SVERIGES LÅS OCH SÄKERHETSLEVERANTÖRERS RIKSFÖRBUND

SLR - GDPR Quick Guide

Dataskyddsförordningen gäller från 25 maj 2018

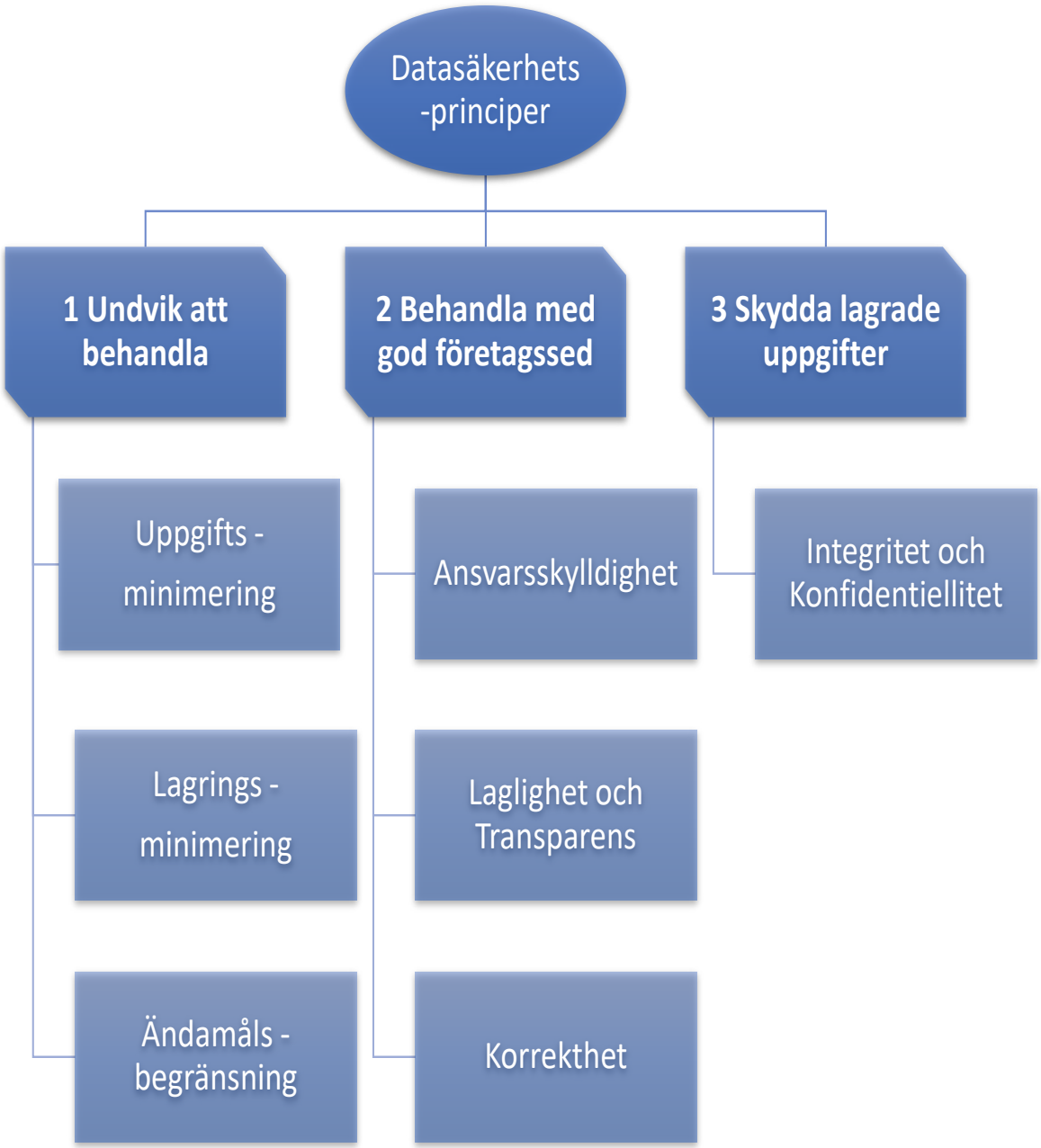
Denna guide är tänkt att göra en komplex fråga väldigt förenklad och ge en mycket enkel grundstart mot att uppnå merparten av de krav som ställs i direktivet. Guiden är allmän och ej uttömmande för vilka åtgärder respektive bolag måste göra. Guiden är i vissa delar förenklad till en grad då den är direkt felaktig, exempelvis om personuppgifter behandlas för en person som lever under skyddad identitet. Gör därför alltid en bedömning vid varje hantering om ytterligare åtgärder behöver göras.

För att uppfylla GDPR ska, bland annat, en kartläggning och en riskbedömning av alla olika behandlingssituationer göras. För att förenkla för SLR:s medlemmar har SLR tagit fram en grundmall för enkel kartläggning och riskanalys, samt att vi i denna guide kommer att beskriva hur denna ska användas. Guiden ger därmed förhoppningsvis verktygen, och tillräcklig förståelse kring GDPR, för att medlemmar ska kunna visa att de vidtagit grundläggande och, sett mot storlek, rimliga åtgärder för att allmänt uppfylla kraven i direktivet.

Att uppfylla GDPR är ett systematiskt, kontinuerligt och långsiktigt arbete. Denna guide har endast till syfte att vara ge en start. Medlemmar kommer att behöva söka kompletterande information och följa utvecklingen. Vi rekommenderar därför **datainspektionen.se** där direktivet, råd och info finns gratis.

Datasäkerhetsprinciper

Direktivet har sju viktiga datasäkerhets-principer i Artikel 5 som behöver uppfyllas. Guiden bygger på dessa principer och vi har delat in dessa i tre steg enligt bilden på nästa sida. Genom guiden belyser vi hur medlemmarna generellt bör göra för att uppfylla principerna.


Datasäkerhets -principer
1 Undvik att behandla
2 Behandla med god företagssed
3 Skydda lagrade uppgifter
Uppgifts - minimering
Lagrings - minimering
Ändamåls - begränsning
Ansvarsskylldighet
Laglighet och Transparens
Korrekthet
Integritet och Konfidentiellitet

Steg 1 undvik att behandla

Enklaste sättet att uppfylla GDPR är att inte behandla personuppgifter alls. Dock är det självklart ofta ett behov att behandla uppgifter som exempelvis personliga telefonnummer, adresser mm. för att kunna bedriva verksamhet. Första steget i att uppfylla GDPR är därmed förenklat att systematiskt minimera hantering, lagring och ändamål av personliga uppgifter till enbart det som rimligen krävs för att utföra våra uppdrag och bedriva verksamheten. Nedan beskrivs hur detta sker praktiskt enligt tre av datasäkerhetsprinciperna.

Uppgiftsminimering – Personuppgifterna ska vara riktiga, relevanta och inte för omfattande

Personnummer, kön, brottsregister, privatekonomi, religion, politisk övertygelse eller sexuell läggning är exempel på extra känsliga uppgifter. Undvik kraftigt att registrera dessa uppgifter så har du kommit en mycket lång bit i att uppfylla kraven som ställs i GPDR.

Exempel på rimliga uppgifter du normalt kan behandla när privatpersoner gör en beställning:

- Kontaktuppgifter, förnamn, telefon och mail
- Uppdragsuppgifter, adress, vägbeskrivning, beskrivning av kundens uppdragsönskemål

Lagringsminimering – Personuppgifter ska endast förvaras så länge det är nödvändigt

Detta innebär att vi ska gallra och rensa uppgifter som inte längre är relevanta för att bedriva verksamheten. Vi har dock rätt och behov av att lagra vissa uppgifter väldigt länge, exempelvis sådant som krävs av annan lag (som bland annat bokföringslagen med flera).

Exempel på sådant som bör makuleras omedelbart efter att syfte med behandling är klar:

- Vandelskontroll på personal, lagra inte, makulera omedelbart efter kontroll
- Kreditprövning på privatperson, lagra inte, makulera omedelbart efter kontroll
- Andra extra känsliga personuppgifter

Exempel på sådant som bör gallras minst en gång per år:

- Registrerade personuppgifter i ändamål att svara på offertförfrågan, som inte längre är aktuell
- Registrerade personuppgifter i slutfört uppdrag som inte längre har ett garantiåtagande

Ändamålsbegränsning – Ändamålen ska vara uttrycklig angivna och berättigad

Här kommer kartläggning av behandling in och genom att du belyser all behandling av personuppgifter i organisationen i denna tar du nästa mycket stora kliv mot att uppfylla kraven i direktivet. För att göra det lite enklare har vi tagit oss friheten att anta några behandlingar i mallen vilket även gör att du enklare kan se hur du använder mallen. Läs dock även steg 2 och 3 innan du börjar med mallen.

Viktigt att tänka på:

- Ändamål för behandling ska vara laglig och behandlingens omfattning ska vara proportionerlig
- Behandla endast de personuppgifter som krävs för ändamålet
- Använd inte personuppgifter till annat än ursprungsändamålet

Steg 2 Behandla med god företagssed

Personuppgifter som behandlas ska hanteras på ett professionellt sätt som hindrar att den personliga integriteten skadas. Det innebär förenklat att ha tydliga och bra rutiner för hur personuppgifter behandlas. Ett tydligt ansvar i att upprätthålla och utarbeta arbetssätt och rutiner så att de överensstämmer med GDPR behövs. Andra steget i att uppfylla GDPR är därför att utse ett Dataskyddsombud och att denna person också är GDPR-kontaktperson, samt delaktig i att denna guide uppfylls.

Ansvarsskyldighet - Personuppgiftsansvarig (på företaget) ansvarar för och ska kunna visa att direktivet efterlevs

Företaget ansvarar för att GDPR blir uppfyllt och Dataskyddsombudet blir företagets kontaktperson i GDPR-frågor. Dataskyddsombudet bör därför vara involverad vid förändringar inom organisationen, exempelvis inköp av nya IT-program. Detta för att kunna riskbedöma uppdateringar av rutiner, samt kunna influera förändring av rutiner kontinuerligt, så att företaget uppfyller kraven i GDPR och kan visa hur de uppfylls.

Våra råd är att utse ett Dataskyddsombud som är:

- Moralisk och upprätthåller god företagssed
- Datakunnig och bra på att hantera Microsoft Excell
- Skicklig på att bedriva kvalitetsarbete och forma rutiner
- Har stort inflytande inom bolaget

Våra råd till dataskyddsombudet är att läsa vanliga frågor och svar på datainspektionens hemsida och att hålla sig uppdaterad inom området. Vi rekommenderar även att ta aggressiv marknadsföring från diverse GDPR-konsulter, angående katastrofskadestånd och liknande, med en nypa salt.

Laglighet och transparens – Behandlingen ska stödjas av lag, GDPR, samt vara rättvis och transparent

Samtycke är en viktig del inom denna princip. Samtycke ska vara frivilligt och behöver i vissa fall vara väldigt tydligt i skrift, exempelvis vid kreditprövning.

Samtycke kan även vara muntligt vid följande exempeltillfällen:

- En kund ringer eller mailar och gör en beställning
- En kund gör ett köp i butik
- En kund ger en offertförfrågan på en mässa

Laglighet är ytterligare en viktig del att uppfylla. Att kräva att få veta vad medarbetare ska rösta på i nästa val är exempelvis inte förenligt med GDPR. Enkelt uttryckt gäller det här att ha god företagssed, sunt förnuft och att respektera personlig integritet samt att följa steg 1, undvik att behandla.

Transparens är slutligen också något som ska uppfyllas, utan kostnad. Dataskyddsförordningen kräver normalt att personuppgifter och information om behandling av dessa ska kunna lämnas ut, i en lätt tillgänglig och skriftlig form på kundens begäran. Detta kan ske elektroniskt och vi rekommenderar att personuppgiftsansvarig person vid en sådan eventuell begäran kollar upp på datainspektion.se vad som krävs i det specifika fallet, samt att kunden besvaras inom rimlig tid, d.v.s. inom cirka en arbetsvecka.

Korrekthet – Personuppgifterna ska vara uppdaterade och korrekta, annars ska de makuleras

Rimliga åtgärder ska vidtas för att säkerställa att personuppgifter raderas eller rättas utan dröjsmål ifall de upptäcks vara felaktiga i förhållande till de ändamål de behandlas. Genom steg 1 kan risken för felaktiga uppgifter minskas kraftigt. För att uppfylla denna princip behöves en rutin som säger något i stil med: ”Rimliga åtgärder ska vidtas för att säkerställa att personuppgifter raderas eller rättas utan dröjsmål ifall det upptäcks att de är felaktiga i förhållande till de ändamål för vilka de behandlas.”

Steg 3 Skydda lagrade uppgifter

Steg 3 är inte bara viktigt för att uppfylla GDPR utan även för att bedriva en pålitlig säkerhetsverksamhet. Skulle ett företag bli utsatt för dataintrång eller på något annat sätt tappa kontroll över personuppgifter, så måste bolaget informera både de personer som uppgifterna gäller och Datainspektionen, om incidenten är allvarlig. Exempelvis om uppgifterna som läckt ut kan leda till att personer utsätts för diskriminering, ID-stölder, bedrägeri eller finansiella förluster. Med tanke på vår bransch är detta ett mycket viktigt steg mot att uppfylla GDPR, samt för att skydda våra kunder.

Integritet och konfidentialitet – Det ska finnas en lämplig säkerhet för personuppgifter, liksom skydd mot obehörig eller otillåten behandling samt mot förlust, förstöring eller skada genom olyckshändelse

För att uppfylla denna princip krävs att dataskyddsombud säkerställer att det finns erforderlig IT-säkerhet. Det kräver även bra rutiner för handhavande av uppgifter, samt utrustning som lagrar eller har tillgång till uppgifter, exempelvis smartphones. Vår rekommendation är att varje företag starkt överväger att anlita extern hjälp i att förbättra bland annat IT säkerheten. SSF kommer inom kort med en norm i området som även hjälper företag att forma nödvändig IT-säkerhet.

Exempel på viktiga saker att riskbedöma och riskminimera skada för med minst årliga revisioner:

- Förlust, stöld eller intrång i mobil, USB-minne, server eller dator
- Förlust, stöld eller kopiering av utskrivna eller handskrivna handlingar
- Felhantering, olycka eller okunskap i att använda uppgifter eller administrativa applikationer
- Bristande mail-, webb- eller telefondisciplin gällande behandling av personuppgifter

Kartläggning och riskbedömning

Med förförståelse för de sju datasäkerhetsprinciperna genom guidens tre steg är det dags att kartlägga och riskbedöma de behandlingssituationer ni arbetar med. Mallen användes sedan för att forma nödvändiga åtgärder och rutinuppdateringar, samt för att vid behov kunna uppvisas för datainspektionen.

Mallen finns i filen **”GDPR kartläggning och riskanalys SLR 1.1”** och bör användas om medlemmar inte själva har ett kvalitetssystem eller annan programvara som löser detta behov på annat sätt. Mallen är uppbyggt i Excell genom tre flikar som beskrivs nedan.

Den första fliken **Grundläggande uppgifter** är till för att uppfylla kriterier i GDPR ifall datainspektionen kräver att få ta del av hur medlemmen uppfyller GDPR.

Den andra fliken **Beskrivning** är till för att skapa definitioner av valbara kategorier i den tredje fliken samt uppfylla kriterier i GDPR. Återigen, utse ett Dataskyddsombud som är bra på att använda Excell.

Den tredje fliken är där **Kartläggning och riskanalys** sker. Här behöver ni revidera grundförslagen så att de stämmer med den verksamhet ni som medlem bedriver. Det är sannolikt att ni har fler behandlingssituationer än de som beskrivs, samt att några av behandlingsexemplen inte är relevanta för just er verksamhet. Känn er fira att bygga om formatet och anpassa mallen för att bättre passa er verksamhet. Återigen, utse ett dataskyddsombud som är bra på att använda Excell, alternativt lös GDPR-frågan på ett annat sätt än att använda mallen.

Slutord

Vi hoppas att denna förenklade guide gett våra medlemmar en kvalitativ snabbstart och bra grundförståelse för GDPR. Datainspektionen.se har GDPR-direktivet med beskrivningar och vi rekommenderar därför att våra medlemmar själva söker mer information via deras hemsida. Utöver detta finns stora mängder hemsidor med tips och tolkningar på GDPR att söka/googla bland.