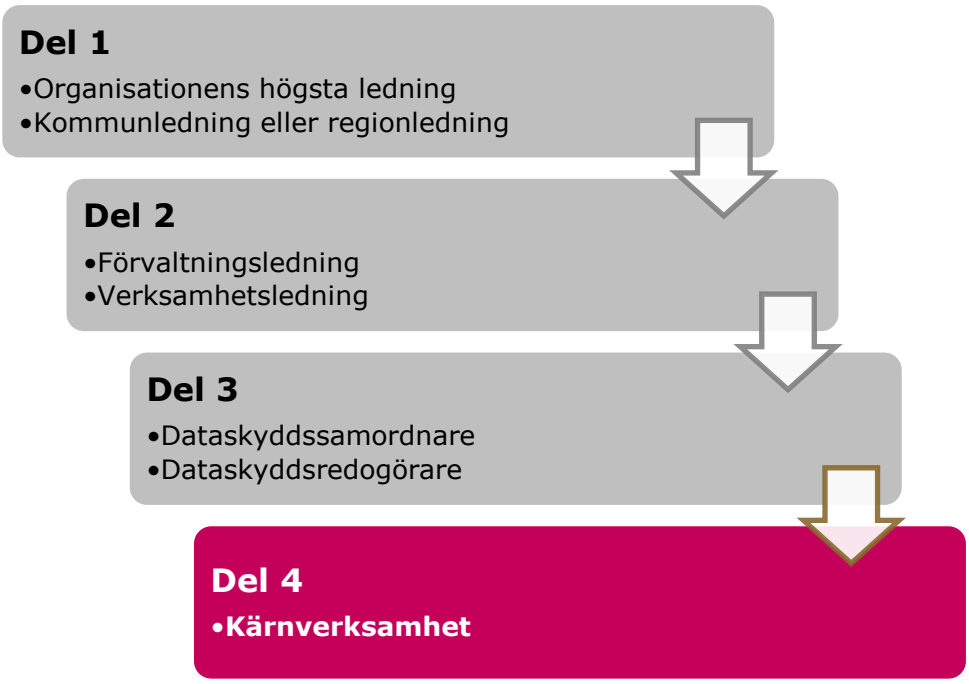
DATASKYDD (GDPR)
Del 4: Kärnverksamheterna



Om dokumentet

I det här dokumentet finns en sammanfattning av det som kärnverksamheterna behöver göra för att uppfylla dataskyddsförordningen som trädde ikraft 25 maj 2018. Målgruppen är chefer och handläggare som finns på kommunernas och regionernas förvaltningar. 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.

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.

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/

1. Personuppgiftsansvar

Varje myndighet är personuppgiftsansvarig (PUA) för sin verksamhetsinformation. Förvaltningsledningen ansvarar för att

informera nämnden/styrelsen om vad det innebär att de är personuppgiftsansvariga. Det är också nämnd/styrelse och ledning som ska se till att verksamheten vet vad som krävs av dem samt att det finns resurser att utföra uppdraget.

Tips! Det finns särskilda vägledningar för Organisationens högsta ledning/Kommunledning eller regionledning samt för Förvaltningsledning/verksamhetsledning.

2. Styrande dokument

Organisationens högsta ledning ska anta övergripande dataskyddspolicy och riktlinjer. Även andra styrande dokument på central nivå, och förvaltningsnivå, kan ha förändrats eller kompletterats med anledning av det nya regelverket.

Tips! Ta reda på vilka förändringar som berör din verksamhet. Fråga till exempel Dataskyddssamordnare eller dataskyddsredogörare på din förvaltning.

3. Individens rättigheter

Dataskyddsförordningen definierar bland annat de rättigheter som en registrerad person har. Styrelse/nämnd och ledningsgrupp ska vara informerade om rättigheterna och vad det ställer för krav på verksamheten.

Tips! Får verksamheten frågor som rör individens rättigheter kontakta i första hand förvaltningens dataskyddsredogörare och därefter den gemensamma dataskyddssamordnaren.

Tydliggör verksamhetens processer

I arbetet med dataskyddsförordningen är tydliga processer en mycket viktig framgångsfaktor. Verksamheten behöver ha kontroll över varje enskild behandling av personuppgifter, inte minst för att kunna säkerställa den registrerades alla rättigheter.

För att få det att fungera och slippa fundera vid varje förfrågan så måste man i verksamheten bygga upp arbetssätt som gör att dataskyddsförordningen efterlevs. Ett av sätten är att det finns tydliga processer. De är ett viktigt hjälpmedel tillsammans med tydliga rutiner. Genom att kartlägga processer och ha tydliga rutiner minskar risken för variationer i arbetssätt.

Utbildning av medarbetare inom verksamheten krävs för att upprätthålla kompetensen kring dataskydd. Ett bra sätt att utbilda är att låta medarbetare fortlöpande processkartlägga sin egen verksamhet. Det arbetssättet är lärande men medför också engagemang. Man blir också delaktig i att hitta lösningar i processkartläggningarna och det gör lösningarna mer hållbara.

1. Processer

Tydliga processer är en framgångsfaktor när det gäller att genomföra dataskyddsförordningen. Processer skapar ordning och reda och tydliga processer förbättrar effektiviteten.

Att komma igång:

- Har ni färdiga processbeskrivningar som ni arbetar utifrån så utgå från dessa.
- Ta reda på om kommunen/regionen eller förvaltningen har satt igång något samordnat arbete att delta i.
- Om det inte finns färdiga processer så börja med att titta på de processer med information som innehåller personuppgifter och som flödar igenom verksamheten. Lägg fokus på de viktigaste först.
- Använd de tillfällen som verksamheterna ändå träffas till att påbörja processkartläggningen om det är svårt att få tid till att boka separata möten för processkartläggning.

Vid processkartläggning:

- Fastställ hur arbetsprocessen ser ut. Se till att alla involveras och är överens.
- Vem kommer informationen från och vem ska den till?
- Inventera och dokumentera vilka personuppgifter ni hanterar:
    - Hur samlas de in?
    - Vilka data kommer in i processen:
        - I form av personuppgifter?
        - I form av personuppgiftstyper?
        - Vilka behandlingar sker personuppgifterna i?
        - Vilka IT-stöd används?
- Inventera och dokumentera vilka personuppgifter ni hanterar och till vem uppgifterna lämnas ut:
    - Vilka data kommer ut i processen:
        - I form av personuppgifter?
        - Vilka behandlingar sker personuppgifterna i?
        - Vilka IT-stöd används?
- Vilka ändamål med processen/behandlingarna finns och vilken är den lagliga grunden för den?
- Om man hittar oklarheter eller avvikelser under processarbetet så markeras detta. Detta arbetas vidare med och förbättringar genomförs i samband med det arbetet.
- Alla oklarheter och avvikelser som hittas sätts också upp på en åtgärdslista för att man ska veta vad det är som måste lösas så kan man bocka av allt eftersom saker löses.

Tips! Använd en enkel modell för processkartläggning om ni inte har IT-stöd. Börja med post-it-lappar i olika färger för att visa vilka processer ni har och hur de förhåller sig till de olika frågorna ni vill ha svar på. Det går lika bra att beskriva processer i text som att rita flödesscheman.

2. Informationsplan/dokumenthanteringsplan

Alla myndigheter måste ha en uppdaterad dokumenthanteringsplan/ informationshanteringsplan för att uppfylla de lagkrav som finns för myndigheter i offentlighets- och sekretesslagen, tryckfrihetsförordningen, arkivlagen och dataskyddsförordningen. En informations-hanteringsplanplan är en förteckning över en myndighets

information, både analog och digital. Planen talar om hur informationen ska hanteras och var den hittas.

Sydarkivera genomför tillsammans med verksamheter workshops där man kartlägger informationsflöden och klassar informationsmängder. Resultaten från dessa kan användas i olika sammanhang av verksamheterna till exempel upphandling, driftsättning och förteckning över var känsliga uppgifter finns.

Tips! Sydarkivera har en mall för dokumenthanteringsplan/ informations-hanteringsplan om verksamheten saknar en och som man kan utgå ifrån. Underlag från workshops där informationsklassning gjorts inom olika verksamhetsområden finns att tillgå om man kontaktar Sydarkivera.

3. IT-stöd

Det inbyggda dataskyddet ska finnas med i hela livscykeln för IT-stödet. Inbyggt dataskydd handlar om att se till att personuppgifter hanteras riktigt, att man tar ansvar för personuppgifternas hantering samt tar 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.

Kartlägg vilka IT-stöd som finns i verksamheten

- Är det några IT-stöd som endast används i er verksamhet?
- Finns alla IT-stöd med på de övergripande systemlistorna för hela organisationen?
- Använder sig verksamheten av molntjänster eller externa tjänster?
- Använder sig verksamheten av sociala media?
- Använder sig verksamheten av olika Appar till telefoner, surfplattor eller liknande.

När det finns en lista över de IT-stöd som verksamheten använder så är det viktigt att för varje IT-stöd fundera över:

- Hur hanteras personuppgifter?
- Hur fungerar det med säkerheten?
- Går det att uppdatera, rensa och underhålla IT-stödet?

- Hur ser behörighetsstyrningen av IT-stödet ut?
- Vad händer om något blir fel?

Förvaltningens dataskyddsredogörare ska vara delaktig i arbetet och man ska rapportera till organisationens övergripande dataskyddsamordnare vad man kommit fram till inom verksamheten.

Tips! Utgå från organisationens systemlista.

4. 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 är många och måste avvärjas ex. intrång, manipulation, hackning, virus, kidnappning av datorer, oavsiktlig radering, stöld eller spionerі. Ju fler känsliga personuppgifter som hanteras, desto större krav måste ställas 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 ska använda sig av både tekniska och organisatoriska åtgärder för att uppfylla kraven kring säkerhet kring dataskydd.

Organisatoriska åtgärder innebär att det hos verksamheten ska finnas rutiner och processer som minimerar mänskliga misstag samt att lämpliga åtgärder vidtas om något händer.

- Skapa anvisningar och instruktioner för personalen som är konkreta och lätta att förstå
- Höj säkerhetsmedvetandet genom att hålla utbildning regelbundet
- Kontrollera regelbundet att anvisningar och rutiner följs

Tekniska åtgärder för dataskydd kan sammanfattas enligt följande:

- Autentisering
- Behörighetsstyrning
- Åtkomstkontroll (loggar och logguppföljning)
- Kommunikationssäkerhet
- Skydd mot intrång och skadlig kod
- Säkerhetskopiering
- Utplåning

Tips! När det gäller informationssäkerhet kan man få hjälp på https://www.informationssakerhet.se/

5. Konsekvensbedömning

Syftet med konsekvensbedömning är att identifiera och hantera risker innan de uppkommer samt bedöma proportionaliteten hos behandlingen av personuppgifter.

Konsekvensbedömningar ska göras när behandlingen av personuppgifter leder till för hög risk för fysiska personers rättigheter och friheter.

Kriterier och exempel på när en konsekvensbedömning ska göras finns hos datainspektionen på deras webb men det är viktigt att förvaltningen gör en egen bedömning om det krävs.

Konsekvensbedömningen är en process för att

- ta reda på vilka risker som finns med att behandla personuppgifter
- ta fram rutiner och åtgärder för att bemöta dessa risker
- visa att man uppfyller dataskyddsförordningens krav.

Man måste inte alltid genomföra en regelrätt konsekvensbedömning utan ibland räcker det med en riskanalys:

1. Analysera vilka risker behandlingen av personuppgifter kan innebära och föreslå lämpliga säkerhetsåtgärder.
2. Dokumentera det man kommer fram till, så att man kan visa att förordningen följs.
3. Utifrån riskanalysen beslutar man om man behöver gå vidare och göra en konsekvensbedömning.

Obs! I tveksamma fall bör man alltid göra en konsekvensbedömning.

Tips! Utgå från Datainspektionens Förteckning över när man ska göra konsekvensbedömning samt de riktlinjer som finns till. Ta också hjälp av organisationens övergripande dataskyddssamordnare om det behövs.

Registerförteckning och dokumentation

Förvaltningen ska föra en registerförteckning över samtliga sina personuppgiftsbehandlingar. Det är förvaltningens dataskydds-redogörare som hanterar det praktiska arbetet kring registerförteckningen. Det är viktigt att verksamheten rapporterar alla behandlingar och eventuella förändringar som sker när det gäller personuppgiftsbehandlingar till dataskyddsredogöraren.

Ta del av de rutiner och instruktioner som förvaltningsledningen tagit fram så att det inte blir ett engångsarbete utan att registerförteckningen kan hållas kontinuerligt uppdaterad. Se också till att ni har den dokumentation som krävs enligt rutiner och instruktioner för att visa att ni följer dataskyddsförordningen.

Incidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.

Exempel:

- diskriminering,
- identitetsstöld,
- bedrägeri,
- skadlig ryktesspridning

- finansiell förlust
- brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har:

- blivit förstörda
- gått förlorade på annat sätt
- kommit i orätta händer.

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

Om en personuppgiftsincident sker har varje medarbetare inom en verksamhet ett tydligt ansvar för att anmäla detta omedelbart enligt de rutiner som tagits fram övergripande för organisationen.

Tips! Om en personuppgiftsincident sker så kontaktas omedelbart förvaltningens dataskyddsredogörare och dataskyddssamordnare. Sydarkivera har en checklista hur man ska tänka i samband en personuppgiftsincident som man kan ta hjälp av.