Vägledning om dataskydd

God integritet vid digital tjänste- och affärsutveckling

Del 1: Inledning

Om författaren

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

Förord

Detta är första delen av en vägledning som är framtagen inom ramen för projektet ”Sjyst data!”. I denna ges en översikt till EU:s nya dataskyddsförordning (GDPR). I andra delen behandlas ett antal praktikfall som beskriver hur förordningens krav kan implementeras ur ett ”data life cycle management”-perspektiv. Fler delar och revideringar kommer att publiceras löpande på projektets webbplats.

Projektet ”Sjyst data!” syftar till att främja digital tjänste- och affärsutveckling med vad vi betecknar som god integritet. Fram till den 25 maj 2018 när företag ska ha anpassat sin verksamhet till de krav som föreskrivs i GDPR kommer mycket fokus att ligga på regelefterlevnad, men företag som betraktar integritet ur detta snäva perspektiv riskerar att gå miste om affärsmöjligheter. God integritet handlar om att skapa tillit så att slutanvändare kan känna sig trygga med att dela med sig av den data som är nödvändig för att bygga de innovativa tjänster som behövs i en digital ekonomi och ett hållbart samhälle.

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, Sandvine AB, Skandinaviska Enskilda Banken AB, TS Mediefakta AB, Urban ICT Arena och Öresundskraft AB. Projektet finansieras med 10 miljoner kronor av Vinnova inom programmet Utmaningsdriven innovation som är en satsning för att lösa samhällsutmaningar som kräver bred samverkan.

Håkan Cavenius, projektledare

Stockholm den 8 mars 2018

Europeiska unionens dataskyddsrätt

Europeiska unionens allmänna dataskyddsförordning (GDPR), som blir tillämplig i Sverige och alla andra EU-medlemsstater den 25 maj 2018, innehåller nya enhetliga regler om skydd för enskildas personuppgifter. Förordningen ersätter 1995 års dataskyddsdirektiv och den svenska personuppgiftslagen. För att säkerställa en enhetlig tillämpning av unionens dataskyddsregler inrättas ett unionsorgan som kallas Europeiska dataskyddsstyrelsen.

Europeiska unionens dataskyddsreform

I januari 2012 lade Europeiska kommissionen fram sitt förslag till dataskyddsreform[1]. Syftet med reformen, som utgör ett led i unionens strategi för en digital inre marknad, var att anpassa unionens regler om dataskydd till den digitala utvecklingen. Data, särskilt personuppgifter, utgör en värdefull resurs i den digitala ekonomin. Samtidigt känner en stor andel av EU-medborgarna en allt större oro över att lämna ut sina personuppgifter på internet[2]. De nuvarande reglerna präglas dessutom av en fragmentering som gör att det är svårt för företag att veta vilka regler som gäller i olika medlemsstater.

Syftet med EU:s dataskyddsregler är att skydda enskilda individers grundläggande fri- och rättigheter, särskilt rätt till skydd för personuppgifter, men även att säkerställa ett fritt flöde av personuppgifter inom unionen. Dessa målsättningar ska uppnås genom en enhetlig och hög nivå av skydd för enskildas personuppgifter som säkerställs genom stränga sanktioner. Målet med dataskyddsreformen är att stärka konsumenters förtroende för hantering av personuppgifter samt göra det enklare och billigare för företag att tillhandahålla gränsöverskridande digitala tjänster.

Europeiska unionens allmänna dataskyddsförordning (GDPR)

Europeiska unionens allmänna dataskyddsförordning (GDPR)[3], som antogs i april 2016, ersätter 1995 års dataskyddsdirektiv[4], som i svensk rätt har genomförts genom personuppgiftslagen (PUL)[5]. Eftersom en EU-förordning i motsats till ett direktiv inte ska genomföras i nationell rätt, utan blir direkt tillämplig i alla medlemsstater, kommer dataskyddsförordningen att ersätta nationell lagstiftning om skydd för personuppgifter[6]. Förordningen lämnar dock ett visst utrymme för och delvis förutsätter kompletterande nationella regler. I februari 2016 gav regeringen därför dataskyddsutredningen i uppdrag att utreda nya nationella regler som på ett generellt plan kompletterar EU:s dataskyddsförordning.[7]

I betänkandet ”Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning” föreslår utredningen att sådana kompletterande nationella bestämmelser införs genom en ny övergripande lag och förordning (i utredningen kallad ”dataskyddslagen”).[8] En ny dataskyddslag som i huvudsak överensstämmer med betänkandet har i februari 2018 föreslagits i regeringens proposition ”Ny dataskyddslag”.[9]

För att säkerställa en korrekt och enhetlig tillämpning av dataskyddsförordningen inrättas genom denna ett unionsorgan som kallas Europeiska dataskyddsstyrelsen (tidigare ”Artikel 29-gruppen”).[10] Styrelsen ska bestå av cheferna för medlemsstaternas tillsynsmyndigheter och den Europeiska datatillsynsmannen. Dess uppgift är bl.a. att utfärda riktlinjer, rekommendationer och bästa praxis. Styrelsens riktlinjer är icke bindande, men kan vara vägledande vid tolkning och tillämpning av dataskyddsförordningen.[11]

Svensk tillsynsmyndighet är Datainspektionen, som under 2018 föreslås få ett breddat uppdrag och byta namn till Integritetsskyddsmyndigheten.[12]

www.datainspektionen.se

Dataskyddsförordningens tillämpningsområde

Dataskyddsförordningen gäller vid behandling av personuppgifter som pågår eller påbörjats efter att förordningen blir tillämplig den 25 maj 2018. Förordningen gäller som huvudregel för personer eller organisationer som antingen är etablerade i Europeiska unionen (EU) eller Europeiska ekonomiska samarbetsområdet (EES). Den gäller dock även för företag som är etablerade utanför unionen när dessa riktar erbjudanden till personer som befinner sig i unionen eller övervakar deras beteende. Det saknar också betydelse var behandlingen utförs.

Vad räknas som personuppgifter?

Med ”personuppgifter” avses varje uppgift som direkt eller indirekt kan identifiera en nu levande människa (”fysisk person” med juridisk terminologi).[13] Ett personnummer är en personuppgift eftersom det är en unik identifierare som direkt kan hänföras till en individ. Eftersom det räcker att en uppgift tillsammans med andra uppgifter indirekt kan identifiera en individ kan nästan vad som helst vara en personuppgift.

Exempel

För att en maskin som ansluts till internet ska kunna identifieras får den ett unikt nummer – ett IP-nummer. Ett IP-nummer i sig själv är inte en personuppgift eftersom det inte är direkt kopplat till en människa. Många IP-nummer räknas trots det som personuppgifter eftersom de indirekt kan kopplas till en människa genom att kombinera detta med andra uppgifter, t.ex. genom ett internetabonnemang eller uppgift om vem som äger en apparat.

En anonym uppgift är däremot inte en personuppgift. För att uppgifter ska räknas som anonyma krävs att det inte går att identifiera någon individ ens om dessa kombineras med andra uppgifter. Det är alltså – som är vanligt inom forskning och statistik – inte tillräckligt att endast pseudonymisera uppgifter. Om det finns en risk att en uppgift eller samling av uppgifter kan användas för att identifiera en nu levande människa ska dessa räknas som en personuppgift i förordningens mening.

Förordningen omfattar däremot inte uppgifter som rör juridiska personer (t.ex. bolag, föreningar, stiftelser, stat eller kommun) samt ofödda eller avlidna människor. Däremot saknar den registrerades nationalitet eller bosättningsort betydelse.[14]

Vad räknas som känsliga personuppgifter?

Dataskyddsförordningen är tillämplig på alla personuppgifter, men för personuppgifter som är särskilt känsliga till sin natur gäller strängare krav än för personuppgifter i allmänhet. Med känsliga personuppgifter avses ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Vad räknas som behandling av personuppgifter?

Med ”behandling av personuppgifter” avses i princip alla åtgärder som vidtas med en ”personuppgift” (se ovan)[15]. Förordningens bestämmelser gäller bl.a. när personuppgifter samlas in, bearbetas, lagras, sprids, ändras eller raderas. Det är här värt att påpeka att det alltså inte krävs någon aktiv handling, det är tillräckligt att en personuppgift bevaras efter att den har samlats in. En personuppgift som finns på ett USB-minne i en skrivbordslåda omfattas av dataskyddsförordningen. Även ren lagring av personuppgifter ska alltså uppfylla alla krav enligt denna. Det måste dock röra sig om påbörjad behandling. Förordningen gäller däremot inte för planering av behandling av personuppgifter. Det är dock värt att här lägga märke till att även inventering av befintliga personuppgifter räknas som behandling av personuppgifter. [16]

När börjar dataskyddsförordningen gälla i Sverige?

Dataskyddsförordningen, som trädde i kraft den 24 maj 2016, blir tillämplig i Sverige och alla andra EU-medlemsstater den 25 maj 2018. Företag, myndigheter och andra organisationer som omfattas av dataskyddsförordningen har alltså två år på sig att uppfylla de nya krav som föreskrivs i förordningen. Det finns inga övergångsbestämmelser. Förordningen är tillämplig på all behandling av personuppgifter som fortfarande pågår eller påbörjas den 25 maj 2018. Den är däremot inte tillämplig på behandling av personuppgifter som avslutats innan detta datum. Om den personuppgiftsansvarige raderat eller avidentifierat personuppgifter innan den 25 maj 2018, omfattas dessa alltså inte av förordningen. Det är dock värt att lägga märke till att sådan behandling kan omfattas av de tidigare bestämmelserna i personuppgiftslagen. Om uppgifterna fortfarande kan användas för att identifiera någon efter den 25 maj 2018 räknas behandlingen inte som avslutad.

Var gäller dataskyddsförordningen?

Dataskyddsförordningen gäller för företag, myndigheter och andra organisationer som är etablerade i något av Europeiska unionens medlemsstater eller i en stat som är medlem i Europeiska ekonomiska samarbetsområdet (EES).[17] Förutom EU:s 28 medlemsstater gäller förordningen alltså även Island, Norge och Lichtenstein.[18] Schweiz är medlem i EFTA, men inte EES och räknas därför som tredje land.

Ett företag i tredje land (t.ex. Schweiz, USA eller Kina) som riktar erbjudanden om varor eller tjänster till personer som befinner sig i unionen eller som övervakar deras beteende i unionen ska också följa EU:s dataskyddsregler.[19] Om en person eller organisation omfattas av förordningen spelar det heller ingen roll var behandlingen utförs.[20] Om ett svenskt företag eller en svensk myndighet anlitar ett företag i tredje land för att t.ex. utföra dess löneutbetalningar omfattas denna behandling av de anställdas personuppgifter fortfarande av dataskyddsförordningen.

När är det tillåtet att överföra personuppgifter till tredje land?

Ett av dataskyddsförordningens syften är att säkerställa en fri rörlighet av personuppgifter inom unionen. Det är däremot som huvudregel förbjudet att överföra personuppgifter till ett land utanför unionen eller EES. För att det ska vara tillåtet att överföra personuppgifter till tredje land krävs som huvudregel att det finns ett beslut om adekvat skyddsnivå.[21]

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").[22] 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.[23]

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").[24] Bestämmelserna ska godkännas av behörig tillsynsmyndighet och fungerar som en intern uppförandekod. Det går även att använda standardavtalsklausuler som har godkänts av kommissionen.[25] Den registrerade kan också lämna ett uttryckligt samtycke till en överföring av hans eller hennes personuppgifter.[26] Det finns även vissa andra undantag.[27]

Ansvar för personuppgifter

Det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för behandling av personuppgifter som utförs under dennes överinseende eller för dennes räkning. Den personuppgiftsansvarige är bl.a. skyldig att vidta tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd av personuppgifter. Den personuppgiftsansvarige är också skyldig att visa att denne uppfyller alla de grundläggande krav på behandling av personuppgifter som ställs upp i förordningen. Även den som endast utför behandling av personuppgifter för någon annans räkning (personuppgiftsbiträde) har vissa egna skyldigheter enligt dataskyddsförordningen. Om den personuppgiftsansvarige anlitar ett sådant biträde ska dessa teckna ett särskilt personuppgiftsbiträdesavtal.

Vad menas med principen om ansvarsskyldighet?

Principen om ansvarsskyldighet (”accountability”) innebär att det är den personuppgiftsansvarige som har det huvudsakliga ansvaret för att all behandling av personuppgifter som utförs under dennes överinseende eller för dennes räkning uppfyller alla grundläggande krav som ställs upp i dataskyddsförordningen. Det är också den personuppgiftsansvariges skyldighet att visa att denne uppfyller dessa krav. Principen om ansvarsskyldighet innebär alltså en omvänd bevisbörda. Den personuppgiftsansvarige ska kunna bevisa att denne efterlever alla krav som föreskrivs i förordningen.[28]

I praktiken innebär det att den personuppgiftsansvarige behöver säkra bevisning genom att dokumentera alla beslut och åtgärder som vidtagits för att efterleva dataskyddsförordningen. Det räcker alltså inte att den personuppgiftsansvarige gjort korrekta bedömningar eller vidtagit tekniska och organisatoriska åtgärder. Dessa måste också dokumenteras på ett sådant sätt att det i efterhand går att visa att den personuppgiftsansvarige uppfyller alla de krav som ställs upp i förordningen. Principen om ansvarsskyldighet innebär alltså att den personuppgiftsansvariges bedömningar och åtgärder avseende dataskydd i praktiken måste vara reviderbara. Brister i dokumentationen kan göra att den personuppgiftsansvarige inte kan bevisa att denne efterlever förordningen och därmed drabbas av sanktioner.

Vem är personuppgiftsansvarig?

Den personuppgiftsansvarige är den organisation som bestämmer ändamålen och medlen för behandling av personuppgifter. Det är denna organisation som har det huvudsakliga ansvaret för behandling av personuppgifter[29] som utförs under dennas överinseende eller för dennas räkning. Den personuppgiftsansvarige är normalt ett företag, en myndighet eller någon annan organisation. Den personuppgiftsansvarige måste dock inte vara en egen juridisk person. En person som driver näringsverksamhet i form av en enskild firma eller ett enkelt bolag kan också vara personuppgiftsansvarig.

Vem räknas som personuppgiftsbiträde?

Ett företag, en myndighet eller annan organisation som endast behandlar personuppgifter för någon annans räkning, utan att bestämma ändamålen eller medlen för behandlingen är ett personuppgiftsbiträde. [30] Det avgörande för om någon ska räknas som ett biträde är graden av självständighet. Ett biträde behandlar osjälvständigt personuppgifter för den personuppgiftsansvariges räkning. Om ett biträde bestämmer ändamålen eller medlen för behandlingen tillsammans med uppdragsgivaren räknas de i stället som gemensamt personuppgiftsansvariga, medan en leverantör som helt på egen hand bestämmer ändamålen och medlen för behandlingen räknas som en fristående personuppgiftsansvarig.[31] Alla leverantörer räknas alltså inte som personuppgiftsbiträden.

Vem ansvarar för anställdas behandling av personuppgifter?

Den personuppgiftsansvarige ansvarar för alla som behandlar personuppgifter under dennes överinseende. Det är alltså normalt arbetsgivaren som ansvarar för sina anställdas behandling av personuppgifter. Den som är anställd får endast utföra behandling av personuppgifter som denne får tillgång till enligt arbetsgivarens instruktioner.[32] Det är arbetsgivarens ansvar att se till att det finns lämpliga tekniska och organisatoriska skyddsåtgärder som hindrar att anställda får obehörig tillgång till personuppgifter.[33]

Vem ansvarar för leverantörers behandling av personuppgifter?

Den personuppgiftsansvarige ansvarar normalt även för behandling av personuppgifter som utförs för dennes räkning av ett personuppgiftsbiträde. Den personuppgiftsansvarige får endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.[34] Ett huvudbiträde ansvarar dessutom för underbiträden som denna i sin tur anlitar. Ett huvudbiträde får heller inte anlita ett underbiträde utan att detta i förväg godkänts skriftligen av den personuppgiftsansvarige. Den som är personuppgiftsansvarig ansvarar emellertid inte för behandling som utförs av en annan fristående personuppgiftsansvarig. Alla leverantörer räknas alltså inte som personuppgiftsbiträde (se ovan om vem som räknas som personuppgiftsbiträde).

När behövs ett personuppgiftsbiträdesavtal?

Om den personuppgiftsansvarige anlitar ett personuppgiftsbiträde (se ovan om vem som räknas som personuppgiftsbiträde) ska det alltid finnas ett personuppgiftsbiträdesavtal. Vilka villkor som ska finnas i ett sådant avtal regleras i dataskyddsförordningen.[35] Ett sådant avtal ska vara skriftligt. Ett avtal krävs också när ett huvudbiträde anlitar ett underbiträde.[36]

Vad händer vid en överträdelse av dataskyddsförordningen?

Sanktionsavgifter

Den som överträder dataskyddsförordningens bestämmelser kan drabbas av stränga sanktioner. Om ett företag överträder förordningen kan tillsynsmyndigheten besluta om en sanktionsavgift som uppgår till 20 miljoner euro eller 4 % av företagets totala globala årsomsättning.[37] För vissa överträdelser är den högsta sanktionsavgiften i stället 10 miljoner euro eller 2 % av företagets totala globala årsomsättning.[38]

Förordningen ger en medlemsstat möjlighet att själv bestämma i vilken utsträckning dessa sanktionsavgifter även ska gälla för myndigheter eller andra offentliga organ.[39] Regeringen har förslagit att svenska myndigheter endast ska betala en sanktionsavgift som uppgår till 10 miljoner kronor eller 5 miljoner kronor i mindre allvarliga fall. [40]

Skadeståndsansvar

Den registrerade har även rätt till skadestånd enligt dataskyddsförordningen.[41] Den personuppgiftsansvarige ska ersätta både ekonomisk och icke-ekonomisk skada som uppkommit på grund av överträdelsen. Den personuppgiftsansvarige kan endast undgå ansvar genom att visa att denne inte på något sätt är ansvarig för den händelse som orsakade skadan. Den personuppgiftsansvarige förutsätts alltså ha orsakat skadan (presumtionsansvar) och det krävs inte att skadan orsakats genom dennes oaktsamhet (strikt ansvar). Om mer än en personuppgiftsansvarig har orsakat skadan ansvarar de solidariskt för hela skadan. Samma regler gäller om skadan orsakats av ett personuppgiftsbiträde.

Andra sanktioner

Dataskyddsförordningen tillåter även att medlemsstaterna inför andra sanktioner.[42] Regeringen har dock föreslagit att straffrättsliga sanktioner (böter och fängelse) samt möjlighet för tillsynsmyndigheten att använda vitesföreläggande inte bör införas i svensk rätt. [43]

Krav vid behandling av personuppgifter

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

Vilka grundläggande krav ställs på behandling av personuppgifter?

All behandling av personuppgifter ska uppfylla ett antal grundläggande krav (principer).[44] 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.

Korrekthet: Personuppgifter ska vara korrekta 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.[45]

När krävs samtycke för behandling av personuppgifter?

Den registrerades samtycke krävs alltid vid behandling av hans eller hennes personuppgifter, om den personuppgiftsansvarige inte kan stödja sig på en annan rättslig grund.[46] Om samtycke saknas kan behandlingen i stället bl.a. grundas på den s.k. ”intresseavvägningsregeln”.[47] Regeln innebär att det kan vara tillåtet att behandla någons personuppgifter om det är nödvändigt för att uppnå ett ändamål som rör den personuppgiftsansvarige eller tredje parts berättigade intressen. Detta förutsätter dock att skyddet av den registrerades intressen eller grundläggande fri- och rättigheter inte väger tyngre.

En nyhet i dataskyddsförordningen är att myndigheter inte kan stödja sig på denna intresseavvägningsregel när de fullgör sina uppgifter.[48] 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.[49] För att utföra behandling som är nödvändig för att fullgöra sådana uppgifter krävs alltså normalt inget samtycke från den registrerade. Det är heller inte säkert att ett sådant samtycke hade varit giltigt eftersom det är tveksamt om det uppfyller det nya striktare kravet på frivillighet (se nedan om vad som krävs för giltigt samtycke). [50]

Det finns även andra rättsliga grunder för behandling av personuppgifter i förordningen och i nationell lagstiftning. För känsliga personuppgifter (t.ex. uppgifter om hälsa) gäller andra striktare krav för att behandlingen ska vara laglig.

Vad räknas som giltigt samtycke till behandling av personuppgifter?

Ett samtycke ska vara frivilligt, specifikt, informerat och otvetydigt.[51] Det är den personuppgiftsansvarige som ska bevisa att alla dessa krav är uppfyllda. 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. Ett tyst samtycke räknas inte.

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.[52] För samtycke till behandling av känsliga personuppgifter krävs dessutom att samtycket är uttryckligt.[53]

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

I svensk rätt gäller som huvudregel att den som är omyndig (under 18 år) inte kan ingå avtal eller företa andra rättshandlingar utan vårdnadshavares samtycke. I dataskyddsförordningen anges att detsamma gäller för ett barns samtycke till behandling av hans eller hennes personuppgifter på internet.[54] Vem som räknas som barn ska dock fastställas i nationell rätt. Regeringen har föreslagit att den som är under 13 år ska räknas som barn i Sverige enligt dataskyddsförordningen.[55] Om förslaget blir lag kan alltså den som är minst 13 år själv samtycka till behandling av sina personuppgifter på internet.

Vilka rättigheter har den registrerade?

Dataskyddsförordningen innebär en viss förstärkning av de rättigheter som den registrerade redan hade enligt dataskyddsdirektivet och personuppgiftslagen. Syftet med dessa rättigheter är att ge den registrerade ökad insyn i och kontroll över behandlingen av hans eller hennes personuppgifter. Förordningen ger därför den registrerade följande rättigheter mot den personuppgiftsansvarige (se rutan till höger).[56]

Rätt till information: Den personuppgiftsansvarige är skyldig att lämna viss obligatorisk information när personuppgifter samlas in från den registrerade, men även när information erhålls från en annan källa. Informationen ska lämnas på den personuppgiftsansvariges eget initiativ samt vara klar och tydlig.

Rätt till tillgång: Den registrerade har på begäran rätt att få en bekräftelse på om personuppgifter som rör honom eller henne behandlas och i så fall även rätt att få viss obligatorisk information om behandlingen samt utan kostnad en kopia av sina personuppgifter.

Rätt till rättelse: Den registrerade har rätt att få felaktiga personuppgifter rättade samt få ofullständiga personuppgifter kompletterade.

Rätt till radering ("rätten att bli bortglömd"): Den registrerade har rätt att få sina personuppgifter raderade förutsatt att vissa villkor är uppfyllda. Vid rättelse och radering måste även mottagare av uppgifterna underrättas.
Rätt till begränsning av behandling: Den registrerade har rätt att kräva att behandlingen begränsas om vissa villkor är uppfyllda. Sådana uppgifter ska markeras och åtgärden innebär att dessa endast får behandlas med samtycke eller för vissa särskilda ändamål. Begränsning av behandling används normalt provisoriskt som alternativ till rättelse eller radering.
Rätt till dataportabilitet: Den registrerade har rätt att få sina personuppgifter överförda till en annan personuppgiftsansvarig i ett strukturerat, allmänt använt och maskinläsbart format. Rätten omfattar endast uppgifter som den registrerade har tillhandahållit och när behandlingen grundar sig på samtycke eller avtal samt sker på automatisk väg. Rätt till portabilitet gäller heller inte myndighets verksamhet.

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

Personuppgiftsansvarigs skyldigheter

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

När måste den personuppgiftsansvarige utse ett dataskyddsombud?

En myndighet måste alltid utse ett dataskyddsombud.[57] Flera myndigheter kan dela på ett och samma ombud under förutsättning att ombudet ändå kan utföra sina uppgifter. Andra organisationer ska utse ett ombud om dess kärnverksamhet antingen består av regelbunden och systematisk övervakning i stor omfattning eller behandling av känsliga personuppgifter i stor omfattning.[58] Dataskyddsombudets kontaktuppgifter ska offentliggöras (t.ex. på organisationens webbplats) samt meddelas till behörig tillsynsmyndighet.

> En anmälan av dataskyddsombud kan tidigast göras hos den behöriga tillsynsmyndigheten den 25 maj 2018.

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.[59]

> Artikel 29-gruppen har utfärdat riktlinjer om dataskyddsombud (WP 243).

Tekniska och organisatoriska åtgärder

För att efterleva dataskyddsförordningen måste den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder.[60]

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

Inbyggt dataskydd och dataskydd som standard

Dataskyddsförordningen kräver att vissa skyddsåtgärder integreras i de system som används för behandling av personuppgifter (”inbyggt dataskydd”).[61] Ett exempel på sådana skyddsåtgärder som nämns i förordningen är pseudonymisering. Förordningen ställer också krav på åtgärder som innebär att behandling i standardfallet endast sker i den omfattning som är nödvändigt för varje ändamål med behandlingen (”dataskydd som standard”).[62] Dessa bestämmelser har sin grund i ”privacy by design”, en designprincip som innebär att integritetskrav ska beaktas redan under utvecklingen av ett IT-system.[63] Det är dock fortfarande oklart vad som närmare avses med kravet på ”inbyggt dataskydd” och ”dataskydd som standard” i dataskyddsförordningens mening. Kravets närmare innebörd behöver klargöras och preciseras genom riktlinjer, tekniska standarder eller godkända uppförandekoder.

Register över behandling av personuppgifter

Dataskyddsförordningen kräver att den personuppgiftsansvarige för ett register över behandling av personuppgifter som utförs under dennes ansvar.[64] Vad som ska antecknas i ett sådant register specificeras i förordningen. Det ska bl.a. innehålla en beskrivning av kategorier av registrerade och kategorier av personuppgifter. Det rör sig däremot inte om en löpande förteckning över varje enskild behandlingsåtgärd eller varje enskild registrerad eller dennes personuppgifter. En organisation som har under 250 anställda kan dock vara undantagen från detta krav på att föra ett register över behandling.

Konsekvensbedömningar avseende dataskydd och förhandssamråd

Om en viss typ av behandling sannolikt leder till en hög risk för enskildas fri- och rättigheter ska den personuppgiftsansvarige utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.[65] 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).[66]

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

Säkerhet för personuppgifter

Dataskyddsförordningen kräver att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig nivå av informationssäkerhet i samband med behandling av personuppgifter.[67] Syftet med dessa säkerhetsåtgärder är att garantera systemens konfidentialitet, integritet, tillgänglighet och motståndskraft. Även dessa åtgärder ska baseras på en bedömning av vilka risker behandlingen innebär för den registrerades fri- och rättigheter. Det kan t.ex. vara lämpligt att skydda personuppgifter genom kryptering och pseudonymisering. Den ansvarige måste också regelbundet testa, undersöka och utvärdera skyddsåtgärdernas verkningsfullhet.

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

Anmälan av personuppgiftsincident

Vid en personuppgiftsincident (t.ex. ett dataintrång) ska den personuppgiftsansvarige utan onödigt dröjsmål eller senast inom 72 timmar anmäla incidenten till behörig tillsynsmyndighet.[68] Vad en sådan anmälan ska innehålla anges i förordningen. Den personuppgiftsansvarige är också skyldig att dokumentera alla personuppgiftsincidenter. Om det finns en hög risk för de registrerades fri- och rättigheter ska den personuppgiftsansvarige dessutom utan onödigt dröjsmål informera dessa om incidenten.[69]

Uppförandekoder och certifiering

Dataskyddsförordningens allmänna regler kan vara svåra att omedelbart tillämpa på de specifika förhållandena inom en industri, bransch eller något annat livsområde. Förordningen gör det därför möjligt att genom viss självreglering specificera hur dess bestämmelser ska tillämpas. En sådan uppförandekod får utarbetas av en branschorganisation eller liknande sammanslutning. För att koden ska få den rättsliga status som avses i förordningen ska den ges in till och godkännas av behörig tillsynsmyndighet. Efterlevnaden av koden ska övervakas av ett organ som ackrediterats av behörig tillsynsmyndighet. En kod som godkänns genom ett särskilt förfarande kan få allmän giltighet i unionen.[70]

Den personuppgiftsansvarige kan även genom certifiering, som utförts enligt en godkänd certifieringsmekanism, visa att dess behandling av personuppgifter är förenlig med förordningen. Certifiering utförs av en behörig tillsynsmyndighet eller ett ackrediterat certifieringsorgan.[71] Det är för närvarande oklart hur sådan certifiering kommer att vara organiserad i Sverige.

Noter

1. Europeiska kommissionens meddelande ”Skydd av den personliga integriteten i en uppkopplad värld – En europeiska ram för personuppgiftsskydd för tjugohundratalet”, COM(2012) 9 slutlig.
2. Europeiska kommissionen, Special Eurobarometer 431, ”Data Protection” (2015). 67 % av de tillfrågade uppgav sig känna oro över att inte ha fullständig kontroll över sina personuppgifter på internet. Endast 15 % kände att de hade fullständig kontroll över sina personuppgifter på internet och 31 % ansåg att de inte hade någon kontroll alls.
3. 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).
4. Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31–50).
5. Personuppgiftslagen (1998:204) (PUL). Kompletterande förskrifter finns i personuppgiftsförordningen (1998:1191) (PUF) samt Datainspektionens föreskrifter (DIFS).
6. Artikel 99 i förordning (EU) 2016/679 anger att denna är till alla delas bindande och direkt tillämplig i alla medlemsstater från och med den 25 maj 2018. Svensk lag och andra författningar upphör inte automatiskt genom att en EU-förordning blir tillämplig i Sverige, utan måste upphävas genom beslut av riksdagen, regeringen eller den myndighet som i enlighet med svensk grundlag antagit dessa föreskrifter. Dataskyddsutredningen har föreslagit att både personuppgiftslagen och dess kompletterande föreskrifter upphävs (SOU 2017:39 s. 78).
7. Kommittédirektiv (2016:15) ”Dataskyddsförordningen”.
8. SOU 2017:39 ”Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning”.
9. Prop. 2017/18:105 ”Ny dataskyddslag”, som också innehåller förslag om ändringar av vissa bestämmelser i offentlighets- och sekretesslagen.
10. Artikel 68 i förordning (EU) 2016/679 genom vilken Europeiska dataskyddsstyrelsens inrättas som ett unionsorgan. Styrelsens organisation, befogenheter och uppgifter m.m. regleras i artiklarna 68–76 i förordningen. Styrelsen ersätter Arbetsgruppen för dataskydd, som inrättades genom artikel 29 i direktiv 95/46/EG (den s.k. ”Artikel 29-gruppen”).
11. Artikel 70 i förordning (EU) 2016/679 ger Europeiska dataskyddsstyrelsen behörighet att anta vissa riktlinjer, rekommendationer och bästa praxis om tillämpningen av förordningen. Artikel 288 i Fördraget om Europeiska unionens funktionssätt (EUT C 326, 26/10/2012, s. 1–390) anges att sådana sekundärrättsaker inte ska vara bindande. Att en rättsakt är icke-bindande innebär inte att den helt saknar rättsverkan och kan enligt EU-domstolens rättspraxis i realiteten ha en bindande verkan när dessa anger hur ett unionsorgan ska utöva ett skönsmässigt utrymme (se bl.a. Hettne/Otken Eriksson, ”EU-rättslig metod – Teori och genomslag i svensk rättstillämpning”, 2011, s. 46–48). I praktiken kan styrelsens riktlinjer (i svensk översättning ofta benämnda ”vägledningar”) antas få stor betydelse för tolkning och tillämpning av dataskyddsförordningen.
12. Regeringens pressmeddelande, ”Datainspektionen blir Integritetsskyddsmyndigheten”, den 15 december 2017, [http://www.regeringen.se/pressmeddelanden/2017/12/datainspektionen-blir-integritetsskyddsmyndigheten] (hämtad 2018-02-08).
13. Artikel 4.1 i förordning (EU) 2016/679 innehåller en definition av begreppet ”personuppgifter”. Motiven till bestämmelsen framgår bl.a. av skäl 26–27 och 30 i ingressen till förordningen. Se även Artikel 29-gruppens yttrande 4/2007 om begreppet personuppgifter, antaget den 20 juni 2007 (WP 136).
14. Skäl 14 och 27 i förordning (EU) 2016/679. Förordningen anger inte uttryckligen att oföddas personuppgifter inte omfattas, men det var Artikel 29-gruppens uppfattning att uppgifter som avsåg ofödda inte utgjorde personuppgifter enligt direktiv 95/46/EG (se Artikel 29-gruppens yttrande, WP 136, s. 23). Det finns inget som hindrar att medlemsstaterna utsträcker skyddet av personuppgifter till ofödda och avlida personer.
15. Artikel 4.2 i förordning (EU) 2016/679 innehåller en definition av begreppet ”behandling” av personuppgifter. Det är värt att lägga märke till att förordningen enligt artikel 2 även är tillämplig på helt manuell behandling av personuppgifter under förutsättning att dessa ingår i eller kommer att ingå i ett register. Detta innebär att sådana uppgifter omfattas om dessa strukturerats på ett sådant sätt att sökning på särskilda kriterier förenklas (se artikel 4.6 i förordning (EU) 2016/679). Det är också värt att lägga märke till att den s.k. ”missbruksregeln”, en svensk nationell särregel i 5 a § personuppgiftslagen (1998:204), upphör att gälla den 28 maj 2018.

16. Inventering av personuppgifter som görs innan den 25 maj 2018 utgör behandling av personuppgifter enligt personuppgiftslagen (1998:204) och måste ske i enlighet med denna lag och andra gällande nationella bestämmelser om skydd för personuppgifter.
17. Artikel 3 i förordning (EU) 2016/679 anger dess territoriella tillämpningsområde. Vad som avses med ”etablerad” i unionen definieras inte i förordningen, men det framgår av skäl 22 att det som avses är ”det faktiska och reella utförandet av verksamhet med hjälp av en stabil struktur” samt att den rättsliga formen inte är avgörande. Se även EU-domstolens dom av den 28 juli 2016 i mål C-191/15 Verein für Konsumenteninformation mot Amazon EU Sàrl (ECLI:EU:C:2016:612), dom av den 1 oktober 2015 i mål C-230/14 Weltimmo s.r.o. mot Nemzeti Adatvédelmi és Információszabadság Hatóság (ECLI:EU:C:2015:639) samt dom av den 13 maj 2014 i mål C-131/12 Google Spain SL och Google Inc. mot Agencia Española de Protección de Datos (AEPD) och Mario Costeja González (ECLI:EU:C:2014:317).
18. Förordning (EU) 2016/679 blir inte omedelbart tillämplig i Norge, Island och Lichtenstein, utan måste först införlivas i Avtalet om Europeiska ekonomiska samarbetsområdet. Se Europeiska kommissionens meddelande ”Starkare skydd, nya möjligheter - riktlinjer från kommissionen om den direkta tillämpningen av den allmänna dataskyddsförordningen från och med den 25 maj 2018”, COM(2018) 43 slutlig. För mer information se [http://www.efta.int/eea-lex/32016R0679].
19. Artikel 3.2 i förordning (EU) 2016/679. Bestämmelsen innebär en utvidgning av Europeiska unionens dataskyddsregler i jämförelse med vad som gäller enligt direktiv 95/46/EG, som endast var tillämpligt på organisationer som var etablerade i unionen.
20. Artikel 3.1 i förordning (EU) 2016/679 anger uttryckligen att behandling inom ramen för verksamhet som bedrivs av en organisation som är etablerad i unionen omfattas av förordningen ”oavsett om behandlingen utförs i unionen eller inte”. Det är värt att lägga märke till att överföring av personuppgifter till en tjänsteleverantör i tredje land dessutom omfattas av de särskilda bestämmelserna om överföring till tredje land.
21. Artikel 44–50 i förordning (EU) 2016/679.
22. Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna (EUT L 207, 1.8.2016, s. 1–112).
23. Artikel 45.9 i förordning (EU) 2016/679. Beslut enligt direktiv 95/46/EG gäller tills de ändrats, ersatts eller upphävts genom kommissionsbeslut.
24. Artikel 47 i förordning (EU) 2016/679. Bindande företagsbestämmelser ska godkännas av behörig tillsynsmyndighet. Se även [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_sv].
25. Artikel 46.2 c i förordning (EU) 2016/679. Se även [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en].
26. Artikel 49.2 a i förordning (EU) 2016/679. Ett samtycke ska vara uttryckligt, vilket innebär ett strängare krav än vad som gäller för den registrerades samtycke till behandling av personuppgifter i allmänhet.
27. Artikel 49 i förordning (EU) 2016/679 innehåller undantag i särskilda situationer när det inte föreligger ett beslut om adekvat skyddsnivå enligt artikel 45 eller om lämpliga skyddsåtgärder enligt artikel 46, vilket innefattar bindande företagsbestämmelser.
28. Artikel 5.2 i förordning (EU) 2016/679. Bestämmelsen hänvisar till de principer för dataskydd som räknas upp i artikel 5.1 i förordningen. Den omvända bevisbördan gäller den personuppgiftsansvariges eller ett personuppgiftsbiträdes efterlevnad av dessa principer.
29. Artikel 4.7 i förordning (EU) 2016/679 innehåller en definition av begreppet ”personuppgiftsansvarig”. Det saknar betydelse om det ifrågavarande organet är en egen juridisk person. Även fysiska personer omfattas, men eftersom behandling av rent privat natur är undantagen enligt artikel 2.2 c gäller förordningen i praktiken främst när en fysisk person bedriver näringsverksamhet. Det är värt att lägga märke till att en myndighet är personuppgiftsansvarig även om den inte är en egen juridisk person enligt svensk rätt. Se även Artikel 29-gruppens yttrande 1/2010 om begreppen ”personuppgiftsansvarig” och ”personuppgiftsbiträde”, antaget den 16 februari 2010 (WP 169).
30. Artikel 4.8 i förordning (EU) 2016/679 innehåller en definition av begreppet ”personuppgiftsbiträde”. Ett biträde måste vara en separat juridisk person enligt Artikel 29-gruppens riktlinjer (Artikel 29-gruppens yttrande 1/2010 om begreppen ”personuppgiftsansvarig” och ”personuppgiftsbiträde”, antaget den 16 februari 2010, WP 169, s. 25)

31. Artikel 26 i förordning (EU) 2016/679 innehåller särskilda regler som gäller för gemensamt personuppgiftsansvariga.
32. Artikel 29 i förordning (EU) 2016/679.
33. Artikel 32.4 i förordning (EU) 2016/679. Ett underbiträde måste åläggas samma skyldigheter i fråga om dataskydd som huvudbiträdet genom personuppgiftsbiträdesavtal har ålagts i förhållande till den personuppgiftsansvarige.
34. Artikel 28 i förordning (EU) 2016/679. Ett personuppgiftsbiträde som överträder förordningen genom att fastställa medlen och ändamålen för behandlingen ska räkans som personuppgiftsansvarig för den behandlingen (se artikel 28.10 i förordning (EU) 2016/679).
35. Artikel 28.3 i förordning (EU) 2016/679.
36. Artikel 28.4 i förordning (EU) 2016/679.
37. Artikel 83.5 i förordning (EU) 2016/679 innehåller en uppräkning av under vilka förutsättningar den högre avgiften på 20 miljoner euro kan tas ut vid överträdelse.
38. Artikel 83.4 i förordning (EU) 2016/679 innehåller en uppräkning av under vilka förutsättningar den högre avgiften på 10 miljoner euro kan tas ut vid överträdelse.
39. Artikel 83.7 i förordning (EU) 2016/679.
40. Prop. 2017/18:105 s. 139–142. Se även dataskyddsutredningens betänkande som föreslog högre maxbelopp, SOU 2017:39 s. 287.
41. Artikel 82 i förordning (EU) 2016/679.
42. Artikel 84 i förordning (EU) 2016/679.
43. Prop. 2017/18:105 s. 142–143. Se även dataskyddsutredningens betänkande som överensstämmer med regeringens förslag SOU 2017:39 s. 294.
44. Artikel 5.1 i förordning (EU) 2016/679.
45. Artikel 5.1 b och e föreskriver att undantag för dessa ändamål kan göras från principerna om ändamålsbegränsning och lagringsminimering under förutsättning att lämpliga åtgärder enligt artikel 89.1 vidtas av den personuppgiftsansvarige.
46. Artikel 6.1 i förordning (EU) 2016/679. Den registrerades samtycke i led a ska inte förväxlas med grunden i led b som gör samtycke överflödigt när behandling är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige.
47. Artikel 6.1 f i förordning (EU) 2016/679. Motiven till bestämmelsen framgår bl.a. av skäl 47 i ingressen till förordningen som ger viss vägledning om hur denna ska tolkas.
48. Artikel 6.1 f andra stycket i förordning (EU) 2016/679.
49. Artikel 6.1 e i förordning (EU) 2016/679.
50. Skäl 43 i ingressen till förordning (EU) 2016/679.
51. Artikel 6.1 a och 7 i förordning (EU) 2016/679. Artikel 4.11 innehåller en definition av vad som avses med ”samtycke”. Motiven till bestämmelsen framgår bl.a. av skäl 32–33 i ingressen till förordningen.
52. Skäl 43 i ingressen till förordning (EU) 2016/679, som anger att det är osannolikt att ett samtycke har lämnats frivilligt när en personuppgiftsansvarig är en myndighet.
53. Artikel 9 i förordning (EU) 2016/679. Begreppet ”känsliga personuppgifter” används inte i förordningen, som i stället räknar upp vissa särskilda kategorier av personuppgifter (”som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning”) som omfattas av förbudet i denna bestämmelse. Se även artikel 10 som innehåller ett förbud mot behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser.
54. Artikel 8 i förordning (EU) 2016/679. Förordningen använder begreppet ”informationssamhällets tjänster”, som definieras i artikel 4.25 genom hänvisning till Europaparlamentets och rådets direktiv (EU) 2015/1535 (EUT L 241, 17.9.2015, s. 1). Det som avses i praktiken är i huvudsak internettjänster, såsom söktjänster och sociala media.

55. Prop. 2017/18:105 s. 64. Se även dataskyddsutredningens betänkande som överensstämmer med regeringens förslag, SOU 2017:39 s. 153.
56. Artikel 13–22 i förordning (EU) 2016/679.
57. Artikel 37.1 a i förordning (EU) 2016/679. Skyldigheten gäller behandling som domstolar utför som en del av domstolens dömande verksamhet.
58. Artikel 37.1 b och c i förordning (EU) 2016/679.
59. Artikel 38–39 i förordning (EU) 2016/679.
60. Artikel 24 i förordning (EU) 2016/679.
61. Artikel 25.1 i förordning (EU) 2016/679.
62. Artikel 25.2 i förordning (EU) 2016/679.
63. För mer information se [https://www.enisa.europa.eu/topics/data-protection/privacy-by-design].
64. Artikel 30 i förordning (EU) 2016/679.
65. Artikel 35 i förordning (EU) 2016/679.
66. Artikel 36 i förordning (EU) 2016/679.
67. Artikel 32 i förordning (EU) 2016/679. Se även Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (”NIS-direktivet”) (EUT L 194, 19.7.2016, s. 1–30), som ska vara genomfört i svensk rätt senast den 10 maj 2018. Förslag till svensk nationell lagstiftning har lämnats i betänkandet SOU 2017:36 Informationssäkerhet för samhällsviktiga och digitala tjänster.
68. Artikel 33 i förordning (EU) 2016/679.
69. Artikel 34 i förordning (EU) 2016/679.
70. Artikel 40–41 i förordning (EU) 2016/679.
71. Artikel 42–43 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 SYD LUND UNIVERSITY Urban ICT Arena SANDVINE SEB