Datainspektionen informerar

Nr 2/2016

Allmänna råd

Checklista för att stöda myndigheter och andra organisationer i deras förberedandearbete **inför EU-dataskyddsförordningens** ikraftträdande i maj 2018.

Checklistan innehåller 12 frågor som organisationerna redan nu kan ta ställning till.

Datainspektionen

den 1 september 2016

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

Inledning[1]

I maj 2018 får Åland nya dataskyddsregler då EU:s förordning[2] om personskydd kommer att ersätta gällande regelverk. Dataskydds-förordningen ger möjlighet att komplettera med viss landskaps-lagstiftning. Syftet med EU-förordningen är att skapa enhetliga dataskyddsregler inom hela EU.

Många av dataskyddsförordningens begrepp och principer går att återfinna i landskapslagen om behandling av personuppgifter[3] inom landskaps- och kommunalförvaltning (personuppgiftslagen). Om myndigheterna redan idag har väl genomarbetade åtgärder och rutiner för att säkerställa att personuppgiftslagen följs, finns en bra grund att utgå ifrån. Dataskyddsförordningen innehåller även stora förändringar och vissa helt nya bestämmelser. Den registeransvarigas ansvar och skyldigheter förtydligas och utökas samt de registrerades rättigheter förstärks[4]. De nya kraven kan komma att medföra stora förändringar i verksamheten. För att myndigheterna ska hinna anpassa verksamheten på ett effektivt och kostnadsbesparande sätt är det viktigt att redan nu börja fundera över vilka konsekvenser förordningen kommer att få för verksamheten.

Checklistan kan användas för att ta reda på de viktigaste skillnaderna mellan den nuvarande lagstiftningen, den nya dataskyddsförordningen och hur förordningen kommer att påverka er verksamhet. Datainspektionen kommer fortlöpande att informera om de kommande förändringarna, bland annat genom att ta fram informations- och utbildningsmaterial. Den så kallade artikel 29-gruppen, som består av samtliga nationella dataskyddsmyndigheter inom EU/EES, kommer att ta fram vägledningar på europeisk nivå.

Dataskyddsförordningen lägger stor vikt på den registeransvarigas skyldighet att kunna visa att förordningen följs vilket kan medföra krav på ökad dokumentation. En anpassning till dataskyddsförordningen kommer att kräva en översyn över den interna styrningen och riktlinjer för hur personuppgifter hanteras inom verksamheten.

[1] Den brittiska datatillsynsmyndigheten (Information Commissioner's Office) har utarbetat en publikation i ämnet som givit inspiration till Datainspektionens vägledning.
[2] http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=SV
[3] Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet
[4] http://www.datainspektionen.se/Documents/diverse/dok-eu-blad-2016.pdf

1 Är er organisation medveten om EU:s nya dataskyddsförordning?

Beslutsfattare och nyckelpersoner inom er organisation bör vara medvetna om att personuppgiftslagen kommer att ersättas av dataskydds-förordningen. Undersök hur er organisation kommer att påverkas av förordningen och identifiera de områden som ni måste arbeta särskilt med.

Ni kan behöva avsätta betydande resurser för att hinna anpassa er organisation till de nya kraven innan dataskyddsförordningen ska börja tillämpas. Inledningsvis bör ni särskilt fokusera på att öka medvetenheten om de kommande förändringarna. Det kan bli både kostsamt och svårt att uppfylla reglerna i förordningen om ni väntar med förberedelserna till sista stund.

2 Vilka personuppgifter behandlar ni?

Ni bör inventera och dokumentera vilka personuppgifter ni behandlar, hur de samlas in och till vem uppgifterna lämnas ut. Ni kan behöva göra en bred översyn för att ta reda på vilka uppgifter som hanteras inom de olika delarna av er organisation.

Dataskyddsförordningen innehåller rättigheter som anpassats till informationssamhället. Om ni till exempel har rättat en felaktig personuppgift som tidigare har lämnats ut till någon annan, behöver ni informera mottagaren om detta så att denna i sin tur kan rätta sina egna register. Ni kommer inte att kunna uppfylla detta krav om ni inte vet vilka uppgifter som ni behandlar, varifrån de samlats in och till vem uppgifterna har lämnats ut. Om ni dokumenterar detta kan det hjälpa er att uppfylla dataskyddsförordningens krav på att ni ska kunna styrka 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.

3 Vilken information lämnar ni?

Ni bör granska den information som ni lämnar till de registrerade och fundera över vilka förändringar som kan bli nödvändiga att göra.

I samband med insamlandet av personuppgifter måste ni enligt personuppgiftslagen lämna viss information såsom för vilket ändamål personuppgifterna samlas in. Dataskyddsförordningen innehåller utökade krav på vilken information som ska lämnas till de registrerade. Bland annat kommer ni att behöva informera om den rättsliga grunden för behandlingen, hur länge personuppgifterna lagras och möjligheten att lämna klagomål till tillsynsmyndigheten (som på Åland är Datainspektionen) om man anser att ens personuppgifter har hanterats felaktigt av er. Viktigt i sammanhanget är att dataskyddsförordningen ställer krav på att informationen som lämnas ska vara kortfattad, lättbegriplig och utformad med ett tydligt och enkelt språk.

4 Hur ska ni tillmötesgå de registrerades rättigheter?

Ni bör se över era rutiner för att säkerställa att ni kan uppfylla alla rättigheter som de registrerade har enligt dataskydds-förordningen, såsom till exempel hur ni raderar personuppgifter och hur ni lämnar ut uppgifter elektroniskt i ett allmänt använt format.

De viktigaste rättigheterna för de registrerade är:

- Att få tillgång till sina personuppgifter
- Att få felaktiga personuppgifter rättade
- Att få sina personuppgifter raderade
- Att motsätta sig att personuppgifterna används för direkt marknadsföring
- Att motsätta sig att personuppgifterna används för automatiserat beslutsfattande och profilering
- Att flytta personuppgifterna (dataportabilitet)

I princip kommer de registrerade att ha samma rättigheter som idag. Dataskyddsförordningen stärker rättigheterna ytterligare. Om ni redan har välfungerande rutiner för att tillmötesgå de registrerades rättigheter borde övergången till den nya förordningen gå rätt smidigt. Det är ett bra tillfälle att se över era rutiner och fundera på hur ni ska behandla en begäran om rättelse från en registrerad. Kan era system hjälpa er att hitta och rätta uppgifterna? Vem kan besluta om att uppgifter ska rättas?

Dataskyddsförordningen innehåller i likhet med personuppgiftslagen en skyldighet att på begäran lämna information till de registrerade om vilka uppgifter som behandlas om dem. Detta ska göras kostnadsfritt. När ni hanterar en sådan anhållan kommer ni dessutom att behöva lämna viss ytterligare information, som till exempel hur länge personuppgifterna kommer att lagras och att man har rätt att få felaktiga uppgifter rättade. Om en sådan begäran görs elektroniskt ska den registrerade också kunna få ut informationen elektroniskt.

En nyhet är rätten till dataportabilitet. Denna rättighet kommer att göra det lättare att flytta sina personuppgifter från en organisation eller leverantör till en annan, till exempel om man vill byta socialt nätverk. För er organisation innebär det 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 anhållan verkligen kommer från den registrerade och undersök därför vilka tekniska lösningar ni kan behöva för att uppfylla detta krav.

5 Med vilket rättsligt stöd behandlar ni personuppgifter?

Ni bör undersöka vilka typer av uppgifter som ni behandlar och med vilket rättsligt stöd ni gör detta. Ni bör också dokumentera era slutsatser.

Många organisationer har inte tydligt pekat ut med vilket rättsligt stöd de behandlar personuppgifter. Det är inte ovanligt att organisationer anser sig ha flera alternativa grunder för sin behandling. Med förordningen följer krav på att informera om den rättsliga grunden redan när uppgifterna samlas in. Det är därför viktigt att redan från början ha klart för sig med vilket stöd detta sker. Dessutom är ett flertal av de registrerades rättigheter beroende av den rättsliga grunden för behandlingen.

De rättsliga grunderna för behandling av personuppgifter är i stort sett oförändrade. Ni kan därför redan nu kartlägga vilka behandlingar ni genomför och med vilken rättslig grund ni gör detta. Ni bör dokumentera era slutsatser för att ni också ska kunna visa att ni uppfyller dataskyddsförordningens krav.

6 Hur inhämtar ni samtycke?

Ni bör undersöka på vilket sätt ni inhämtar samtycke, vilken information ni lämnar och hur ni sparar uppgiften om att samtycke har lämnats av den registrerade.

Ett giltigt samtycke enligt dataskyddsförordningen har samma innebörd som gällande personuppgiftslag. Det måste vara fråga om en frivillig, specifik och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandlingen av personuppgifter som rör honom eller henne. Det får inte råda någon tvekan om att den registrerade godtar behandlingen av personuppgifter. Till exempel godtas inte ett tyst samtycke eller en på förhand ikryssad ruta på en

webbplats. Om ni stöder er på samtycke för att behandla personuppgifter behöver ni försäkra er om att kraven på samtycke i förordningen är uppfyllda. Om så inte är fallet, måste ni antingen förändra era rutiner eller finna en annan rättslig grund för behandlingen.

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.

7 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 på nätet.

Genom dataskyddsförordningen införs ett förstärkt skydd för barns personuppgifter, särskilt när det gäller kommersiella internettjänster som sociala nätverk. Om ni erbjuder den typen av tjänster till barn måste ni inhämta vårdnadshavares samtycke för att få behandla barnets uppgifter. Enligt förordningen gäller det barn under 16 år. Medlemsstaterna kan själva bestämma en lägre åldersgräs, 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 all den information som riktar sig till barn vara skriven på ett tydligt och enkelt sätt som barn förstår.

8 Vad ska ni göra vid personuppgiftsincidenter?

Ni bör se till att ni har tillräckliga rutiner 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 osannorlikt 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 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.

9 Vilka särskilda integritetsrisker finns med er behandling?

Ni bör fundera på om er personuppgiftsbehandling är förenad med särskilda risker för enskildas grundlagsenliga fri- och rättigheter samt om ni i så fall måste göra en konsekvensbedömning avseende dataskyddet 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 behandling av personuppgifter 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 kamera-övervakning 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 11.

10 Har ni byggt in skydd för personuppgifter i era IT-system?

Ni bör redan nu ta hänsyn till dataskyddsförordningens bestämmelser när ni tar fram nya IT-system eller förändrar befintliga. Det ger en större möjlighet att följa bestämmelserna, höja säkerheten och förhindra onödiga framtida kostnader.

Grundläggande principer inom integritetsskydd är att inte samla in mer information än vad som behövs, inte ha kvar informationen längre än nödvändigt och inte använda uppgifterna till något annat än vad som var syftet när de samlades in.

Genom att ta hänsyn till dessa principer när man utvecklar nya eller ändrar befintliga IT-system blir det enklare för organisationer att uppfylla bestämmelserna i förordningen. Att bygga in dataskydd i systemen kallas privacy by design och regleras uttryckligen i förordningen.

När ni behandlar personuppgifter ska ni vidta lämpliga tekniska och organisatoriska åtgärder för att uppfylla kraven i förordningen både när ni fattar beslut om hur behandlingen ska genomföras och under hela den fortsatta behandlingen. Vilka åtgärder som behövs beror på uppgifternas art, omfattning och syfte med behandlingen samt vilka risker för enskildas rättigheter och friheter som behandlingen kan innebära. Åtgärderna kan till exempel vara pseudonymisering, som medför att uppgifterna inte går att koppla till en enskild person utan ytterligare information (nyckel) som hålls avskild, eller dataminimering, det vill säga att endast behandla de uppgifter som är nödvändiga för varje enskilt ändamål.

11 Vem ansvarar för dataskyddsfrågor i er organisation?

Ni bör bestämma var i er organisation som ansvaret för dataskydds-frågor ska ligga. Om dataskyddsförordningen kräver det måste ni även formellt utse ett dataskyddsombud.

Förordningen ställer krav på att vissa organisationer ska utse ett dataskyddsombud. Det gäller till exempel offentliga myndigheter och organisationer vars verksamhet involverar särskilt riskfylld behandling, som till exempel regelbunden och systematisk övervakning av registrerade i stor skala eller omfattande behandling av känsliga personuppgifter.

Den person som utses måste ha tillräcklig kunskap om dataskydd och få det stöd och befogenheter som krävs för att kunna utföra sitt uppdrag på ett effektivt och oberoende sätt.

Ni bör redan nu överväga om er verksamhet kräver att ni utser ett dataskyddsombud.

12 Har ni verksamhet i flera länder?

Om er organisation bedriver verksamhet i flera olika EU-länder bör ni ta reda på vilken dataskyddsmyndighet som ansvarar för tillsynen av personuppgiftsbehandlingar ni utför.

Huvudregeln i dataskyddsförordningen är att bara en organisation ska behöva svara inför dataskyddsmyndigheten i ett av EU:s medlemsländer. Om ni har verksamhet i flera länder är det därför viktigt att bedöma vilken dataskyddsmyndighet som ansvarar för tillsynen av de personuppgiftsbehandlingar som ni utför. Förordningens regler kring detta är komplicerade men förenklat utryckt bestäms ansvarig dataskyddsmyndighet utifrån var er organisation har sin centrala förvaltning eller var beslut om personuppgiftsbehandling fattas. I organisationer med traditionella upplägg, där alla viktiga beslut fattas på huvudkontoret, skapar detta normalt inga större problem. Det kan dock bli svårare att avgöra i organisationer med spridda ansvarsområden, där beslut om personuppgiftsbehandlingen ofta fattas på olika ställen. I sådana fall kan olika behandlingar falla under olika tillsynsmyndigheters behörighet.

Det kan alltså vara nödvändigt att kartlägga var i er organisation de viktigaste och mest betydelsefulla besluten om personuppgiftsbehandling fattas.