Dataskyddsombudets granskningsrapport av dataskyddsarbete 2023

2024-01-25

Författad av
Camilla Eriksson
Dataskyddsombud

Med stöd av
Sofia Pinheiro Chipelo
Dataskyddssamordnare

Inledning

Dataskyddsombudet (DSO) har 2023 genomfört en granskning av dataskyddsarbete. Samtliga organisationer har granskats genom en enkät.

Granskningen 2023 har fokuserat på sex olika huvudområden:

- Organisera arbetet/strategi
- Rutiner/dokumentation/processer
- Utbildning/medvetenhet/följsamhet och kultur
- Register över personuppgiftsbehandlingar
- Dataskyddsorganisation
- Dataskyddsombud

Detta har skett som en del av dataskyddsombudets övervakande arbete 2023 och med avsikt till 5års tillsynsplanen[1]. Granskningen har genomförts på liknande sätt hos Sundsvall, Timrå och Ånge kommuns nämnder, bolag och förbund som använder sig av DSO tillhandahållet av Sundsvalls kommun. Granskningsarbetets omfattning berodde på organisationens verksamhet, antal registrerade (anställda, kunder, medborgare), hur många personuppgifter som behandlas, hur stor andel som är känsliga eller skyddsvärda personuppgifter. På grund av det hade granskningen uppdelats på tre olika nivåer: liten, mellan och stor granskning. Granskningens syfte är att kontrollera hur Personuppgiftsansvariga (PUA) arbetar strategiskt med dataskyddsfrågor samt hur det systematiska arbetet med dataskydd är organiserat hos PUA. Det övergripande resultatet av granskningen har sammanfattats i diagram i syftet att skapa en snabb överblick över de 33 organisationernas mående och mognad som en grupp. Dataskyddsombudets rekommendationer har som grund i att GDPR ger Dataskyddsombudet befogenheten att informera samt ge råd till den PUA och de anställda som behandlar personuppgifter.

[1] Se ”Tillsynsplan Dataskyddsarbete 2023–2027”

Organisationer som ingick i tillsynen

Sundsvall

Organisation	Namn	Typ av granskning
Bolag	Mitthem	Mellangranskning
Bolag	MittSverige Vatten och Avfall AB	Mellangranskning
Bolag	Servanet	Mellangranskning
Bolag	SKIFU AB	Mellangranskning
Bolag	Stadsbacken AB	Liten granskning
Bolag	Sundsvall Timrå Airport	Mellangranskning
Bolag	Sundsvalls Elnät AB	Mellangranskning
Bolag	Sundsvalls Energi AB	Mellangranskning
Bolag	Sundsvalls Hamn AB	Liten granskning
Bolag	Sundsvalls Oljehamn AB	Liten granskning
Förbund	Medelpads räddningsförbund	Mellangranskning
Nämnd	Barn- och utbildningsnämnden	Stor granskning
Nämnd	Individ- och arbetsmarknadsnämnden	Stor granskning
Nämnd	Kommunstyrelsen	Stor granskning
Nämnd	Kultur- och Fritidsnämnden	Mellangranskning
Nämnd	Lantmäterinämnden	Liten granskning
Nämnd	Miljönämnden	Mellangranskning
Nämnd	Stadsbyggnadsnämnden	Mellangranskning
Nämnd	Valnämnden	Liten granskning
Nämnd	Vård- och omsorgsnämnden	Mellangranskning
Nämnd	Överförmyndarnämnden	Liten granskning

Timrå

Organisation	Namn	Typ av granskning
Bolag	Timråbo	Mellangranskning
Nämnd	Barn- och utbildningsnämnden	Stor granskning
Nämnd	Kommunstyrelsen	Stor granskning
Nämnd	Kultur- och tekniknämnden	Stor granskning
Nämnd	Miljö- och byggnadsnämnden	Mellangranskning
Nämnd	Socialnämnden	Stor granskning
Nämnd	Valnämnden	Liten granskning

Ånge

Organisation	Namn	Typ av granskning
Bolag	Ånge Energi AB	Mellangranskning
Bolag	Ånge Fastighets och Industri AB	Mellangranskning
Nämnd	Kommunstyrelsen	Stor granskning
Nämnd	Myndighetsnämnden	Stor granskning
Nämnd	Valnämnden	Liten granskning

Organisera arbetet/strategi

Dataskyddsarbetet ska vara en integrerad del i organisationens verksamhetskultur. Hela dataskyddsförordningen förutsätter att en rad arbetsinsatser behöver genomföras och därefter kontinuerligt underhållas. Upprättande av grundläggande dokumentation (riktlinjer, styrdokument, osv.) är ett övergripande beslut som fattas av kommunen men införande av processer relaterade till GDPR och ökning av kunskapsnivån är respektive PUA:s ansvar. Det måste därför skapas övergripande förutsättningar för att dataskyddarbetet ska kunna genomföras.

Av granskningen framgår det att de flesta organisationer har dataskyddsarbetet inbyggt i de övriga verksamhetsprocesserna. Valnämnden köper dataskydd som en tjänst av Sundsvalls Kommun men har ingen beslutad verksamhetsplan för dataskyddarbetet.

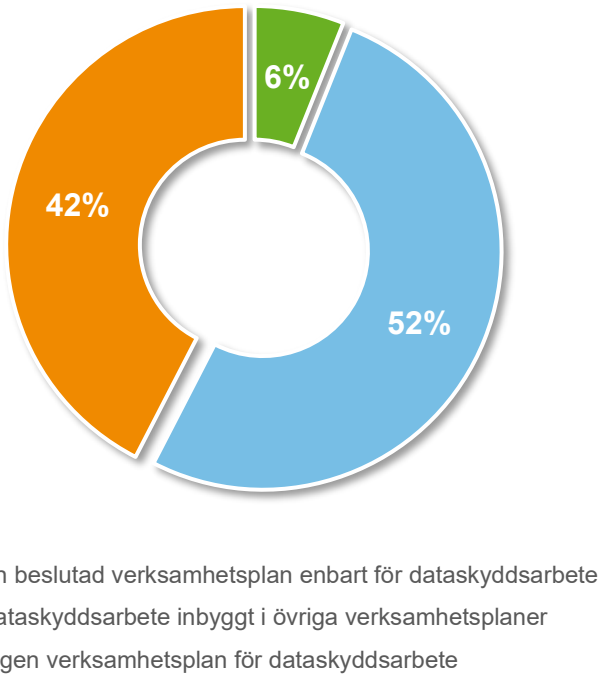

Diagram 1

Dataskyddsombudets rekommendation

Rekommendationen är att det tas fram en verksamhetsplan för dataskyddsarbetet som anpassas efter verksamhetens behov, ambitionsnivå och baseras på vägledning från Dataskyddsombudet. Att skapa en handlingsplan handlar om att, på ett övergripande sätt, beskriva hur organisationen ska säkra att man lever upp till dataskyddslagstiftningen. I handlingsplanen kan det framgå vilka mål organisationen sätter för sig själv under 2024.

Rutiner/dokumentation/processer

Strukturerad planering av dataskyddsarbete underlättar uppföljning och implementering av styrdokument och riktlinjer samt att det kan användas som ett verktyg för självskattning inom kontrollramverk för dataskyddsefterlevnad.

Av granskningen framgår det att få organisationer arbetar processbaserat med dataskydd vilket stämmer för Valnämnden.

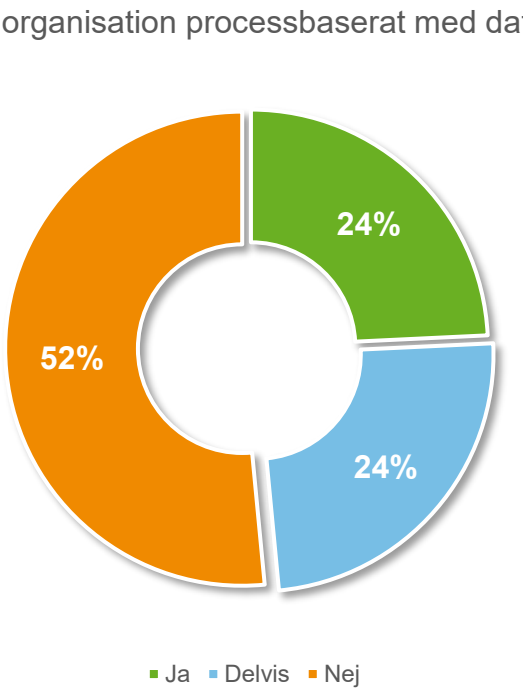

Diagram 2

Dataskyddsombudets rekommendation

För att skapa struktur och framförhållning är det viktigt att ha koll på vad som ska göras under året. Utifrån verksamhetsplanen och ambitionsnivån kan årshjulet med aktivitetsplanering under kalenderåret utformas. Ett förslag till årshjul finns framtaget av Dataskyddsombudet.

Som aktivitetsförslag rekommenderas det att stort fokus under det första halvåret ska läggas på registerförteckning över personuppgiftsbehandlingar och att den ska vara uppdaterad. Regelbunden leverantörsuppföljning är ett annat mål som kan anses vara viktig under 2024. För dataskydd innebär det att inventera alla personuppgiftsbiträden, granska och uppdatera PUB-avtal och kontrollera att konsekvensbedömningar (DPIA) har utförts för de verksamhetskritiska leverantörerna. Detta ska även bättre byggas in i processen för framtida upphandlingar.

Utbildning/medvetenhet/följsamhet och kultur

Det är PUA:s ansvar att se till att medarbetaren ska ha rätt kompetens utifrån deras roll. För att kunna uppfylla den ansvarsskyldigheten är det även viktigt att dokumentera och kunna visa upp att alla anställda som hanterar personuppgifter har fått relevant utbildning i dataskyddsfrågor. Utbildning är en förutsättning för att se till att de rutiner och processer framtagen av verksamheten är kända av alla anställda och efterlevs. Exempelvis om anställda inte vet vad en personuppgiftsincident är kan en sådan inte heller anmälas.

Av granskningen framgår det ett dåligt resultat på dokumentation av utbildningsinsatser:

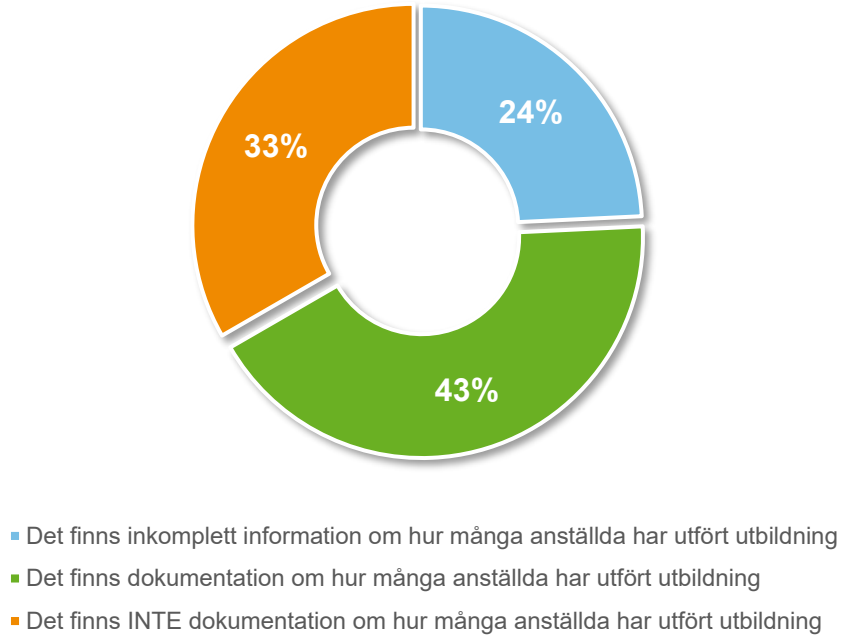

Diagram 3

Det har även konstaterats vissa brister vid utbildning av nyanställda hos några verksamheter:

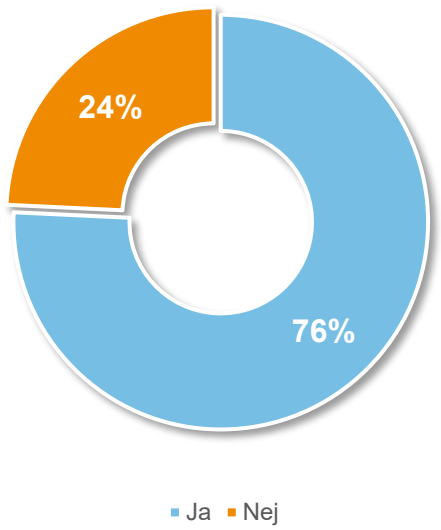

Diagram 4

För Valnämnden får förtroendevalda information om GDPR varje mandatperiod. Det fanns då en pågående insats med Nanolearning utbildning för informationssäkerhet och det finns dokumenterat i form av statistik från Nanolearning.

Dataskyddsombudets rekommendation

Valnämnd har en väldigt liten verksamhet med ett mycket viktigt uppdrag. Det är därför extra viktigt att se till att alla medarbetare får kunskap och information om dataskyddsförordningen. Informationsinsatserna bör vara mätbara och återrapporteras till nämnd.

En rollanpassad utbildningsplan bör tas fram. En uppdelning kan vara att medarbetare går den kortare digital Nanolearning utbildningen och de som har ledande roller genomgår en fysisk utbildning som är mer utökad lite under 2024. Det bör också vara mätbart vilka som har gått någon utbildning inom området.

Register över personuppgiftsbehandlingar

Att PUA ska ha en registerförteckning över personuppgiftsbehandlingar är en skyldighet enligt GDPR. En fullständig registerförteckning är en förutsättning för ett godkänt dataskyddsarbete.

Dataskyddsombudets rekommendation

För att underlätta den kontinuerlig arbetet med registerförteckningen kan den ses över och även kopplas till informationshanteringsplanen.

Dataskyddsorganisation

Enligt dataskyddsförordningen ska den PUA tillhandahålla dataskyddsombudet de resurser som krävs för att fullgöra dataskyddsombudets uppgifter. Varje PUA bör därför utse personer inom den dagliga verksamheten som ansvarar för dataskyddsarbetet samt organisera deras arbete på ett sådant sätt att krav i dataskyddsförordningen uppfylls. Av granskningen framgår det att flera organisationer saknar en dataskyddsorganisation med tydliga roller och arbetsuppgifter:

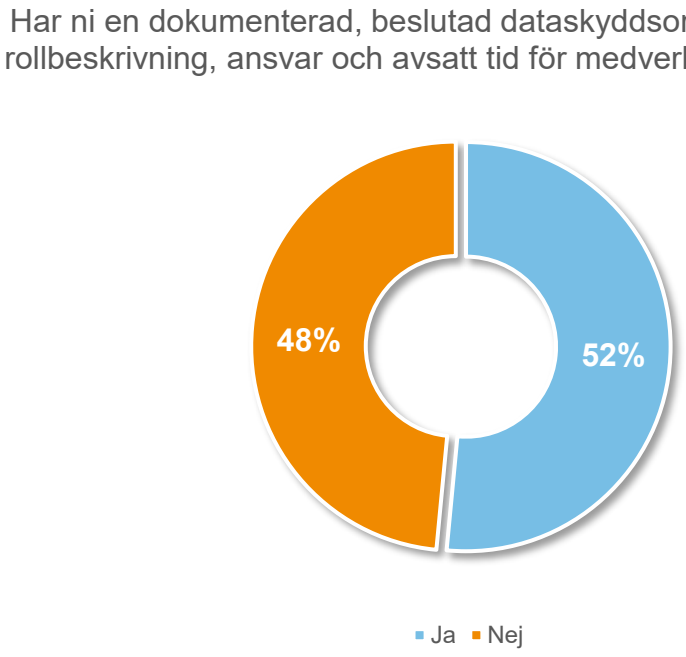

Diagram 5

Dataskyddsombudets rekommendation

Dataskyddsombudet konstaterar att det finns en grundläggande dataskyddsorganisation för Valnämnden i form av en utsedd dataskyddsamordnare som kan leda och samordna dataskyddsarbetet och agera kontaktperson. Dataskyddssamordnare är en stödfunktion och beskrivningen på rollen samt arbetsuppgifter kan produceras av dataskyddsombudet. Ett

underlag för hur mycket tid av sin tjänst som dataskyddssamordnare har till sitt förfogande bör dock tas fram. För ett mer effektivt arbetssätt måste dataskyddssamordnare ha stöd från beslutsfattare samt befogenhet att själv fatta beslut inom sina ansvarsområden. Det kan exempelvis handla om att kunna förändra rutiner och arbetssätt.

Sundsvalls Kommun har en utsedd kommunövergripande dataskyddssamordnare som har som uppgift att hålla direktkontakt med DSO och övriga dataskyddssamordnare för respektive verksamheter för Sundsvall, Ånge och Timrå.

Dataskyddsombud

Under våren 2023 tillsattes ett nytt Dataskyddsombud, Camilla Eriksson, som har arbetet under året med att informera och utbilda alla nämnder och ledningsgrupper i kommunerna. Syftet är att alla ska får samma information samt att alla ska få information vilket inte har skett regelbundet sedan 2018 när GDPR trädde i kraft.

Dataskyddsombudets arbete och stöd i dataskyddsfrågor kommer att ges främst från dataskyddssamordnare Sofia Pinheiro Chipelo samt Dataskyddsombudet Camilla Eriksson. Dataskyddsombudsfrågor kan likväl stödjas av dataskyddssamordnare då tanken är att det inte ska vara personberoende vilket är ett nytt arbetssätt. Tidigare har det varit personberoende på ett sätt som gjort att vissa perioder, exempelvis under sommaren, har det inte funnits något stöd alls i dataskyddsombudsfrågor. Den förändringen påbörjades under 2023 och kommer fortsätta implementeras framåt.

En femårig tillsynsplan har tagits fram för att skapa ett systematiskt och långsiktigt tillsynsarbete inom dataskyddet där syftet under de första fem åren är att optimera tillsynsmodellen. Under perioden kommer det ske förändringar och förbättringar på tillsynen och rapporteringen för att göra arbetet så bra som möjligt för verksamheterna.

2023 avslutas med arbetet att göra sammanställningar av svaren på tillsynen som gjordes på 33 PUA samt skriva rapporterna.

IMYs granskning av dataskyddsombudens roll och ställning

Under 2023 har IMY inlett en tillsyn för att undersöka dataskyddsombudens roll och ställning och den 11 oktober rapporterad IMY sina iakttagelser till EDPB. Ett 50-tal verksamheter har granskats där ett 30-tal tillhör offentlig sektorn. I sin rapportering har IMY identifierat fyra problemområden samt lämnat förslag på möjliga lösningar. Bland annat konstateras att flera Dataskyddsombud har andra uppgifter/roller utöver rollen som Dataskyddsombud vilket kan innebär att en intressekonflikt kan uppstå. IMY föreslår att termen ”intressekonflikt” förtydligas av EDPB. Tiden som dataskyddsombuden ägna åt kompetensutveckling varierar drastisk i de olika verksamheter och vart femte ombud anser att de inte får tillräckligt med utbildning och kompetensutveckling. IMY anser då att detta tyder på att det finns ett behov för närmare vägledning i den här frågan. Mängden resurser som görs tillgänglig för

dataskyddsombuden varierar. Detta påverkas även om verksamheten i frågan hantera stora mängder personuppgifter och att flera dataskyddsombuden har andra arbetsuppgifter eller arbetar inte heltid med dataskyddsfrågor. Tillsynen visar att organisationer har olika uppfattningar om vad som ska ingå i dataskyddsombudsuppdrag.

Dataskyddsombudets rekommendation

Rekommendationen är att nämnden samt förvaltningsledning ska kalla till möten i början av året vartannat år där rapportering sker tillsammans med respektive dataskyddssamordnare.

Bilaga 1

Sammanställning av de frågor som ställdes till de 33 granskade organisationer[2] som ligger till underlag av diagram i rapporten.

Organisera arbetet/strategi

Diagram 1

”Finns det en beslutad budget och/eller verksamhetsplan för dataskyddsarbetet som gäller för år 2023?”	Antal	Procent
Har en beslutad verksamhetsplan enbart för dataskyddsarbete	2	6%
Har dataskyddsarbete inbyggt i övriga verksamhetsplaner	17	52%
Har ingen verksamhetsplan för dataskyddsarbete	15	42%

Rutiner/dokumentation/processer

Diagram 2

”Arbetar er organisation processbaserat med dataskyddet?”	Antal	Procent
Ja	8	24%
Nej	17	52%
Delvis	8	24%

Utbildning/medvetenhet/följsamhet och kultur

Diagram 3

”Finns det dokumentation över vilken utbildning som anställda har fått om GDPR?	Antal	Procent
Det finns inkomplett information om hur många anställda har utfört utbildning	8	24%
Det finns dokumentation om hur många anställda har utfört utbildning	14	42%
Det finns INTE dokumentation om hur många anställda har utfört utbildning	11	33%

Diagram 4

”Får nyanställda utbildning om GDPR?”	Antal	Procent
Ja	25	76%
Nej	8	24%

[2] Se sida 3 för vilka organisationer som ingick i granskningen

Dataskyddsorganisation

Diagram 5

”Har ni en dokumenterad, beslutad dataskyddsorganisation, med rollbeskrivning, ansvar och avsatt tid för medverkande personer?”	Antal	Procent
Ja	17	52%
Nej	16	48%