

Dataskyddsombudets Årsrapport 2025

Innehåll

1. Bakgrund	1
2. Sammanfattning och kontrollpunkter	1
3. Uppföljning av tidigare rekommendationer	2
4. Fasta kontrollpunkter	2
4.1 Personuppgiftsincidenter	2
4.2 Personuppgiftsbiträdesavtal	3
5. Fördjupad kontroll 2026	4
6. DSOs rekommendationer	4

1. Bakgrund

Dataskyddsförordningen (The General Data Protection Regulation EU 2016/679) trädde i kraft som lag i Sverige den 25 maj 2018. Dataskyddsförordningen kompletterades med nationell lagstiftning i form av Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning som trädde i kraft vid samma datum. Tillsammans benämnda dataskyddslagstiftningen. Syftet med dataskyddsförordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (20132/C 362/02).

Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU. Enligt dataskyddsförordningen är varje nämnd inom Region Västerbotten ansvarig för att verksamheten följer dataskyddslagstiftningen. Det innebär att nämnder behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter. Varje nämnd har utsett ett Dataskyddsombud ("DSO"). DSO har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå i enlighet med beskrivning av DSO ställning och uppgifter i art 38 och 39 i dataskyddsförordningen

Denna årsrapport utgör rapporten till den personuppgiftsansvariges högsta förvaltningsnivå, i enlighet med artikel 38.3 i dataskyddsförordningen.

Årsrapporten för 2025 har blivit försenad till februari 2026 på grund av oplanerade frånvaro och hög arbetsbelastning.

2. Sammanfattning och kontrollpunkter

I egenskap av ert Dataskyddsombud, fortsättningsvis kallad DSO, lämnas följande årsrapport.

Under året har DSO genomfört utbildningar under december 2025 för nätverket för personuppgiftshandläggare. Utöver detta har det även genomfört informationsinsatser i mindre grupperingar i särskilda frågor.

DSO har involverats i frågor från verksamheten och lämnat råd och stöd i ärendeberedning, avtalsskrivande och konsekvensbedömningar.

Undertecknad blev i januari 2025 utsedd som Dataskyddsombud för Regionstyrelsen, Hälso- och sjukvårdsnämnden och Regionala utvecklingsnämnden. I mars 2025 utsågs undertecknad som Dataskyddsombud för Patientnämnden. I september 2025 utsågs undertecknad som Dataskyddsombud för Folkhögskolestyrelsen. Kontrollerna genomförs därför för dessa nämnder gemensamt i denna årsrapport.

Nedan redogörs för den genomförda granskningen, slutsatser samt rekommendationer gällande de kontroller som genomförts.

3. Uppföljning av tidigare rekommendationer

I årsrapport från 2022 och 2023 har tidigare Dataskyddsombud återkommande lämnat rekommendationer att nämnderna ska arbeta för att säkerställa att följande genomförs:

- Registerförteckna samtliga personuppgiftsbehandlingar.
- Utse personuppgiftshandläggare i enlighet med riktlinjer.
- Höja kunskapsnivån gällande delvis rapportering av personuppgiftsincidenter men även generellt gällande GDPR och att en plan för utbildning rekommenderas.
- Ta fram rutiner för dokumentationen av personuppgiftsincidenter, tredjelandsoverföring och konsekvensbedömningar.

Under 2024 skrevs ingen rapport.

4. Fasta kontrollpunkter

4.1 Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter. Incidenter vara avsiktlig eller oavsiktlig. Om det inte är osannolikt att incidenten innebär en risk för den enskildes fri- och rättigheter ska incidenten inom 72 timmar anmälas till Integritetsskyddsmyndigheten (IMY).

Enligt Region Västerbottens rutin ”Rapportering och utredning av personuppgiftsincidenter” ska personuppgiftsincidenter diarieföras. Detta oavsett om personuppgiftsincidenten ska anmälas till IMY eller inte.

DSO har med hjälp av informationssäkerhetsstrateg gjort sökningar i diarieföringssystemet Platina för att få fram följande underlag. Sökningen har gjorts för perioden 1 december 2024 till 31 november 2025, under denna period har det diarieförts följande antal rapporter om personuppgiftsincidenter:

- Hälso- och sjukvårdsnämnden: 30 ärenden registrerade.
- Regionstyrelsen: 4 ärenden registrerade.
- Regionala utvecklingsnämnden: Inga ärenden registrerade.
- Folkhögskolestyrelsen: Inga ärenden registrerade.
- Patientnämnden: Inga ärenden registrerade.

Som jämförelse diariefördes för perioden 1 december 2023 till 31 november 2024 följande antal rapporter om personuppgiftsincidenter:

- Hälso och sjukvårdsnämnden: 54 ärenden.
- Regionstyrelsen: 6 ärenden.
- Regionala utvecklingsnämnden: 2 ärenden.
- Folkhögskolestyrelsen: Inga ärenden
- Patientnämnden: Inga ärenden.

Skillnaden mellan 2024 och 2025 är 28 ärenden, vilket är en kraftig minskning. Om detta innebär att antalet personuppgiftsincidenter sjunkit eller om färre incidenter diarieförts är

svårt för DSO att avgöra. Det har inom ramen för nätverket för personuppgiftshandläggare inkommit information om att dokumentationsriktlinjerna är svåra att förstå och inte alltid väl anpassade till verksamhetens utformning och behov.

I tidigare rapporter har bl.a. Regionala utvecklingsnämnden angett att de haft bristande kunskap kring hanteringen av personuppgiftsincidenter vilket kan vara en orsak till att inga incidenter är diarieförts.

DSO har under året haft kontakt med flertalet personuppgiftshandläggare för att ge råd och information i bedömningen av enskilda personuppgiftsincidenters allvar. Detta delvis utifrån att för vissa handläggare är hanteringen av personuppgiftsincidenter sällan uppgifter och delvis utifrån gränsdragningar om dataskyddslagstiftningen alls blir tillämplig på avvikelser. DSO har även varit i kontakt med verksamheter där det finns etablerade och utifrån DSOs bedömning välfungerade rutiner för att hantera och dokumentera incidenter utifrån verksamhetens storlek och organisation och behovet snarare har varit i återkommande utbildning eller för att stödja i framtagande av olika lokalt anpassade mallar.

Det som övergripande framkommer när DSO har kontakt med både verksamhetschefer, chefsassistenter, personuppgiftshandläggare och övrig personal är en önskan om ytterligare utbildning och då särskilt i frågor där annan lagstiftning ska vägas tillsammans med dataskyddslagstiftningen.

Det är för DSO tydligt att samtliga nämnden behöver återkommande arbeta med utbildning av personal med fokus på arbetsledande funktioner i flera led samt att se över sina rutiner för att diarieföra personuppgiftsincidenter så att dessa är tydliga och anpassade för verksamheten. Då diarieföring sker centralt behöver dessa rutiner även förankras med personal inom registratur.

4.2 Personuppgiftsbiträdesavtal

Det finns i art 28 dataskyddsförordningen krav på personuppgiftsbiträdesavtal (PUB-avtal) ska tecknas innan en behandling påbörjas. Enligt de rättsliga principerna i art 5 dataskyddsförordningen ska nämnderna utifrån principen om ansvarsskyldighet kunna visa hur de lever upp till kraven som ställs i dataskyddsförordningen. I en så stor organisation som Region Västerbotten är därmed sökbarhet avgörande och diarieföring en förutsättning för att denna princip ska kunna efterlevas.

Utöver personuppgiftsincidenter så har DSO därmed gjort stickprov kopplat till om upprättade PUB-avtal är diarieförts. I likhet med kontrollen av personuppgiftsincidenter är kontrollen riktad på diarieföring då det saknas möjlighet för DSO att veta om ett PUB-avtal tecknats eller inte. I årets rapport har DSO valt att titta på fem av Regionstyrelsens teknikkomponenter. DSO har med stöd av informationssäkerhetsstrateg gjorts sökningar efter aktuella PUB-avtal i både diarieföringssystemet Platina och i Avtalsdatabasen.

Följande fem teknikkomponenterna, här benämnda utifrån hur de är registrerade i Avtalsdatabasen, har kontrollerats;

- Platina (diarieföring)
- System Visual (arkivering)
- Whistlelink (Visselblåsarfunktion)
- Personec P/Visma Enterprise (HR-system)

- Tidomat (tidsredovisning)

Av dessa saknar tre diarieförda personuppgiftsbiträdesavtal; Platina, System Visual och Tidomat. DSO ser det faktum att vissa centrala system inte har diarieförda PUBA som allvarligt. Det behöver finnas tydliga rutiner för hur avtal ska diarieföras så att dessa blir sökbara. Dessa rutiner behöver även följas upp särskilt för centrala system.

DSO uppmanar samtliga nämnder att göra återkommande uppföljningar av system för att kontrollera att PUB-avtalen motsvarar den funktionalitet som systemet har samt säkerställa att PUB-avtalet diarieförts korrekt.

5. Fördjupad kontroll 2026

Inför kommande år avser DSO att återigen granska diarieföringen av personuppgiftsincidenter och av PUB-avtal i centrala diarieföringssystem.

Den 17 februari 2025 publicerade Integritetsskyddsmyndigheten en vägledning och praktisk guide för konsekvensbedömningar tillsammans med mallar för både konsekvensbedömning och tröskelanalys.

En konsekvensbedömning är en pågående och dokumenterad process som hjälper personuppgiftsansvariga att följa dataskyddslagstiftningen. Processen behöver enbart göras vid behandlingar av personuppgifter som kan leda till höga risker (högriskbehandlingar). Det är inte en engångsaktivitet med ett tydligt avslut utan en kontinuerlig process. Processen ger ett stöd i att bedöma risker med en planerad behandling och avgöra om riskerna är proportionerliga i förhållande till syftet med behandlingen. En väl utförd och dokumenterad konsekvensbedömning är en viktig del i att följa dataskyddsförordningen och visa detta.

I en konsekvensbedömning ska även DSO rådfrågas enligt art 35 punkt 2 dataskyddsförordningen. DSO avser att under 2026 göra kontroller för hur personuppgiftsansvariga nämnder arbetar för att strukturerat få in arbetet med konsekvensbedömningar i sin verksamhet.

6. DSOs rekommendationer

DSO har lämnat vissa rekommendationer under kontrollpunkterna som granskats ovan. Utöver dessa riktade rekommendationer vill DSO även lyfta de generella rekommendationer som gjorts tidigare år som även tas upp under punkt 3.

Vidare ser DSO att det finns ett fortsatt behov av återkommande utbildningstillfällen för verksamhetschefer och anställda i arbetsledande ställning om dataskyddslagstiftningen. Detta bör särskilt förenas med information om t.ex. Förvaltningslagen, Patientdatalagen och Biobankslagen om dessa påverkar dataskyddslagstiftningens tillämpning i den aktuella verksamheten.