Förberedelser inför EU:s dataskyddsförordning

Vägledning till personuppgiftsansvariga

Hur kan ni som hanterar personuppgifter förbereda er inför EU:s nya dataskyddsförordning?
13 frågor att besvara redan idag

Datainspektionen

Inledning

Denna checklista tar upp 13 frågor som ni som behandlar personuppgifter bör ta ställning till redan nu för att förbereda er inför införandet av EU:s dataskyddsförordning som ska börja tillämpas i mitten av 2018.

Dataskyddsförordningen kommer att gälla som lag i Sverige och ersätta personuppgiftslagen. Den kommer dock behöva kompletteras med vissa nationella regler. Regeringen har tillsatt en utredning som ska föreslå hur den svenska lagstiftningen på området bäst anpassas till förordningen. Syftet är att skapa enhetliga dataskyddsregler inom hela EU vilket underlättar för företag att verka på hela unionens inre marknad.

Många av dataskyddsförordningens begrepp och principer går att återfinna i personuppgiftslagens bestämmelser. Om ni redan idag har väl genomarbetade åtgärder och rutiner för att säkerställa att personuppgiftslagen följs, kommer ni att ha en bra grund att utgå från. Det är dock viktigt att poängtera att dataskyddsförordningen även innehåller stora förändringar och vissa helt nya bestämmelser. Den personuppgiftsansvariges ansvar och skyldigheter förtydligas och utökas och de registrerades rättigheter förstärks. De nya kraven kan komma att medföra stora förändringar i er verksamhet. För att ni ska hinna anpassa verksamheten på ett effektivt och kostnadsbesparande sätt, är det är därför viktigt att ni redan nu börjar fundera över vilka konsekvenser förordningen kommer att få för er.

Denna vägledning kan användas som en checklista när ni ska ta reda på vilka de viktigaste skillnaderna är mellan den nuvarande lagstiftningen och den nya dataskyddsförordningen och hur de påverkar er. Datainspektionen kommer löpande att informera om de kommande förändringarna, bland annat genom att ta fram informationsmaterial och anordna utbildningar. Den så kallade Artikel 29-gruppen, som består av samtliga dataskyddsmyndigheter inom EU/EES, kommer att ta fram vägledningar på europeisk nivå.

Det är viktigt att ni redan nu börjar planera hur ni ska anpassa er till dataskyddsförordningen och söker stöd från nyckelpersoner i er organisation. Ni kan till exempel behöva införa nya rutiner för att tillmötesgå dataskyddsförordningens utökade krav på öppenhet och de registrerades rättigheter. I större organisationer kan detta få stor påverkan i frågor om budget, it-system, personal, styrning och kommunikation.

Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att förordningen följs, vilket kan medföra krav på ökad dokumentation. Det kommer att införas möjligheter för

tillsynsmyndigheten att i vissa fall döma ut en administrativ sanktionsavgift på upp till 20 miljoner euro eller 4 procent av organisationens omsättning när en organisation missköter sin behandling av personuppgifter. En anpassning till dataskyddsförordningen kommer kräva att ni ser över er interna styrning och era riktlinjer för hur ni hanterar personuppgifter.

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

Ni bör försäkra er om att beslutsfattare och nyckelpersoner inom er organisation är medvetna om att personuppgiftslagen kommer att ersättas av dataskyddsförordningen. Ni bör också undersöka 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 i mitten av 2018. 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 hanterar ni?

Ni bör inventera och dokumentera vilka personuppgifter ni hanterar, 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 denne i sin tur kan rätta sina egna register. Ni kommer inte att kunna uppfylla detta krav om ni inte vet vilka uppgifter som ni hanterar, varifrån de samlades in och till vem uppgifterna har lämnats ut. Om ni dokumenterar detta 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.

3. Använder ni missbruksregeln idag?

Ni bör undersöka om ni i er verksamhet har utnyttjat personuppgiftslagens undantag för att behandla personuppgifter i ostrukturerat material, den så kallade missbruksregeln. Denna regel kommer inte att finnas kvar i förordningen. Ni bör därför särskilt undersöka om behandling som idag stödjer sig på missbruksregeln är förenlig med dataskyddsförordningens bestämmelser.

Behandling i ostrukturerat material, till exempel löpande text på internet, är enligt personuppgiftslagen tillåten så länge behandlingen inte utgör en kränkning av den registrerades personliga integritet. När dataskyddsförordningen träder i kraft försvinner denna svenska särreglering. Förordningen ska tillämpas i sin helhet på all automatiserad behandling av personuppgifter. Har ni i er organisation utnyttjat undantaget för behandling i ostrukturerat material, till exempel vid publicering av personuppgifter på en webbplats eller i annan löpande text, är det viktigt att ni undersöker vilka förutsättningar ni har för att behandla uppgifterna enligt förordningens bestämmelser. Ni kan till exempel behöva undersöka om ni har en rättslig grund för behandlingen, att ni uppfyller de grundläggande kraven på behandlingen och att ni informerar de registrerade på ett korrekt sätt.

4. Vilken information lämnar ni?

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

När ni samlar in personuppgifter måste ni enligt personuppgiftslagen lämna viss information, till exempel om er identitet och ändamålet med behandlingen. 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 i Sverige 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.

5. 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 dataskyddsförordningen, som exempelvis 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
- 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 (dataportabilitet)

På det stora hela kommer de registrerade att ha samma rättigheter som idag men rättigheterna förstärks med dataskyddsförordningen. Om ni redan idag tillmötesgår de registrerades rättigheter bör övergången till den nya förordningen gå relativt smidigt. Det är därför ett bra tillfälle att nu se över era rutiner och fundera på hur ni ska hantera 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 begäran kommer ni dessutom att behöva lämna viss ytterligare information, som exempelvis 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 begära att få ut informationen elektroniskt.

Nytt i dataskyddsförordningen 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 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.

6. Med vilket rättligt stöd behandlar ni personuppgifter?

Ni bör undersöka vilka olika 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. Det finns till exempel större möjligheter för en registrerad att motsätta sig en behandling som sker med stöd av en intresseavvägning.

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.

Observera att myndigheter inte kommer att kunna stödja sin behandling på en intresseavvägning.

7. 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 i personuppgiftslagen. 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 stödjer 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.

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 all 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.

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 tidfristerna 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.

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 12.

11. Har ni byggt in skydd för personuppgifter i era it-system?

Ni bör redan nu ta hänsyn till dataskyddsförordningens regler när ni tar fram nya it-system eller förändrar befintliga. Det ger en större möjlighet att följa reglerna, 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 reglerna 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 liksom 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.

12. Vem ansvarar för dataskyddsfrågor i er organisation?

Ni bör bestämma var i er organisation som ansvaret för dataskyddsfrågor ska ligga. Om det krävs enligt dataskyddsförordningen 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 exempelvis 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 de 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.

På Datainspektionens webbplats finns mycket information om dataskyddsombudets (nuvarande personuppgiftsombudets) roll. Myndigheten ordnar löpande utbildningar för blivande ombud.
Läs mer här:
www.datainspektionen.se/personuppgiftsombud/
www.datainspektionen.se/utbildning/

13. 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 de personuppgiftsbehandlingar ni utför.

Huvudregeln i dataskyddsförordningen är att en organisation bara 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 uttryckt 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.