliga uppgifter sammanställs. Bearbetning kan också innebära att nya uppgifter skapas genom att de härleds från befintliga uppgifter. Användningsfallet omfattar emellertid inte att uppgifter överförs till eller från en annan personuppgiftsansvarig (se **utlämnande**).

Ändamålsbegränsning

Principen om ändamålsbegränsning innebär att personuppgifter inte får användas för ett ändamål som är oförenligt med det ändamål för vilket de ursprungligen samlades in. När personuppgifter används måste det alltid göras en bedömning av om denna är förenlig med det ändamål för vilket de samlades in. När behandlingen sker för arkivändamål av allmän intresse, forskningsändamål eller statistiska ändamål ska en sådan förenlig normalt presumeras förutsatt att lämpliga skyddsåtgärder har vidtagits. För andra ändamål måste en bedömning i stället göras enligt de kriterier som föreskrivs i artikel 6.4 i GDPR.

Uppgiftsminimering

Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Detta gäller vid all användning av personuppgifter. Exempelvis får en sökning i en databas för att sammanställa en lista med potentiella kunder inte omfatta fler uppgifter än vad som är nödvändigt.

Rättslig grund

Ett samtycke omfattar endast det eller de specifika ändamål som den registrerade fick information om i samband med att medgivandet lämnades. En löpande bedömning måste göras av om senare användning innebär att uppgifterna används för ett nytt ändamål. Om så är fallet krävs en kontroll av om det nya ändamålet har stöd i någon av de rättsliga grunder som föreskrivs i EU:s dataskyddsförordningen. Det kan annars krävas ett nytt samtycke för att behandlingen ska vara tillåten. Även om uppgifterna samlats in för ett annat ändamål kan det vara tillåtet att använda dem i marknadsföringssyfte, men det förutsätter exempelvis att åtgärden är förenlig med intresseavvägningsregeln.

Öppenhet

Behandling av personuppgifter ska vara transparent i förhållande till den registrerade. När personuppgifter behandlas för ett annat ändamål än det för vilket de ursprungligen samlades in måste den registrerade underrättas om detta innan den nya behandlingen påbörjas. Den registrerade ska få information om det nya ändamålet samt annan information som är relevant för att säkerställa en rättvis och öppen behandling. Det är värt att lägga märke till att denna informationsskyldighet gäller oberoende av om det krävs ett nytt samtycke. Det finns dock vissa situationer när det inte är nödvändigt att informera den registrerade om att hans eller hennes personuppgifter kommer att behandlas för ett nytt ändamål, nämligen i de fall när sådan information inte behövde lämnas i samband med att uppgifterna ursprungligen togs emot av den personuppgiftsansvarige (se artikel 13.4 och 14.5 i GDPR).

Konsekvensbedömning

Eftersom en eventuell konsekvensbedömning avseende dataskydd ska göras innan behandlingen påbörjas är det alltid nödvändigt att avgöra om en sådan krävs innan personuppgifter börjar behandlas för ett nytt ändamål. Det som ska bedömas är om den nya behandlingen sannolikt kan medföra en hög risk för registrerades fri- och rättigheter. Det är först efter att ha konstaterat att så inte är fallet som behandlingen kan påbörjas utan en formell konsekvensbedömning och ett eventuellt förhandssamråd med tillsynsmyndigheten.

Säkerhet

EU:s dataskyddsförordning kräver inte bara att personuppgifter och de system som används för behandlingen skyddas mot externa dataintrång eller dataläckor. Den personuppgiftsansvarige måste också vidta åtgärder för att säkerställa att anställda och andra som behandlar personuppgifter under dennes överinseende endast behandlar dessa på instruktion från den personuppgiftsansvarige. Det kan exempelvis behövas behörighetskontroll så att endast den som har behov av det kan få tillgång till uppgifterna. Det senare gäller särskilt vid behandling av känsliga personuppgifter, såsom uppgifter om hälsa.

Utlämnande

I det här avsnittet beskrivs krav som är särskilt relevanta i samband med utlämnade av personuppgifter.

Användningsfall: Utlämnande kan innefatta all behandling som innebär att personuppgifter görs tillgängliga för tredje part genom överföring, spridning eller tillhandahålls på annat sätt. Exempelvis att uppgifterna publiceras på en webbplats eller görs tillgängliga genom en webbtjänst. Användningsfallet innefattar däremot inte situationer när uppgifterna görs tillgängliga för anställda och andra som står under den personuppgiftsansvariges ansvar. Det senare inkluderar när ett personuppgiftsbiträde får tillgång till personuppgifter som ska behandlas på uppdrag av den personuppgiftsansvarige.

Ändamålsbegränsning

Principen om ändamålsbegränsning innebär att personuppgifter inte får användas för ett ändamål som är oförenligt med det ändamål för vilket de ursprungligen samlades in. Om uppgifterna samlades inför att publiceras på en webbplats räknas offentliggörandet inte som ett nytt ändamål, men ett utlämnande kan också i syfte att uppgifterna ska vidareutnyttjas. Uppgifter som samlats in för att upprätta ett medlemsregister i en förening kan komma att lämnas ut till tredje part som har för avsikt att använda dessa för direkt marknadsföring. Om ett sådant vidareutnyttjande strider mot principen om ändamålsbegränsning (se ovan avsnitt om **bearbetning**) torde redan ett utlämnande för detta syfte vara otillåtet. Rättsläget är dock inte helt klart. Exempelvis kan den som publicerar personuppgifter på en öppen webbplats inte gärna på förhand kontrollera alla sätt på vilka dessa kan komma att vidareutnyttjas.

Rättslig grund

Eftersom utlämnande räknas som behandling ska även ett utlämnande ske med den registrerades samtycke eller en annan rättslig grund. Ett utlämnande kan utgöra en separat behandling eller ett osjälvständigt led i en behandlingskedja. I det senare fallet kan utlämnandet normalt ske med stöd av samma rättsliga grund som övriga led i denna kedja. När utlämnandet sker för ett annat ändamål kan det dock krävas ett nytt samtycke eller annan rättslig grund. Exempelvis kan personuppgifter som ursprungligen samlats in för internt bruk göras tillgängliga som öppna data endast under förutsättning att offentliggörandet t.ex. kan grundas på intresseavvägningsregeln. Detsamma gäller vid försäljning av data för vidareutnyttjande, t.ex. försäljning av e-postadresser för direkt marknadsföring.

Öppenhet

Den lämnar ut uppgifter till tredje part har ingen skyldighet att informera den registrerade om det enskilda utlämnandet, endast vilka som de insamlade uppgifterna i framtiden kan komma att lämnas ut till. Informationsskyldigheten för de utlämnade uppgifterna åvilar i stället den som mottagit dessa. Den som mottar uppgifter från en annan källa än den registrerade ska lämna samma information till den registrerade som när personuppgifterna samlas in direkt från honom eller henne (se ovan avsnitt om **insamling**) samt följande ytterligare upplysningar:

- De kategorier av personuppgifter som behandlingen gäller.
- Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor.

Undantag för göras för sådan information som den registrerade redan förfogar över, men det finns också ett antal andra undantag som inte gäller när uppgifterna samlas in direkt från den registrerade. Information behöver bl.a. inte lämnas om det är omöjligt eller skulle medföra en oproportionerlig ansträngning. När det rör sig om ett stort antal registrerade och kontaktuppgifter saknas kan undantaget normalt tillämpas. Det senare torde dock inte vara fallet om mottagaren har tillgång till den registrerades e-postadress. Informationen ska normalt lämnas inom rimlig tid efter att uppgifterna har mottagits, men denna tidpunkt kan skjutas upp i vissa särskilda situationer som räkans upp i dataskyddsförordningen.

Överföring till tredje land

Ett utlämnande kan innebära att personuppgifter överförs till tredje land. En sådan överföring är endast tillåten när denna sker i enlighet med kapitel V i EU:s dataskyddsförordning. Att publicera personuppgifter på en webbplats räknas dock enligt EU-domstolens rättspraxis inte sig som en överföring till tredje land.

Konsekvensbedömning

När utlämnande av uppgifter medför att dessa behandlas för ett nytt ändamål bör en ny bedömning göras av om detta kan innebära nya risker som kräver en konsekvensbedömning avseende dataskydd och ett eventuellt förhandssamråd med tillsynsmyndigheten. En sådan bedömning bör normalt ske innan personuppgifter görs tillgängliga för vidareutnyttjande som öppna data.

Säkerhet

När personuppgifter överförs gäller samma krav på informationssäkerhet som vid annan behandling av personuppgifter. Den personuppgiftsansvarige måste säkerställa att ingen obehörig får tillgång till uppgifterna, vilket kan kräva att överföringen sker krypterat. Det är t.ex. inte tillåtet att skicka sjukjournaler med e-post som inte är krypterad.

Bevarande

I det här avsnittet beskrivs krav som är särskilt relevanta i samband med bevarande av personuppgifter.

Användningsfall: Bevarande omfattar alla former av lagring av personuppgifter, vilket inkluderar arkivering av uppgifterna.

Rättslig grund

Lagring av personuppgifter utgör en form av behandling, men så länge lagringen inte sker för ett nytt syfte krävs ingen separat rättslig grund. När bevarandet sker för arkivändamål av allmänt intresse presumeras dessutom normalt att användningen är förenlig med principen om ändamålsbegränsning.

Öppenhet

Det är först om bevarandet utgör ett nytt ändamål som den personuppgiftsansvarige är skyldig att lämna information om behandlingen till den registrerade. Detta sammanfaller normalt med att uppgifterna överförs till en arkivmyndighet eller motsvarande organisation.

Lagringsminimering

Personuppgifter får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till det ändamål för vilket de behandlas. Uppgifterna ska härefter raderas eller anonymiseras. Undantag görs när uppgifterna behöver bevaras för arkivändamål av allmänt intresse, forskningsändamål och statistiska ändamål förutsatt att lämpliga skyddsåtgärder vidtas.

Radering

I det här avsnittet beskrivs krav som är särskilt relevanta i samband med radering av personuppgifter.

Användningsfall: Radering innefattar alla former av utplåning av personuppgifter, men även att dessa anonymiseras.

Radering av personuppgifter utgör en form av behandling, men får normalt betraktas som ett osjälvständigt led i en behandlingskedja. Det krävs därför ingen separat rättslig grund. Personuppgifter kan normalt alltid raderas eller anonymiseras utan den registrerades samtycke. Den är heller inte nödvändigt att informera den registrerade om att dennes personuppgifter raderats. Genom raderingen eller anonymiseringen upphör uppgifterna att omfattas av personuppgiftslagen. Det finns ingen skyldighet att bevara personuppgifter när de ändamål för vilka dessa behandlas av den personuppgiftsansvarige inte längre kräver det. Undantag görs när den registrerade motsatt sig radering och i stället krävt att deras användning ska begränsas. En oavsiktlig förstöring eller förlust av uppgifterna ska dessutom räknas som en personuppgiftsincident.

Noter

[1] Artikel 12 i Förenta nationernas allmänna förklaring om de mänskliga rättigheterna (”The Universal Declaration of Human Rights”), även känd som FN:s deklaration om de mänskliga rättigheterna.

[2] Artikel 17 i Förenta nationernas internationella konvention om medborgerliga och politiska rättigheter (”The International Covenant on Civil and Political Rights”).

[3] Artikel 8 i Europarådets konvention om de mänskliga rättigheterna och de grundläggande friheterna.

[4] 2 kap. 6 och 19 §§ regeringsformen. Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

[5] Artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna.

[6] Artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna.

[7] Artikel 51 i Europeiska unionens stadga om de grundläggande rättigheterna.

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

[9] Artikel 52.1 i Europeiska unionens stadga om grundläggande rättigheter.

[10] Det går dock inte att förutsätta att den avvägning som lagstiftaren gjort alltid har blivit rätt. EU-domstolen har exempelvis funnit att EU:s dataskyddsdirektiv stred mot stadgan och ogiltigförklarade detta. Se EU-domstolens dom (stora avdelningen) av den 8 april 2014 i förenade målen C-293/12 och C-594/12 Digital Rights Ireland och Seitlinger m.fl. (ECLI:EU:C:2014:238).

[11] Europeiska kommissionen, Special Eurobarometer 431, ”Data protection”, juni 2015.

[12] Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen, EUT L 303, 28.11.2018, s. 59–68.

[13] 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.

[14] 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, EUT L 281, 23.11.1995, s. 31–50.

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

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

[17] 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, p. 89–131.

[18] Brottsdatalag (2018:1177).

[19] 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), EUT L 201, 31.7.2002, p. 37–47.

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

[21] Marknadsföringslag (2008:486).

[22] Förslag till Europaparlamentets 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/2017/010 slutlig.

[23] 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.

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

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

[26] Lag (2019:497) om ändring i lagen (2003:389) om elektronisk kommunikation. Datalagring – brottsbekämpning och integritet (SOU 2017:75) och regeringens proposition Datalagring vid brottsbekämpning – anpassningar till EU-rätten (Prop. 2018/19:86).

[27] 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.

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

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

SÖDERTÖRN UNIVERSITY | STOCKHOLM LUND UNIVERSITY Urban ICT Arena SANDVINE SEB