SVERIGES TIDSKRIFTER

Lindahl

FRÅGOR OCH SVAR INFÖR DATASKYDDSFÖRORDNINGENS IKRAFTTRÄDANDE

28 september 2017

---

1 ALLMÄNT OM DATASKYDDSFÖRORDNINGEN

Nuvarande reglering för behandling av personuppgifter

Den nuvarande regleringen för behandling av personuppgifter bygger på ett EU-direktiv (95/46/EG). I Sverige har direktivet genomförts genom personuppgiftslagen (1998:207). Personuppgiftslagen innehåller bland annat definitioner av vad som är en personuppgift och vem som är ansvarig för behandling av personuppgifter.

En personuppgift är all information som direkt eller indirekt kan härledas till en fysisk och levande person. Det innebär att inte bara namn, telefonnummer och personnummer utgör personuppgifter utan att också transaktionshistorik, besökshistorik, fotografier och ljudupptagningar på individer kan anses vara personuppgifter. Krypterade uppgifter och olika slags elektroniska identiteter, t.ex. IP-nummer, utgör också personuppgifter om de kan kopplas till en fysisk person.

Behandling av personuppgifter omfattar alla typer av åtgärder som rör personuppgifter, t.ex. inhämtning, åtkomst, lagring och överföring, oavsett om åtgärderna sker automatiskt eller manuellt.

Personuppgiftsansvarig är den som bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige är ansvarig gentemot den vars personuppgifter behandlas, den registrerade, för att behandlingen är förenlig med dataskyddsregleringen.

Den kommande dataskyddsförordningen

EU har under en längre tid förberett en reform av befintlig dataskyddsreglering. Reformen har resulterat i en ny dataskyddsförordning som träder i kraft i maj 2018. Den nya dataskyddsförordningen innehåller nyheter och ändringar avseende behandling av personuppgifter.

Om den personuppgiftsansvarige inte uppfyller kraven enligt dataskyddsförordningen kan en nationell dataskyddsmyndighet, i Sverige Datainspektionen, ålägga den personuppgiftsansvarige att betala en sanktionsavgift om upp till 20 000 000 euro eller 4 procent av en koncerns globala omsättning, beroende på vilket belopp som är högst. En

dataskyddsmyndighet kan utdöma sanktionsavgift på eget initiativ eller efter anmälan av en registrerad.

När dataskyddsförordningen gäller

Dataskyddsförordningen gäller för behandling av personuppgifter som utförs av bolag, föreningar, myndigheter och i vissa fall av privatpersoner. Dataskyddsförordningen gäller dock inte personuppgiftsbehandling som sker av en privatperson för rent personligt bruk, behandling av personuppgifter i områden utanför EU:rätten, såsom försvar och nationell säkerhet eller behandling av personuppgifter i brottsbekämpande verksamhet.

Dataskyddsförordningen gäller för personuppgiftsansvariga som är etablerade i EU eller personuppgiftsansvariga som är etablerade utanför EU om de behandlar personuppgifter i samband med att de erbjuder varor och tjänster till EU-medborgare eller behandlar personuppgifter i samband med profilering av EU-medborgare. Med det sistnämnda avses till exempel att man spårar enskilda personers beteende på internet för att skapa kundprofiler eller liknande.

Utgivningsbevis

Dataskyddsförordningen kommer inte att påverka förhållandet till svenska grundlagar. Yttrandefrihetsgrundlagens bestämmelser om exempelvis utgivningsbevis kommer alltså att fortsätta gälla. Detta omfattar både sådana utgivningsbevis som gäller automatiskt för massmedieföretag och sådana som gäller efter ansökan, så kallade frivilliga utgivningsbevis. Dataskyddsförordningens bestämmelser är därför inte tillämpliga i den mån de inkräktar på rätten till yttrandefrihet.

1.1 Personuppgiftsansvar och personuppgiftsbiträden

Liksom enligt personuppgiftslagen uppställer dataskyddsförordningen ett krav på att ett personuppgiftsbiträdesavtal träffas mellan den personuppgiftansvarige och andra som behandlar personuppgifter för den personuppgiftsansvariges räkning, s.k. personuppgiftsbiträden. Exempel på personuppgiftsbiträden kan vara systemleverantörer och tjänsteleverantörer. Personuppgiftsbiträdsavtalet ska reglera hur personuppgiftsbiträdet får behandla personuppgifter för den personuppgiftsansvariges räkning.

Den personuppgiftsansvarige är precis som enligt personuppgiftslagen ansvarig för skada som uppstår till följd av att personuppgifter har behandlats i strid med lag. Enligt dataskyddsförordningen kan ett personuppgiftsbiträde dock också bli ansvarigt om biträdet har brutit mot de bestämmelser i förordningen som specifikt riktar sig till biträden eller har behandlat uppgifter i strid med den ansvariges instruktioner.

1.2 Dataskyddsombud (Personuppgiftsombud)

Det som i personuppgiftslagen betecknas personuppgiftsombud betecknas i dataskyddsförordningen dataskyddsombud. I vissa fall ska personuppgiftsansvariga och personuppgiftsbiträden enligt dataskyddsförordningen utse ett dataskyddsombud. Så är fallet om den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av personuppgiftsbehandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning eller om den

personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet i stor utsträckning består av behandling av så kallade känsliga personuppgifter eller brottsuppgifter. I övriga fall får en personuppgiftsansvarig eller ett personuppgiftsbiträde utse ett dataskyddsombud om denne så önskar.

Ett dataskyddsombuds uppgifter är bl.a. att informera och ge råd inom den egna organisationen om vilka skyldigheter som gäller enligt såväl dataskyddsförordningen som nationella bestämmelser om dataskydd samt att bevaka att dessa regler följs och ge råd om den konsekvensbedömning avseende dataskydd som ska göras.

Ett dataskyddsombud ska utses på grundval av sina yrkesmässiga kvalifikationer, särskilt vad gäller kunskap i lagstiftning och praxis kring dataskydd. Dataskyddsförordningen föreskriver också att dataskyddsombudet ska involveras i god tid i alla frågor som rör personuppgifter och ges nödvändiga resurser för att utföra sina arbetsuppgifter. Dataskyddsombudet får inte bestraffas eller utsättas för repressalier för utförandet av sina uppgifter och ska rapportera direkt till högsta ledningen.

2 FÖRBEREDELSER FÖR PERSONUPPGIFTSANSVARIGA

Dataskyddsförordningen kommer när den träder i kraft den 25 maj 2018 att gälla som lag i Sverige. Detta innebär även att dataskyddsförordningen kommer att ersätta personuppgiftslagen. Regeringen har tillsatt en utredning som ska föreslå hur den svenska lagstiftningen på området bäst anpassas till förordningen och vilken kompletterande lagstiftning som krävs. Syftet med dataskyddsförordningen är att skapa enhetliga dataskyddsregler inom hela EU vilket underlättar för företag att verka på hela unionens inre marknad.

Om er organisation i dag har en god kunskap om behandling av personuppgifter enligt personuppgiftslagen är det en stor fördel vid föreberedelserna inför dataskyddsförordningen. Många av de begrepp och bestämmelser som finns i personuppgiftslagen återkommer i dataskyddsförordningen. Det är dock viktigt att uppmärksamma att dataskyddsförordningen även innehåller ett flertal förändringar och nya bestämmelser som ändrar hur er personuppgiftsbehandling ska utföras. Genom dataskyddsförordningen utökas exempelvis den personuppgiftsansvariges ansvar och skyldigheter och nya rättigheter för registrerades införs. Sammantaget kan ikraftträdandet av dataskyddsförordningen innebära att ni måste genomföra stora förändringar i er verksamhet för att leva upp till förordningens krav. De nya kraven kan komma att medföra stora förändringar i er verksamhet och det kan kräva en längre implementerings- och anpassningsperiod för att förbereda er organisation inför dataskyddsförordningens ikraftträdande. Det är därför av stor betydelse att anpassningen till dataskyddsförordningen påbörjas så snart som möjligt, vid eventuell utveckling eller utbyte av system kan medföra långa anpassningsperioder.

Nedan följer en sammanställning av de vanligaste frågorna som ni som personuppgiftsansvarig eller personuppgiftsbiträde behöver besvara under förberedelsearbetet inför dataskyddsförordningen.

2.1 Hur ska arbetet påbörjas?

Det viktigaste vid påbörjandet av ett projekt i syfte att förbereda organisationen inför den nya dataskyddsförordningen är att det finns en projektgrupp eller projektledare som ansvarar för att projektet genomförs. Därefter bör organisationen ta höjd i sin interna budget för anpassning till dataskyddsförordningen. Betydande resurser kan behöva avsättas för att säkerställa att organisationen lever upp till kraven i förordningen.

Projektgruppen eller projektledaren bör så snart som möjligt sedan söka stöd hos nyckelpersoner i er organisation. Nyckelpersoner kan bestå av IT-ansvariga, systemägare, registrator, personuppgiftsombud om det finns något sådant och andra nyckelpersoner som har kunskap om era IT-system, register, CRM-system, HR-administration och marknadsföring/kommunikation.

Till skillnad från personuppgiftslagen föreskriver dataskyddsförordningen att den personuppgiftsansvarige ska kunna visa att förordningen följs vilket kan medföra krav på ökad dokumentation. Nationella dataskyddsmyndigheter, såsom svenska Datainspektionen, ges även möjlighet att döma ut en administrativ sanktionsavgift på upp till 20 miljoner euro eller fyra procent av organisationens omsättning när en organisation missköter sin behandling av personuppgifter enligt förordningen.

2.2 Vilka personuppgifter behandlas?

För att veta vilka av dataskyddsförordningens bestämmelser som är tillämpliga på er behandling av personuppgifter krävs att samtliga delar av organisationen utreds för att fastställa vilka olika typer av personuppgifter som behandlas, hur de samlas in och till vem uppgifterna lämnas ut. Olika typer av personuppgifter kan exempelvis vara namn, e-postadress, telefonnummer, personnummer, ekonomisk information såsom exempelvis bankinformation, uppgifter om hälsa, uppgifter om facklig tillhörighet och i vissa fall IP-nummer. Ni bör också sammanställa vilka uppgifter som hanteras inom de olika delarna av er organisation och för vilka ändamål.

Om ni dokumenterar er personuppgiftsbehandling kan det hjälpa er att uppfylla dataskyddsförordningens krav på att ni måste kunna visa att förordningens bestämmelser följs. Andra sätt att uppfylla detta krav är att införa en effektiv policy för dataskydd och tydliga rutiner vid hanteringen av personuppgifter.

2.3 Används journalistundantaget?

Sverige har vid implementeringen av dataskyddsdirektivet infört ett undantag i personuppgiftslagen. Undantaget rör behandling av personuppgifter i ostrukturerat material, den så kallade missbruksregeln eller journalistundantaget. Detta undantag kommer att tas bort genom dataskyddsförordningen. Av den anledningen är det viktigt att ni utreder om ni i nuläget behandlar personuppgifter med stöd av journalistundantaget.

Undantaget innebär att behandling av personuppgifter i ostrukturerat material, till exempel löpande text på internet, är tillåten så länge behandlingen inte utgör en kränkning av den registrerades personliga integritet. Detta undantag försvinner när dataskyddsförordningen träder i kraft eftersom förordningen omfattar all automatiserad behandling av personuppgifter. Om er organisation behandlar personuppgifter i ostrukturerat material behöver ni se över

behandlingen så att den lever upp till dataskyddsförordningens krav, såsom rättslig grund för behandlingen och information till de registrerade.

2.4 Vilken information ska lämnas till den registrerade?

Dataskyddsförordningen medför strängare krav på hur den registrerade ska informeras om behandlingen. Informationen som lämnas ska vara kortfattad, lättbegriplig och utformad med ett tydligt och enkelt språk. Det strängare informationskravet medför att ni bör granska den information som ni lämnar till den registrerade och vid behov revidera denna.

Enligt dataskyddsförordningen ska informationen som lämnas till den registrerade bl.a. omfatta den rättsliga grunden för behandlingen, hur lång tid personuppgifterna kommer att lagras, den registrerades rättigheter enligt dataskyddsförordningen samt möjligheten att lämna klagomål till tillsynsmyndigheten.

2.5 Hur ska ni tillmötesgå de registrerades rättigheter?

Den registrerades rättigheter utökas genom dataskyddsförordningen i jämförelse med personuppgiftslagen. Ni bör utreda hur ni uppfyller de registrerades rättigheter, särskilt nya rättigheter såsom exempelvis rätten till dataportabilitet.

Exempel på registrerades rättigheter är

- få tillgång till sina personuppgifter
- få felaktiga personuppgifter rättade
- få sina personuppgifter raderade
- invända mot att personuppgifterna används för direktmarknadsföring
- invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering
- flytta personuppgifterna i ett allmänt använt, läsbart format (dataportabilitet)

Sammantaget förstärks befintliga rättigheter och några nya rättigheter införs. Förutsatt att er organisation är anpassad för att uppfylla den registrerades rättigheter enligt nuvarande reglering är det troligtvis tillräckligt att för befintliga rättigheter se över rutiner och administration för uppfyllande av rättigheter, såsom exempelvis hur en begäran om registerutdrag eller rättelse ska hanteras. Vissa befintliga rättigheter utökas något, exempelvis rätten för den registrerade att på begäran få en kopia av de personuppgifter som den personuppgiftsansvarige behandlar. Rätten till registerutdrag enligt dataskyddsförordningen omfattar en rätt att kostnadsfritt ta del av de personuppgifter den personuppgiftsansvarige behandlar. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat. Om den registrerade begär ytterligare kopior får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna. Kopian av de personuppgifter som behandlas ska även innehålla information om exempelvis hur länge personuppgifterna kommer att lagras och att den registrerade har en rätt att få felaktiga uppgifter rättade.

En rättighet för den registrerade som införs genom dataskyddsförordningen är rätten till dataportabilitet. Rätten till dataportabilitet innebär att den registrerade har rätt att flytta de personuppgifter som den registrerade själv lämnat från en organisation eller leverantör till en annan, i ett allmänt använt och maskinläsbart

format. För er organisation innebär detta att ni i många fall måste kunna tillhandahålla uppgifterna i ett allmänt använt och maskinläsbart format. Tänk på att det är viktigt att säkerställa att en sådan begäran verkligen kommer från den registrerade och undersök därför vilka tekniska lösningar ni kan behöva för detta.

2.6 Med vilket rättsligt stöd behandlar ni personuppgifter?

För att behandling av personuppgifter ska vara laglig krävs att behandlingen har ett rättsligt stöd. Exempel på rättsligt stöd är avtal med den registrerade, samtycke från den registrerade eller rättslig förpliktelse. Det är viktigt att ni inom er organisation tar ställning till på vilken eller vilka rättsliga grunder ni behandlar personuppgifter. Dataskyddsförordningen uppställer krav på att den personuppgiftsansvarige informerar om den rättsliga grunden redan när uppgifterna samlas in vilket gör att det är ännu viktigare att utreda med vilket rättsligt stöd ni behandlar personuppgifter. Vilken rättslig grund ni stödjer behandlingen av personuppgifter på påverkar den registrerades rättigheter. Dessutom är ett flertal av de registrerades rättigheter beroende av den rättsliga grunden för behandlingen. Den registrerade har exempelvis större möjligheter att motsätta sig behandlingen om intresseavvägning utgör den rättsliga grunden för behandlingen.

En annan anledning till att utreda och dokumentera vilken eller vilka rättsliga grunder som är tillämpliga för den behandling av personuppgifter ni utför är att dataskyddsförordningen uppställer krav på *accountability* vilket innebär att den personuppgiftsansvarige ska kunna visa att förordningens bestämmelser följs.

2.7 Hur inhämtar ni eventuellt samtycke

Dataskyddsförordningens definition av samtycke är liksom enligt personuppgiftslagen en frivillig, specifik och otvetydig viljeyttring. För att ett lämnat samtycke ska utgöra en otvetydig viljeyttring är det inte tillräckligt att tillämpa exempelvis en på förhand ikryssad ruta eller ett s.k. tyst samtycke. Till exempel godtas inte ett tyst samtycke eller en på förhand ikryssad ruta på en webbplats.

Dataskyddsförordningen ställer tydliga krav på att den som behandlar personuppgifter med stöd av samtycke måste kunna visa att ett samtycke har lämnats. Ni bör fundera över hur ni i efterhand ska kunna visa att ett giltigt samtycke har lämnats.

2.8 Behandlar ni personuppgifter om barn?

Ni bör redan nu fundera på hur ni ska kontrollera en persons ålder och hur ni ska inhämta vårdnadshavares samtycke i samband med behandling av barns personuppgifter online.

Genom dataskyddsförordningen införs ett förstärkt skydd för barns personuppgifter, särskilt när det gäller kommersiella internettjänster som sociala nätverk. Kort sagt, om ni erbjuder den typen av tjänster till barn måste ni inhämta vårdnadshavares samtycke för att få behandla barnets uppgifter. Detta gäller enligt förordningen, barn under 16 år. Medlemsstaterna kan själva bestämma en lägre åldersgräns, dock lägst 13 år. Reglerna kan få betydande konsekvenser om er organisation erbjuder denna typ av tjänster till barn. Kom

ihåg att ni då också måste kunna visa att vårdnadshavarens samtycke har lämnats.

Eftersom barn enligt förordningen förtjänar särskilt skydd måste den information som riktar sig till barn vara skriven på ett tydligt och enkelt sätt som barn förstår. Barns skyddsvärda ställning ska också vägas in vid en intresseavvägning.

2.9 Vad ska ni göra vid personuppgiftsincidenter?

Ni bör se till att ni har tillräckliga rutiner på plats för att upptäcka, rapportera och utreda personuppgiftsincidenter.

Dataskyddsförordningen innehåller nya bestämmelser om vad ni som organisation måste göra om ni blir utsatta för dataintrång eller på något annat sätt förlorar kontrollen över de uppgifter ni behandlar. Ni måste dokumentera alla sådana händelser. När det inte är osannolikt att incidenten medför risker för enskildas fri- och rättigheter måste ni anmäla händelsen till tillsynsmyndigheten inom 72 timmar.

Om incidenten kan leda till att personer utsätts för allvarliga risker såsom diskriminering, id-stölder, bedrägerier eller finansiella stölder ska ni även informera de registrerade om händelsen så att de kan vidta nödvändiga åtgärder.

För att kunna leva upp till de nya skyldigheterna enligt förordningen är det viktigt att ni har tillräckliga rutiner på plats för att ni ska kunna upptäcka, rapportera och utreda personuppgiftsincidenter. Ni bör även fundera över vilka risker en sådan incident kan medföra och när ni behöver anmäla händelsen till tillsynsmyndigheten. Tänk på att tidsfristerna för att rapportera personuppgiftsincidenter är korta. Det är därför bra att redan nu bestämma var ansvaret för att göra en sådan anmälan ska ligga i er organisation så att anmälan kan göras i rätt tid.

2.10 Vilka särskilda integritetsrisker finns med er behandling?

Ni bör fundera på om er personuppgiftsbehandling är förenad med särskilda risker för enskildas fri- och rättigheter och om ni i så fall måste göra en konsekvensbedömning avseende dataskydd enligt dataskyddsförordningen.

Förordningen ställer särskilda krav på den som vill behandla personuppgifter på ett sätt som kan medföra stora integritetsrisker för enskilda. Om er organisation avser att utföra en riskfylld personuppgiftsbehandling måste ni först göra en noggrann analys av vilka konsekvenser behandlingen kan få för enskilda. Sådan riskfylld behandling kan till exempel vara storskaliga register som innehåller känsliga personuppgifter, profilering eller omfattande kameraövervakning på allmän plats. Om er analys visar att risken är hög, måste ni samråda med tillsynsmyndigheten innan behandlingen får påbörjas. Observera även kravet på att utse dataskyddsombud vid riskfylld behandling, se mer under punkt 1.2.

2.11 Innehåller era system inbyggt skydd för personuppgifter?

Dataskyddsförordningen ställer krav på att de IT-system ni använder möjliggör ett tillräckligt skydd för personuppgifter. För att systemen ska vara så säkra så

möjligt behövs dataskydd byggas in direkt i systemen. I dataskyddsförordningen betecknas detta privacy by design.

Privacy by design innebär att de grundläggande principerna inom integritetsskydd ska uppfyllas genom systemet, t.ex. att inte mer information än nödvändigt samlas in, att informationen inte lagras längre än nödvändigt och att uppgifterna inte kan användas till något annat än vad som var syftet när de samlades in. Ett annat exempel på privacy by design kan vara att systemen tillåter pseudonymisering, som medför att uppgifterna inte går att koppla till en enskild person utan ytterligare information som hålls avskild eller behörighetsbegränsning som reglerar vem i organisationen som har tillgång till personuppgifter.

2.12 Vem ansvarar för dataskyddsfrågor i er organisation?

Ni bör slutligen bestämma vem eller vilka i er organisation som ska ansvara för att ni följer dataskyddslagsregleringen framöver. Om det krävs enligt dataskyddsförordningen eller om ni väljer att utse ett dataskyddsombud kan denne ansvara för att organisationen följer reglerna. Arbetet tar inte slut vid dataskyddsförordningens ikraftträdande i maj 2018 utan är pågående och kräver regelbunden genomsyn och anpassning. På så sätt kan ni vara säkra på att ni gör allt ni kan för att leva upp till dataskyddsregleringens krav.