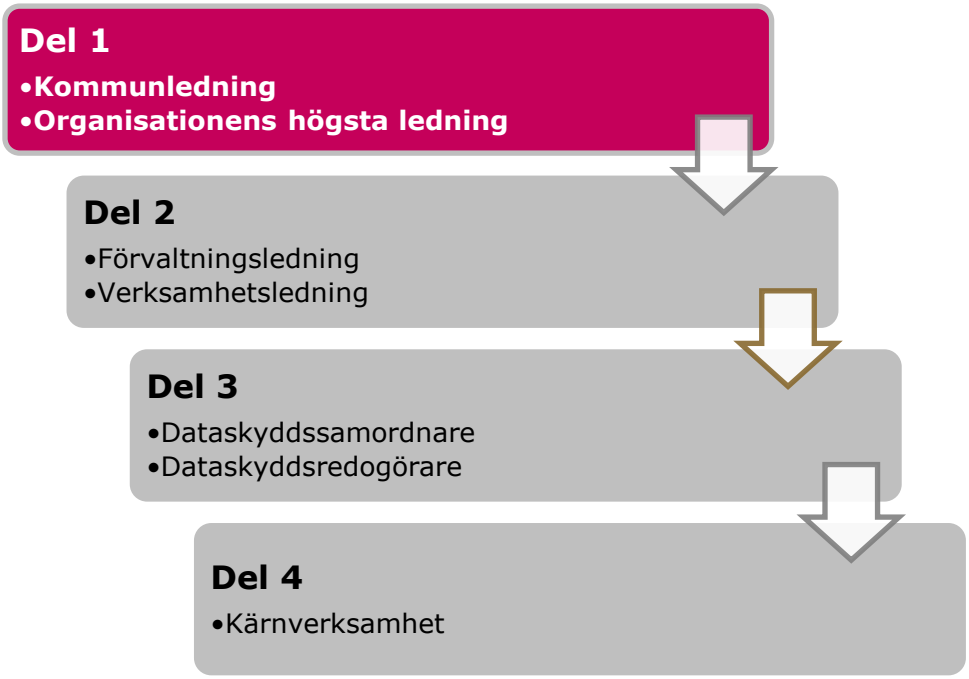
DATASKYDD (GDPR)
Del 1: Kommun-/regionledning



Om dokumentet

I det här dokumentet finns en sammanfattning av det som ledningen centralt behöver göra för att uppfylla dataskyddsförordningen som trädde ikraft 2018. Målgruppen är både den politiska ledningen och ledningsgrupp på central förvaltning. Informationen riktar sig till organisationer som avtalat med Sydarkivera om gemensamt dataskyddsombud som anslutande tjänst.

Texten baseras framför allt på:

- Vägledningar från Sveriges kommuner och landsting (SKL)
- Vägledningar från Datainspektionen

- *Dataskyddsförordningen GDPR – förstå och tillämpa i praktiken*, Monika Wendleby och Dag Wetterberg (2019).

Bakgrund

Dataskyddsförordningen, eller GDPR (*General Data Protection Regulation*) som den också kallas, innehåller regler om hur man får behandla personuppgifter. Syftet är att skapa ett enhetligt regelverk inom EU för behandling av personuppgifter. Förordningen började gälla den 25 maj 2018 och ersätter helt personuppgiftslagen (PuL). Sverige har också tagit fram kompletterande lagstiftning i dataskyddslagen som började gälla 25 maj 2018.

Den 1 maj 2018 startade Kommunalförbundet Sydarkivera en verksamhet som gemensamt dataskyddsombud för de förbundsmedlemmar som tecknat avtal om anslutande tjänst. Bestämmelser om samverkan inom ramen för Sydarkivera finns i förbundsordningen som antagits av samtliga fullmäktige inom medlemskretsen.

Förbered verksamheten och organisera GDPR-arbetet

1. Informera internt

Dataskyddsförordningen kommer att ersätta personuppgiftslagen. Detta medför att det blir ändringar och kompletteringar i många svenska lagar. Försäkra er om att beslutsfattare, medarbetare och nyckelpersoner inom er organisation får information om förändringen och vad det innebär.

Tips! Informera via ledningsgrupper, intranät eller nyhetsbrev.

2. Informera externt om rättigheter

Det behöver finnas information på webbplatsen eller andra kontaktytor så att allmänheten kan få information om de behandlingar som utförs, om de registrerades rättigheter och hur de kan utöva dem.

Tips! SKL har tagit fram vägledning och mallar för kommunikatörer för att underlätta detta arbete.

3. Intern organisation och samordnare

Varje myndighet, nämnd eller styrelse, är personuppgiftsansvarig för sin verksamhetsinformation. Se till att det finns en organisation med utpekat ansvar och roller som kontinuerligt arbetar med dataskydd. Denna organisation kan se ut på många sätt beroende på de arbetssätt och förutsättningar som finns.

Beslut om intern/lokal organisation för dataskydd ska beslutas av kommunstyrelse eller motsvarande.

Tips! En enkel organisation att starta med finns nedan. Det finns ett särskilt dokument som riktar sig till dem som ska arbeta praktiskt med dataskydd.

- Dataskyddssamordnare: Leder det övergripande arbetet inom kommunen och samordnar dataskyddsredogörarna. Denna person rapporterar till ledningen.
- Dataskyddsredogörare: Varje förvaltning utser en eller flera personer som arbetar med dataskydd på verksamhetsnivå.

4. Gemensam organisation för dataskyddsombud

Hos Sydarkivera finns ett team med olika kompetenser som är gemensamma resurser när det gäller frågor om dataskydd. Teamet kommer att arbeta nära tillsammans med samordnaren i den organisation som har Sydarkivera som dataskyddsombud. Träffar för erfarenhetsutbyte och gemensam arbetsplats på webben finns för att dela information och ställa frågor. I uppdraget ingår:

- Information, mallar, rådgivning och utbildning.
- Kontroll av att bestämmelserna om dataskydd efterlevs.
- Kontaktperson mot tillsynsmyndighet (datainspektionen)
- Följa rättsutvecklingen inom området.

Tips! *Om man har frågor kring dataskydd ställs dessa till Sydarkivera på dataskydd@sydarkivera.se.*

5. Utse dataskyddsombud

Varje myndighet ska utse dataskyddsombud inom en kommun eller region, Kommunalförbund och bolag utser dataskyddsombud i styrelsen.

- Det är Sydarkiveras förbundsjurist Therese Jigsved som är dataskyddsombud.

Tips! Utgå från mall för tjänsteskrivelse som tagits fram i samarbete samt den förifyllda blankett som ska skickas in till Datainspektionen.

6. Dataskyddspolicy

Anta dataskyddspolicy samt riktlinjer för dataskydd. I dataskyddspolicyn anges vision och de övergripande mål som kommunen/regionen/myndigheten har med sitt dataskyddsarbete. ”. I policyn ska det framgå vilken strategi man har för skydd av personuppgifter. Syftet med en dataskyddspolicy är att alla ska förstå vad kommunen/regionen/myndigheten gör, varför och hur. Enligt lagen ska man ge informationen ”i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk

Tips! *Utgå från mallarna för dataskyddspolicy och riktlinjer som Sydarkivera tagit fram.*

7. Översyn styrande dokument

Gå igenom organisationens styrande dokument och uppdatera dem om det behövs. Översynen gäller inte enbart dokument relaterade till it och säkerhet utan även andra styrdokument.
Börja med de styrande dokumenten som direkt berörs av dataskyddsförordningen:

- Dataskyddspolicy och riktlinjer för dataskydd
- Integritetspolicy/Sekretesspolicy för utläggning på webb
- Säkerhetspolicy och riktlinjer för säkerhet
- Informationssäkerhetspolicy och riktlinjer för informationssäkerhet
- Riktlinjer för incidentrapportering

- Riktlinjer för anställda/förtroendevalda hur personuppgifter ska/inte får behandlas i epost, SMS, chatt och på internet eller annat ostrukturerat material
- Riktlinjer för rättelse, radering, begränsning av behandling och vid invändning av användande av personuppgifter
- Upphandlingspolicy och riktlinjer för upphandling ex. kring säkerhet och molntjänster
- Övriga styrdokument som finns ska ses över som t.ex. personalpolicy, finanspolicy och näringslivspolicy. Det är inte säkert alla styrdokument berörs och behöver uppdateras men det är viktigt att alla policys och riktlinjer gås igenom. Kontrollera om det på något sett berörs av den nya lagstiftningen och om så är fallet så uppdatera dem.

Tips! *Utgå från mallarna för olika policys och riktlinjer som Sydarkivera har. Texter att använda i olika styrdokument finns också.*

8. Incidenter

För att kunna leva upp till de nya skyldigheterna enligt dataskyddsförordningen är det viktigt att organisationer som behandlar personuppgifter har rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter. Det är viktigt att arbeta medvetet och proaktivt för att undvika personuppgiftsincidenter. Se till att skapa tydliga rutiner för att enkelt kunna upptäcka personuppgiftsincidenter, upprätta en handlingsplan för de fall en personuppgiftsincident inträffar och dokumentera alla personuppgiftsincidenter, även dem som inte måste anmälas till Datainspektionen.

Tips! *Utgå från mall för Riktlinjer för personuppgiftincidenter samt den vägledning som finns hos Datainspektionen. Datainspektionen har också blankett och instruktioner hur anmälan till dem ska gå till.*

9. Registerförteckning

Både personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register eller en förteckning över behandlingar av

personuppgifter. Dessa register ska upprättas skriftligen, vara tillgängliga i elektronisk format och hållas uppdaterade.
På begäran ska registret göras tillgängligt för Datainspektionen.
Det är viktigt att den övergripande ledningen för kommun/region i form av datasamordnare ser till att samtliga myndigheter som tillhör deras organisation har en registerförteckning över alla personuppgiftsbehandlingar. Om det finns en registerförteckning enligt personuppgiftslagen behöver den kompletteras och uppdateras. Om det inte finns ett gemensamt system i organisationen kan den mall som tagits fram av SKL användas för att påbörja en enkel registerförteckning.

Tips! *Utgå från den instruktion och mall som SKL tagit fram för registerförteckning om organisationen inte har ett eget verktyg.*

10. Dokumentation

Samla systematiskt och fortlöpande dokumentation som visar hur ni följer dataskyddsförordningen, utöver registerförteckningen.

Se till att dokumentation om dataskydd hålls på ett ordnat och systematiskt sätt och att rutiner finns för att hålla det uppdaterat.

Se också till att dokumentation som visar hur organisationen uppfyller kraven i dataskyddsförordningen som helhet eller per myndighet finns samlad tillsammans med registerförteckningar. Dokumentation som visar detta kan t.ex. vara policys, riktlinjer, checklistor, konsekvensbedömningar, riskanalyser, blanketter.

Tips! *Diarieför de styrdokument, rutiner och instruktioner som gäller för organisationen så de är lättåtkomliga vid kontroll. Använd också gärna ett register/system som visar vilka dokument, ex styrdokument och registerförteckning ni har för att klara dataskydd men även över konsekvensbedömningar, informationskartläggningar etc. Man kan använda ett*

verktyg eller samarbetsyta eller pärm för att få överblick över hur dataskyddet hanteras övergripande i organisationen.