



WHITE PAPER

Dataskyddsförordningen – Vad innebär den?

Detta white paper handlar om dataskyddsförordningen. Vad innebär den egentligen?

När du läst igenom dokumentet hittar du ett flertal stödmallar på området i DokuMeras dokumentmallsbas under:

Alla mallar > Dataskyddsförordningen

**www.dokumera.se
info@dokumera.se**

VAD INNEBÄR DATASKYDDS-FÖRORDNINGEN?

EU har antagit en förordning om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, även kallad den allmänna dataskyddsförordningen. På engelska kallas denna för General Data Protection Regulation, därav förkortningen GDPR.

I den här promemorian kan du läsa mer om hur din verksamhet kan komma att påverkas av dataskyddsförordningen. Promemorian ger endast en översiktlig bild av regelverket.

3

När är dataskyddsförordningen tillämplig?

Dataskyddsförordningen är tillämplig vid behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Detta innebär att i princip all behandling av personuppgifter omfattas av förordningen.

Begreppen personuppgift och behandling

Varje upplysning som kan hänföras till en viss person är att betrakta som en personuppgift. Flera upplysningar som i kombination gör det möjligt att identifiera en person är också att betrakta som personuppgifter. Några exempel på personuppgifter är namn, adress, e-postadress, IP-nummer och konto- och kreditkortsnummer. Observera att begreppet är vidsträckt, i synnerhet då en upplysning som i sig inte är att betrakta som en personuppgift kan komma att utgöra en personuppgift i kombination med andra upplysningar.

Med behandling avses bland annat insamling, registrering, lagring, bearbetning och spridning. Begreppet kan i princip sägas innefatta allt som görs med personuppgifterna.

Vem är skyldig att följa dataskyddsförordningen?

Den som behandlar personuppgifter enligt ovan är skyldig att följa dataskyddsförordningen. Den gäller för både privat och offentlig verksamhet och är därmed tillämplig för exempelvis myndigheter, föreningar och företag. Den omfattar i princip all behandling av personuppgifter. Däremot ska dataskyddsförordningen inte tillämpas på behandling av personuppgifter som en fysisk person utför av rent privat natur eller som har ett samband med dennes hushåll.

Dataskyddsförordningen kan något förenklat sägas vara tillämplig för företag som har sitt säte i ett EU-land. I förordningen uttrycks det som att den personuppgiftsansvarige ska vara etablerad i unionen, även om själva behandlingen av personuppgifter sker utanför unionen. Det är oftast företaget som juridisk person som är den personuppgiftsansvarige, dvs. bestämmer vilka personuppgifter som ska behandlas och i vilket syfte.

Under vissa förutsättningar är även förordningen tillämplig om den personuppgiftsansvarige är etablerad utanför unionen. Den EU-rättsliga lagstiftaren har med denna reglering velat visa att skyddet för de registrerade ska vara mycket långtgående.

Förordningen är också tillämplig för de företag som behandlar personuppgifter för en personuppgiftsansvarig, t.ex. IT-leverantörer.

Hur skiljer sig dataskyddsförordningen från personuppgiftslagen?

Dataskyddsförordningen har ersatt personuppgiftslagen, vilket innebär att den senare lagen inte längre är tillämplig. Nästan alla de krav som gällde enligt personuppgiftslagen gäller även enligt dataskyddsförordningen – om än med vissa förändringar. Den anmälningsskyldighet om hantering av personuppgifter som fanns i personuppgiftslagen finns inte längre kvar. Begreppet personuppgiftsombud har försvunnit och i stället ersatts av begreppet dataskyddsombud, vars roll skiljer sig en del från personuppgiftsombudets. Här nedan listar vi några av de viktigaste förändringarna.

4

Integritetsskydd och IT-säkerhet

Dataskyddsförordningen ställer höga krav på att du ska skydda de personuppgifter som behandlas. Det innebär att du behöver se över hur ni hanterar personuppgifter, vilket skydd ni har och om det skyddet är tillräckligt för att leva upp till dataskyddsförordningens olika krav.

“Dataskyddsförordningen ställer höga krav på att du ska skydda de personuppgifter som behandlas.”

Personuppgiftsincidenter

Trots hög säkerhet kan olyckan ändå vara framme, dvs. en säkerhetsincident som t.ex. leder till att obehöriga får tillgång till personuppgifter eller att personuppgifter missbrukas. Om det sker kan du vara skyldig att informera Integritetsskyddsmyndigheten inom en viss tid sedan du har fått vetskap om detta. Under vissa omständigheter kan du även vara skyldig att informera de registrerade som berörs av incidenten. Du behöver också dokumentera händelsen angående bl.a. vad du ska göra för att hindra att det inträffar igen.

Rättslig grund för behandling av personuppgifter

Dataskyddsförordningen ställer krav på att du ska kunna visa rättslig grund för de personuppgifter som behandlas, dvs. att du faktiskt har rätt att behandla de personuppgifter som du har samlat in. Detta innebär att du bl.a. behöver kartlägga vilka personuppgifter som samlas in och på vilket sätt det sker.

Samtycke är en rättslig grund för behandling av personuppgifter. Det finns särskilda regler om samtycke, vilka kan sägas ha skärpts i dataskyddsförordningen. Det innebär att du kan behöva se över bl.a. kundavtal och allmänna villkor för att se om du uppfyller kraven.

Tidigare var det möjligt att använda sig av den s.k. missbruksregeln vid behandling av personuppgifter i ostrukturerat material. Denna regel gäller dock inte längre enligt dataskyddsförordningen.

Information till registrerade

Dataskyddsförordningen innehåller utökade krav på vilken information som ska lämnas till de registrerade jämfört med personuppgiftslagen. Du ska t.ex. kunna visa hur du har fått tag i personuppgifter som behandlas och enligt vilken rättslig grund som uppgifter behandlas. Generellt kan sägas att ansvaret för att informera de registrerade i olika avseenden har utökats genom dataskyddsförordningen. Förordningen ställer också krav på att informationen som lämnas ska vara kortfattad, lättbegriplig och utformad med ett tydligt och enkelt språk.

5

Registrerades rättigheter

En registrerad kan bl.a. begära att du rättar felaktiga uppgifter eller att du tar bort personuppgifter (rätten att bli glömd). En registrerad kan också motsätta sig att du använder personuppgifter för vissa särskilda ändamål eller begära att personuppgifter ska flyttas till annan aktör (s.k. dataportabilitet).

Sanktioner

Dataskyddsförordningen innehåller bestämmelser om administrativa sanktionsavgifter, vilka har till syfte att säkerställa förordningens efterlevnad. Avgifterna är avsedda att verka effektivt, proportionellt och avskräckande. Vid bedömningen av storleken på sanktionsavgiften ska hänsyn bl.a. tas till överträdelsens karaktär, svårighet och varaktighet med beaktande av den aktuella uppgiftsbehandlings karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.

Sanktionsavgifterna kan uppgå till 20 000 000 euro eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Vad behöver du göra?

Vad du behöver göra för att leva upp till dataskyddsförordningens krav beror dels på hur din organisation ser ut i dag, dels hur personuppgiftsarbetet ser ut och dels vilken IT-säkerhet din organisation har. Om du vill säkerställa att din verksamhet lever upp till kraven i dataskyddsförordningen kan du börja med att se över nedanstående, vilket kan sägas vara en miniminivå för vilka åtgärder som behöver vidtas.

- Skaffa kännedom om dataskyddsförordningens innebörd.
- Se över vilka personuppgifter ni hanterar i organisationen.
- Se över om ni har rätt att behandla personuppgifterna i fråga.
- Se över hur ni Informerar de registrerade.
- Se över IT-säkerhetsfrågor.
- Se över rutiner och policy-dokument angående personuppgiftsbehandling.
- Undersök om det finns särskilda integritetsrisker.
- Undersök om ett dataskyddsombud behövs eller krävs.
- Säkerställ vad som gäller beträffande tillsyn vid internationell verksamhet.

Om DokuMera

Hos alla företag – stora som små – finns möjligheten att arbeta effektivare genom att använda sig av färdiga mallar. Avancerade dokument är tidsödande att upprätta samtidigt som de kräver expertkunskap för framtagandet. Och som vi alla vet: Experter kostar pengar – mycket pengar.

DokuMera är ett B2B-företag som hjälper människor i svenska företag till en lönsammare och bekvämare tillvaro genom att tillhandahålla digitala dokument via internet. Tillsammans med sakkunniga experter har vi under åren tagit fram tusentals mallar för bland annat juridiska och ekonomiska dokument som säljs både via e-handel och genom personlig försäljning.

Under åren har DokuMera utvecklat Sveriges största databas av digitala, exempelbaserade dokumentmallar, riktade mot företag och organisationer. Produkterna laddas enkelt ned från Internet av våra kunder – företag och organisationer – och kan köpas styckvis eller genom att teckna ett årsabonnemang.

www.dokumera.se

info@dokumera.se