

Juridik och säkerhet  
Dataskyddsombud  
Region Västerbotten

## Dataskyddsombudets årsrapport 2022

# Innehåll

<b>Dataskyddsombudets årsrapport 2022</b>	<b>1</b>
<b>1. Bakgrund</b>	<b>3</b>
<b>2. Sammanfattning och kontrollpunkter</b>	<b>3</b>
<b>3. Uppföljning av tidigare rekommendationer</b>	<b>3</b>
Registerförteckning	4
Personuppgiftshandläggare	4
Personuppgiftsincidenter	5
<b>4. DSOs rekommendationer</b>	<b>6</b>

# 1. Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen 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. 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:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

I enlighet med artikel 38.3 i dataskyddsförordningen ska DSO rapportera om dataskyddsarbetet till den personuppgiftsansvariges högsta förvaltningsnivå, vilket sker genom denna årsrapport.

# 2. Sammanfattning och kontrollpunkter

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

Under året har DSO genomfört utbildningar för personer med särskilt ansvar för personuppgifter och personuppgiftshandläggare. DSO har även involverats i frågor från verksamheten och lämnat råd och stöd i ärendeberedning.

Revisorerna har under 2022 genomfört granskning av dataskyddsarbetet och utöver detta har DSO tagit fram en plan för årliga kontroller i syfte att göra återkommande genomlysningar av Regionens dataskyddsarbete.

För året 2022 har DSO fokuserat på att följa upp tidigare genomförda granskningar.

Under 2022 har undertecknad varit utsedd som Dataskyddsombud för Regionstyrelsen och Hälso- och sjukvårdsnämnden, Folkhögskolestyrelsen och sedan 2022-11-01 även för Regionala utvecklingsnämnden. Patientnämnden har utsett ett annat dataskyddsombud, denna rapport omfattar således inte den verksamheten.

Nedan redogörs för den genomförda granskningen och DSO:ns slutsatser samt rekommendationer gällande de kontrollerna som genomförts.

# 3. Uppföljning av tidigare rekommendationer

DSO har tidigare rekommenderat att

- registerförteckna alla personuppgiftsbehandlingar
- utse personuppgiftshandläggare
- höja kunskapsnivån gällande rapportering av personuppgiftsincidenter

## Registerförteckning

Registerförteckningen är ett krav enligt förordningen och ska kunna visas för tillsynsmyndigheten vid efterfrågan. I Regionen används i nuläget en sharepointlösning där verksamheterna registrerar sina behandlingar. Dataskyddsförordningen ställer krav på vad som ska förekomma i registret över personuppgiftsbehandlingar. Det handlar bland annat om ändamål för behandlingen, kategorier av registrerade och huruvida överföring av personuppgifter till tredjeland sker. Eftersom tillsynsmyndigheten kan begära att ta del av registret är det av yttersta vikt att verksamheten dokumenterar sina behandlingar korrekt i registret.

### Granskningen

Granskningen har genomförts genom att i den SharePoint lösning Regionen använder för registerförteckningar göra 10 stickprov per nämnd och kontrollera att dessa förteckningar är ifyllda korrekt.

### Utfall av granskningen

#### **Regionstyrelsen**

Regionstyrelsen har 154 st. noterade registerförteckningar i verktyget. DSO noterar dock att de förteckningar som gäller personuppgiftsbehandlingar som sker i regionövergripande system inte är komplett. DSO rekommenderar därför att objektägare/objektförvaltare registerförtecknar de personuppgiftsbehandlingar som sker i de regionövergripande systemen.

#### **Hälso- och sjukvårdsnämnden-**

Hälso och sjukvårdsnämnden har 586 st. noterade registerförteckningar i verktyget.

#### **Regionala utvecklingsnämnden**

Då Regionala utvecklingsnämnden enbart har 3 st. registrerade förteckningar i det av Regionen utsedda verktyget för registerförteckningar har en stickprovskontroll inte varit möjlig att genomföra. Rekommendationen till nämnden är att skyndsamt registerförteckna alla personuppgiftsbehandlingar i verktyget. Nämnden har tidigare haft ett annat verktyg för att registerförteckna personuppgiftsbehandlingar, då detta avskaffades har inte förteckningarna förts över.

#### **Folkhögskolestyrelsen**

Då folkhögskolestyrelsen helt saknar registerförteckningar i det av Regionen avsedda verktyget rekommenderar DSO att nämnden skyndsamt registerförteckna alla personuppgiftsbehandlingar i verktyget.

## Personuppgiftshandläggare

Verksamhetschefen ansvarar för att utse personuppgiftshandläggare vid enheten. Personuppgiftshandläggarna är en del av organisationen för att säkerställa att vi har kunskapen och resurserna att hantera dataskyddsfrågor på ett korrekt sätt. Personuppgiftshandläggaren skall fungera som verksamhetschefens förlängda arm i dataskyddsfrågor och vara en tydlig kanal in till det dataskyddsombud som är utsett för nämndens verksamhetsområde. Personuppgiftshandläggaren skall utöver att samråda med dataskyddsombudet i dataskyddsfrågor vid enheten även ta fram de rutiner som behövs vid enheten i dataskyddsfrågor, kontakta

*dataskyddsbudet i frågor som gäller dataskydd och laglighet i behandlingar samt ingå i det nätverk som dataskyddsbudet leder.*

### Granskning

Granskningen har genomförts genom att kontrollera om personuppgiftshandläggare har utsetts per nämnd och isåfall om de genomgått utbildning för uppdraget.

### Utfall av granskningen

#### **Regionstyrelsen**

Enligt DSOs uppgifter har Regionstyrelsen utsett 7 st personuppgiftshandläggare för olika verksamheter, 3 st av dessa har deltagit i utbildning under 2022.

#### **Hälso- och sjukvårdsnämnden**

Enligt DSOs uppgifter har Hälso- och sjukvårdsnämnden utsett 56 st. personuppgiftshandläggare för olika verksamheter, 25 st av dessa har deltagit i utbildning under 2022.

#### **Regionala utvecklingsnämnden**

Regionala utvecklingsnämnden har utsett personuppgiftshandläggare för nämnden, personen har även tidigare deltagit i utbildning.

#### **Folkhögskolestyrelsen**

Folkhögskolestyrelsen har inte utsett personuppgiftshandläggare för nämnden, DSO rekommenderar därför verksamheterna under styrelsen att göra detta för att bistå i verksamhetens arbete.

Sammanfattningsvis uppmanar DSO att utse personuppgiftshandläggare och att hänvisa utsedda personuppgiftshandläggare att kontakta DSO så att en aktuell lista över personuppgiftshandläggare upprättas, denna lista skapas genom den teamskanal dataskyddsbudet administrerar. DSO kan då enkelt skapa kontakt med dessa och påtala när utbildningstillfällen skall genomföras.

## **Personuppgiftsincidenter**

*En personuppgiftsincident definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig, förstöring, förlust, ändring, obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna. Alla personuppgiftsincidenter skall dokumenteras och om incidenten kan leda till att de registrerade utsätts för allvarliga risker, måste Integritetsskyddsmyndigheten underrättas inom 72 timmar från upptäckten.*

### Granskning

Granskningen har genomförts genom att kontrollera om personuppgiftsincidenter har rapporterats i diariet samt om dessa har dokumenterats på ett riktigt sätt.

### Utfall av granskningen

#### **Regionstyrelsen**

Under 2022 har det registrerats 6 st. personuppgiftsincidenter i Platina. Med tanke på att tex. IT ligger under Regionstyrelsen är den siffran väldigt låg och kan vara ett

tecken på brister i rapporteringsrutiner. Exempel på personuppgiftsincidenter är att en dator som innehåller personuppgifter förloras eller att en obehörig part (internt eller externt) får tillgång till personuppgifter. DSO rekommenderar därför Regionstyrelsen att se över sina rutiner för rapportering inom dessa områden och säkerställa att samtliga personuppgiftsincidenter registreras. I de registrerade incidenterna saknas ofta ställningstagande till om händelsen är en sk. Allvarlig händelse och skall rapporteras till tillsynsmyndigheten. DSO rekommenderar därför att styrelsen säkerställer att personuppgiftsincidenter dokumenteras i tillräcklig omfattning.

#### **Hälsa- och sjukvårdsnämnden**

Under 2022 har det registrerats 15 st. personuppgiftsincidenter i Platina. Personuppgiftsincidenterna har dokumenterats men i stor utsträckning saknas ett ställningstagande kring om händelsen är en sk. Allvarlig och skall rapporteras vidare till tillsynsmyndigheten. DSO rekommenderar därför att nämnden säkerställer att personuppgiftsincidenter och bedömningar dokumenteras i tillräcklig omfattning.

#### **Regionala utvecklingsnämnden**

Under 2022 har det inte registrerats några personuppgiftsincidenter i Platina gällande personuppgiftsincidenter för Regionala utvecklingsnämnden. Detta kan vara ett tecken på att rutinerna eller kunskap om rapportering av personuppgiftsincidenter är bristfälliga. DSO rekommenderar nämnden att informera all personal om vad en personuppgiftsincident är och skyldigheten att rapportera incidenter samt att dokumentera de incidenter som inträffar.

#### **Folkhögskolestyrelsen**

Under 2022 har det inte registrerats några personuppgiftsincidenter i Platina gällande personuppgiftsincidenter för Folkhögskolestyrelsen. Detta kan vara ett tecken på att rutinerna för rapportering av personuppgiftsincidenter är bristfälliga. DSO rekommenderar nämnden att informera all personal om vad en personuppgiftsincident är och skyldigheten att rapportera incidenter samt att dokumentera de incidenter som inträffar.

## **4. DSOs rekommendationer**

DSO har lämnat rekommendationer för varje punkt som granskats ovan. Utöver dessa specifikt riktade rekommendationerna vill DSO även lyfta fram generella rekommendationer utifrån de observationer som har gjorts för år 2022.

- Varje personuppgiftsansvarig har en ansvarsskyldighet. Denna ansvarsskyldighet innebär en skyldighet att kunna visa att dataskyddsförordningen uppfylls. Det är utifrån detta otroligt viktigt att ha kontroll över de personuppgiftsbehandlingar som sker inom personuppgiftsansvariges område och förteckna dessa samt de omständigheter som finns kring personuppgiftsbehandlingarna såsom personuppgiftsincidenter, tredjelandsoverföringar eller konsekvensbedömningar. DSO rekommenderar samtliga nämnder att ta fram rutiner för denna typ av dokumentation.

- Kunskapen inom verksamheterna gällande GDPR behöver generellt förbättras, en plan för utbildning av anställda och andra nyckelpersoner rekommenderas.

Umeå 12-01-2022