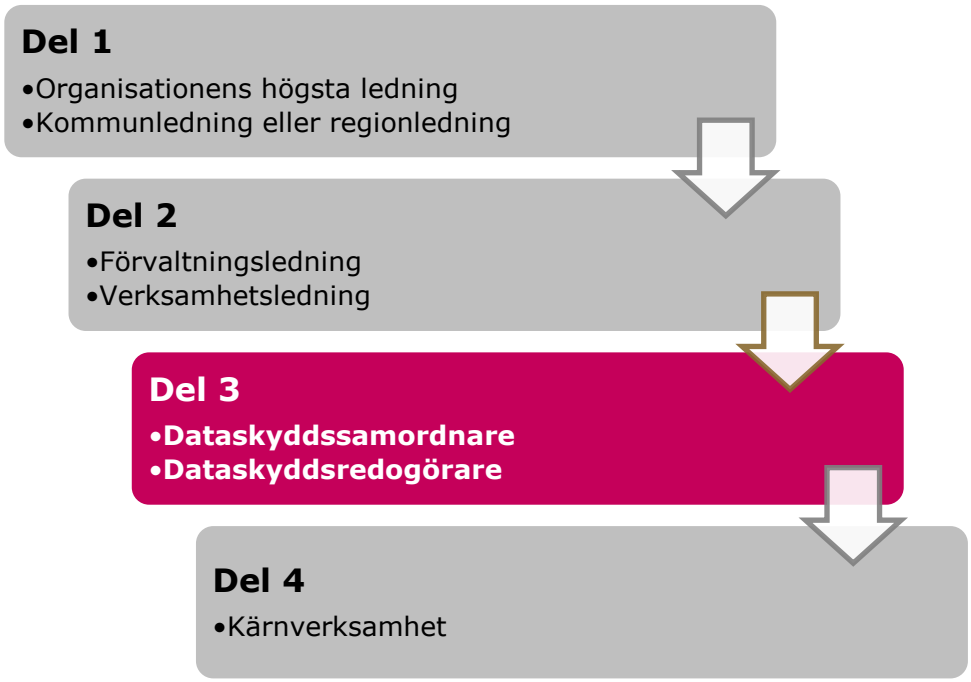
# DATASKYDD (GDPR) Del 3: Dataskydds-samordnare och Dataskyddsredogörare




## Om dokumentet

I det här dokumentet finns ett antal frågor som checklista för dig som är dataskyddssamordnare eller dataskyddsredogörare.

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 personuppgifter ska behandlas. 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.

## Roller och ansvar

- Varje myndighet (nämnd eller styrelse) är personuppgifts-ansvarig (PUA) för sin verksamhetsinformation.
- **Dataskyddssamordnaren** leder det övergripande arbetet inom kommun/region och rapporterar till ledningen.
- **Dataskyddsredogörare** och **biträdande dataskyddsredogörare** utses av nämnd/styrelse och arbetar med dataskydd på förvaltningsnivå.

## Sydarkiveras team för dataskyddsombud

Hos Sydarkivera finns ett team med olika kompetenser som är gemensamma resurser när det gäller frågor om dataskydd. Teamet arbetar nära tillsammans med dataskyddssamordnaren i kommunen. I teamet ingår jurist, arkivarie och informationssäkerhetsspecialist.

I uppdraget ingår:

- Ge information, rådgivning och utbildning samt skapa och tillhandahålla mallar.
- Kontrollera att bestämmelserna om dataskydd efterlevs.
- Kontaktperson mot tillsynsmyndighet (datainspektionen)
- Följa rättsutvecklingen inom området.

Träffar för erfarenhetsutbyte och utbildningar erbjuds fortlöpande. Anmäl dig till aktiviteter via Sydarkiveras bokningsportal:

https://sites.legaonline.se/sydarkivera/Kurser

För dataskyddssamordnare och dataskyddsredogörare finns en gemensam arbetsplats på webben för att dela information och ställa frågor.

https://www.yammer.com/dataskyddsydarkivera/

Det finns en gemensam handbok för dataskydd på Sydarkiveras webb där man kan hitta svar på frågor och mallar till olika dokument som man behöver för dataskydd.

https://sydarkivera.se/handbok/dataskydd/

Det finns grupper för GDPR, informationssäkerhet med mera på Sydarkiveras nätverk för förbundsmedlemmarna på Yammer:

https://www.yammer.com/sydarkivera/

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

## Individens rättigheter

Det är viktigt att det finns rutiner på plats för att säkerställa att ni kan uppfylla alla rättigheter som de registrerade har.

När det gäller rättigheten att få sina personuppgifter raderade finns det undantag för behandling som görs av myndigheter. Uppgifter i register och dokument som är allmän handling och som myndigheter är skyldiga att bevara enligt arkivlagen kan inte raderas hur som helst. Till det krävs gallringsbeslut.

**Frågor som stöd i arbetet:**

- ☐ Finns det rutiner för att den enskilde vid begäran ska kunna få tillgång till sina personuppgifter (registerutdrag)?
- ☐ Finns det rutiner för att den enskilde ska kunna få felaktiga personuppgifter rättade?
- ☐ Finns det rutiner för att på begäran kunna leverera registerförteckning över system/behandlingar till Datainspektionen?

- ☐ Hur har den enskilde möjlighet att invända mot att personuppgifter används för automatiserat beslutsfattande och profilering? Tänk på att dessa kräver samtycke.

***Tips!*** Utgå från den mall för presentation och de broschyrer för personuppgiftsansvariga och övriga som har tagits fram av Sydarkivera.

## Styrande dokument

Gå igenom organisationens styrande dokument och uppdatera dem om det behövs. Det gäller inte enbart dokument relaterade till it och säkerhet utan även andra styrdokument. Till exempel personalområdet påverkas av dataskyddsförordningen. Styrdokumenten ska tydliggöra hur organisationen ska beakta det inbyggda dataskyddet strategiskt.

För mallar och texter som kan användas i styrdokument se: https://sydarkivera.se/handbok/dataskydd/

## Intern styrning och riktlinjer

Se över den interna styrningen och riktlinjerna för hur personuppgifter ska hanteras i verksamheterna. Det kan vara så att nya rutiner behöver införas. Arbetet berör flera olika funktioner som informationssäkerhet, dokument- och ärendehantering, upphandling, systemförvaltning och it.

**Frågor som stöd i arbetet:**

- ☐ Hur hanterar vi IT-inköp och säkerhet (kravställning vid upphandling)?
- ☐ Hur ska mobila enheter användas?
- ☐ Vilka Appar för mobila enheter ska användas och hur får de användas?
- ☐ Har PUB-avtal tecknats med personuppgiftsbiträden som tillhandahåller externa tjänster?
- ☐ Har instruktioner bifogats PUB-avtalet där man talar om hur personuppgifterna ska behandlas?
- ☐ Har man i huvudavtalet för externa tjänster talat om när och hur åtkomst till personuppgifterna ska ske?
- ☐ Har man i huvudavtalet talat om hur personuppgifterna ska säkerhetskopieras.
- ☐ Har arbetet påbörjats för att bygga in stöd för dataskydd i de IT-stöd som används? (Kallas ibland för *Privacy by Design*)
- ☐ Finns frågor om dataskydd med i arbetet inför upphandlingar av system, tjänster eller utveckling?

- ☐ Hur säkerställer ledningen att medarbetarna har rätt kunskaper och förståelse (att det finns ett lärande i organisationen) kring inbyggt dataskydd?
- ☐ Hur planerar organisationen för att upprätthålla ett långsiktigt arbete kring dataskydd?
- ☐ Är befintliga processer och styrdokument relevanta och tillräckligt tydliga?
- ☐ Har ni integrerat dataskyddsarbetet i risk- eller avvikelsehantering?
- ☐ Har ni byggt in skydd för personuppgifter i era IT-system?

***Tips!*** Arbeta praktiskt med dataskydd i samband med förändringar i verksamheten, som till exempel upphandlingar av system och tjänster. Använd verktyg för risk-och sårbarhetsanalys och gör konsekvensanalyser vid upphandling. Utgå från mallarna som Sydarkivera har. Texter att använda i olika policys och riktlinjer finns också att utgå ifrån.

## Registerförteckning

Det behöver finnas en registerförteckning över alla personuppgiftsbehandlingar för alla nämnder/styrelser. Om det finns en registerförteckning/system enligt personuppgiftslagen behöver den kompletteras och uppdateras. Om det inte finns ett gemensamt verktyg för registerförteckningar i organisationen kan den mall som tagits fram av SKL användas för att påbörja en enkel registerförteckning.

Registerförteckningen för en organisation ger en praktisk fördel eftersom man får en god överblick och kontroll över vilka behandlingar som görs inom organisationen. Är den välgjord kan den användas när en registrerad frågar efter registerutdrag eller om man råkar ut för personuppgiftsincident.

Bestäm hur registerförteckningen ska se ut i organisationen och se till att rutiner och instruktioner är gemensamma för hela organisationen så alla styrelser/nämnder fyller i likadant så resultatet går att jämföra och använda. Ta också fram rutiner för hur registerförteckningen ska hållas kontinuerligt uppdaterad hela tiden.

***Tips!*** Utgå från den instruktion och mall som SKL tagit fram för registerförteckning om inte den övergripande organisationen har ett verktyg. Mall för inventering av system (med registerförteckning) med koppling till SKL:s PUB-avtal och instruktioner finns tillgänglig hos Sydarkivera.

## Dokumentation

Dataskyddsförordningen kräver att organisationen har god ordning på sina styrande dokument. Det innebär att alla viktiga styrdokument ska vara uppdaterade och enkla att hitta. Det gäller såväl styrande dokument (strategier och policyer) som rutiner, det vill säga allt som kan påverka hur organisationen hanterar det inbyggda dataskyddet.

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

Om organisationen inte har kontroll över sina styrdokument kan man inte säga att den följer principen i dataskyddsförordningen om ansvarsskyldighet. Den innebär att rutiner/policyer för dataskydd ska vara kända inom organisationen och dessa ska tillämpas på lämplig ledningsnivå.

***Tips!*** Diarieför de styrdokument, rutiner och instruktioner som är framtagna för förvaltningen 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 med mera. Man kan använda ett verktyg, samarbetsyta på webben eller pärm för att få överblick över hur dataskyddet hanteras.

## Leverantörer och avtal

- ☐ Se över aktuella avtal och säkerställ att de är uppdaterade med personuppgiftsbiträdesavtal och instruktioner som är anpassade till dataskyddsförordningen.
- ☐ Kontrollera med er upphandlingsenhet om de avser hantera uppdateringen av de avtal som redan finns eller om förvaltningarna själva måste uppdatera dem.
- ☐ Avtal med leverantörer/samarbetspartners där personuppgiftsbiträdesavtal saknas behöver upprättas.

Tänk på att inte alla situationer kräver personuppgiftsbiträdesavtal utan det kan vara mer lämpligt med andra typer av avtal för att uppfylla lagen.

***Tips!*** Använd den mall från SKL som tagits fram för personuppgiftbiträdesavtal med instruktion kring hantering av personuppgifter. Sydarkivera har också mallar för datadelning och samarbete mellan olika organisationer där det inte krävs regelrätta personbiträdesavtal.

## Incidenter

För att kunna leva upp till de nya skyldigheterna enligt dataskyddsförordningen behöver 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.
Ha tydliga rutiner för att enkelt kunna upptäcka personuppgifts-incidenter och hur organisationen som helhet ska agera i de fallen samt vad nämnder och styrelser som drabbas ska göra när en personuppgiftsincident upptäcks. Ett gott dataskydd innefattar att man också reflekterar över sina incidenter så man lär sig för framtiden. Därför ska de framtagna rutinerna också innefatta efterarbete inklusive uppföljning.

Upprätta en handlingsplan för de fall en personuppgiftsincident inträffar och dokumentera alla personuppgiftsincidenter, även de som inte måste anmälas till Datainspektionen.

- ☐ Är det tydligt vem som har det övergripande ansvaret för personuppgiftsincidenter?
- ☐ Är det tydligt vilket ansvar varje medarbetare har (t.ex. att anmäla incidenter) och hur de ska hantera det ansvaret?
- ☐ Klarar vi att anmäla incidenter inom 72 timmar till Datainspektionen? Finns det tydliga rutiner hur vi ska göra?
- ☐ Är det tydligt i våra interna rutiner hur vi hanterar formkraven på anmälan? Datainspektionen förväntar sig ingen omfattande beskrivning eftersom sekretessen inte kan garanteras utan därför är det extra viktigt att man internt gör en mer omfattande dokumentation på incidenten.
- ☐ Har vi tydliga rutiner för dokumentation av inträffade incidenter? Följer vi upp dem på ett bra sätt?
- ☐ Har vi förmåga att underrätta drabbade registrerade? Hur ska vi göra detta? Finns tydliga rutiner?

***Tips!*** Vid incident har Datainspektionen blankett och instruktioner hur anmälan till dem ska gå till. Sydarkivera har tagit fram en checklista som kan användas när en personuppgiftsincident inträffar.

## IT-stöd

Det är väsentligt att ha en bra bild över vilka informationssystem och IT-stöd och manuella register som organisationen använder för att sedan se så de används rätt. Man behöver ha kontroll över hur personuppgifter används i befintliga IT-stöd och informationssystem eftersom all hantering i dem ska uppfylla kraven i dataskyddsförordningen.

Vilka IT-stöd och informationssystem och manuella register finns i organisationen? Lista de stöd som används. Lista dem gärna efter typer av informationssystem som används och vilka behov av anpassningar som kan finnas beträffande varje stöd.

- ☐ Systemstöd för ärendehantering, kundhantering, leveranshantering, ekonomihantering, medlemshantering, marknadsföring med mera.
- ☐ System för e-post, uppgifter och kalendrar
- ☐ IT-stöd för att skapa och underhålla egna webbplatser och intranät.
- ☐ Molntjänster och andra lagringstjänster.
- ☐ Appar och olika verktyg som tillhandahålls från externa webbplatser.

Det är viktigt med tydlighet i hur IT-stöden används. Man ska beskriva hur uppgifterna tas in ett system om de fördelas till andra system eller register. Det är viktigt att fundera över ändamål och laglig grund. Kan man använda uppgifterna i systemet i andra register? Är det samma ändamål, om inte måste man hitta ett berättigat ändamål för att återanvända uppgifterna i ett annat system/register. Har man ett bra inbyggt dataskydd ska delning av uppgifter från övergripande system till andra system och register ha retts ut så att ändamålet med behandlingen täcker alla delningar.

Det inbyggda dataskyddet aktualiseras fortlöpande i samband med nyanskaffningar av system, där organisationen bör välja IT-stöd som ger de bästa förutsättningarna för inbyggt dataskydd. Det handlar om en strävan efter att ständigt bli bättre. Man ska när man tar strategiska beslut väga in dels den senaste tekniska utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål och riskerna för fysiska personers rättigheter

och integritet. Inbyggt dataskydd handlar om att se till att personuppgifter hanteras riktigt, att man tar ansvar för personuppgifternas hantering samt hänsyn till de registrerades rättigheter. I samband med detta ska man också ta hänsyn till dataskydd som standard vilket innebär att man ska se till att personuppgifter inte behandlas i onödan.

Glöm inte bort de eventuella analoga register som används för att hantera personuppgifter. Det kan röra sig om register som finns i pärmar, hängmappar eller liknande.

***Tips!*** Utgå från organisationens systemlista eller om det saknas den systemlista som Sydarkivera har.

## Säkerhet inom dataskydd

Inbyggt dataskyddsarbete innebär att organisationen fortlöpande måste se över sin säkerhetshantering avseende personuppgifter så att integritet och sekretess kan hanteras och personuppgiftsincidenter förhindras. Hoten som måste avvärjas är många: intrång, manipulation, hackning, virus, kidnappning av datorer, oavsiktlig radering, stöld eller spioneri. Ju känsliga personuppgifter som hanteras, desto större krav ställs på säkerheten

Vid behandling av personuppgifter ska man se över vilken säkerhetsnivå som är lämplig i förhållande till risken av att behandla personuppgifter. Särskild hänsyn ska tas till risken för förstöring, förlust eller ändring och obehörigt röjande eller obehörig åtkomst.

Det finns olika sätt att hantera riskerna. Man kan använda till exempel använda pseudonymisering (kodning) och kryptering, kontinuitetsplanering, incidentrapportering och testa, undersöka och utvärdera åtgärderna för att får fram lämplig säkerhetsnivå. Man ska använda sig av både tekniska och organisatoriska åtgärder för att uppfylla kraven kring säkerhet kring dataskydd.

Följande checklista kan användas:

- ☐ Kan pseudonymisering eller kryptering användas av personuppgifter? Detta kan minska riskerna. Till exempel bör känsliga personuppgifter inte skickas i okrypterad e-post enligt Datainspektionen.

- ☐ Finns det en god förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos verksamhetssystem och andra IT-stöd? Klarar organisationen de grundläggande principerna?
- ☐ Finns det en god förmåga att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident? En god sådan förmåga är en positiv faktor om det blir fråga om att pröva sanktionsavgifter.
- ☐ Finns det ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet (görs fortlöpande säkerhetsanalyser)? Om inte bör detta finnas i styrdokument?
- ☐ Finns det regler om behörighetsbegränsning för anställda, konsulter med flera som behandlar personuppgifter så att användningen av personuppgifter begränsas till dem som verkligen behöver dem? Klarar organisationen de grundläggande principerna?
- ☐ Klarar organisationen kraven på konsekvensbedömningar och anmälan om personuppgiftsincidenter?

***Tips!*** Datainspektionen har tagit fram riktlinjer och vägledningar för när och hur konsekvensbedömning ska göras. Mall för riskanalys har tagits fram av Sydarkivera. När det gäller informationssäkerhet kan man få hjälp på https://www.informationssakerhet.se/

## Kärnverksamheterna

Kärnverksamheterna under nämnder/styrelser ska inventera och analyser sina personuppgiftsbehandlingar. Det är bra om dataskydds-samordnaren är behjälplig i det arbetet liksom i arbetet med att kartlägga processer och göra konsekvensbedömningar. Det är dock kärnverksamheterna som kan sin verksamhet om som måste ta det största ansvaret för arbetet eftersom de är de som vet vilken information de har och hur personuppgifterna hanteras samt hur processerna i verksamheten ser ut.

***Tips!*** Se till så att alla förvaltningar använder samma mall för registerförteckning, riskanalys och konsekvensbedömning. Om det finns ett system för processkartläggning inom organisationen se till att samtliga använder det.