GRANSKNINGSRAPPORT

Dataskyddsförordningen

PERSONUPPGIFTSANSVARIG

Finnvedens samordningsförbund

GRANSKAT OMRÅDE

Hantering av personuppgiftsincidenter (och översiktlig kontroll av artikel 30-registret)

DATUM

2024-03-28

Erik Österberg
Dataskyddsombud
dso.finsam-finnveden@insatt.com

Insatt AB
Kyrkogatan 4
553 16 Jönköping

www.insatt.com

Innehållsförteckning

1. Inledning

I uppdraget som dataskyddsombud ingår att övervaka efterlevnaden av dataskyddsförordningen och nationella kompletterande dataskyddsbestämmelser och organisationens arbete och implementerade styrdokument för skydd av personuppgifter. Granskningsdelen i uppdraget omfattar ansvarstilldelning, information till och utbildning av personal som deltar i behandling och organisationens styrdokument med mera.

Som en del av ovanstående uppdrag har en sådan granskning genomförts och resultatet av den granskningen presenteras i den här rapporten.

1.1 Granskningens innehåll och omfattning

Granskningen omfattar Finnvedens samordningsförbunds (”Förbundet”) hantering av personuppgiftsincidenter samt en översiktlig kontroll av dess artikel 30-register.

Granskningen utgår från följande underlag:

- förbundets svar på frågor om dess incidenthantering,
- förbundets styrdokument för incidenthantering (plan, rutin eller motsvarande), samt
- förbundets artikel 30-register.

1.2 Syfte

Syftet med granskningsrapporten är att återkoppla granskningsresultatet och, när det är påkallat, åtgärdsförslag för förbättringar till organisationens ledning.

1.3 Disposition

I kapitel 2 sammanfattas dataskyddsombudets slutsatser och rekommenderade åtgärder. Kapitel 3 utgörs av den juridiska utgångspunkten för granskningen. Kapitel 4 innefattar själva granskningen och dess resultat med dataskyddsombudets löpande slutsatser och kommentarer.

2. Sammanfattande åtgärder

2.1 Dataskyddsombudets sammanfattande slutsatser

Förbundet har upprättat ”Rutin vid personuppgiftsincident enligt dataskyddsförordningen GDPR” uppdaterad den 31 oktober 2023. Rutinen beskriver vad en personuppgiftsincident är samt hur förbundet ska upptäcka, hantera och dokumentera personuppgiftsincidenter. Vidare har förbundet tagit fram ”Logg för personuppgiftsincidenter i Finnvedens SF”. Dataskyddsombudet ser positivt på att såväl intern rutin som logg tagits fram och att samtliga personuppgiftsbiträdesavtal innehåller information om hur biträdet ska informera förbundet om biträdet upptäcker en personuppgiftsincident.

Förbundet har anmärkningsvärt få dokumenterade personuppgiftsincidenter. Frågan är om fler incidenter skett som inte upptäckts eller om verksamheten faktiskt bara har haft sammanlagt en personuppgiftsincident (2022). Verksamheten är visserligen liten med endast ett fåtal anställda och en kärnverksamhet utan någon betydande personuppgiftsbehandling, men eftersom det krävs väldigt lite för att kvalificera en händelse som en personuppgiftsincident är det inte osannolikt att verksamheten har haft fler incidenter som inte identifierats. Dataskyddsombudet vill här betona vikten av att förbundet fortsätter utbilda och påminna anställda om incidenter och de interna rutinerna.

Dataskyddsombudet har vissa rekommendationer på förtydliganden och tillägg till förbundets rutin och logg för incidenter.

2.2 Förbundet rekommenderas att:

- Komplettera ”Rutin vid personuppgiftsincident enligt dataskyddsförordningen GDPR” enligt följande:
  - Säkerställ att det är tydligt för alla anställda och att de ska eskalera pågående samt misstänkta incidenter till förbundschefen. Det kan vara svårt för alla anställda att själva bedöma om en händelse utgör en incident eller inte, varför även misstänkta fall bör lyftas till förbundschefen vilken i sin tur kan eskalera frågan till dataskyddsombudet vid behov,
  - Överväg att specificera informationen om incidenten som behöver finnas med i eventuell anmälan till IMY så att de anställda kan samla in och förmedla denna till förbundschefen vid den interna incidentrapporteringen,
  - Uppmana till att skicka in anmälan direkt via IMY:s hemsida eller ladda ner blanketten och skicka den per e-post (i stället för per post),
  - Ange information om vem som ansvarar för att intern dokumentering av incidenter,
  - Säkerställ att det i rutinen framgår att information till registrerade ska lämnas *utan onödigt dröjsmål* och
  - Överväg att se över dispositionen av rutinens olika avsnitt till att bättre stämma överens med kronologin i bedömningen av en personuppgiftsincident.
- Komplettera ”Logg för personuppgiftsincidenter i Finnvedens SF”.
  - med en kolumn för ”Vilka personuppgifter har påverkats?”.
- Förbundet rekommenderas att involvera dataskyddsombudet när det råder tvekan vid bedömningen av huruvida en händelse ska klassas som en personuppgiftsincident.

- Uppdatera artikel 30-registret genom att
  - se över samtliga behandlingar och lämna kolumn L i registret toms för de behandlingar som inte innehåller några känslig personuppgifter och
  - utreda huruvida behandlingarna ”Hälsoenkäten EQ5D” och ”Deltagaruppgifter från insatser” omfattar personuppgifter (om de direkt eller indirekt är hänförliga till en identifierad eller identifierbar levande person) och om inte överväga att ta bort dessa behandlingar från behandlingsregistret.

3. Juridisk utgångspunkt för granskningen

Granskningen har genomförts med beaktande av dataskyddsförordningen:

- artikel 4 (12): definitionen av en personuppgiftsincident
- artikel 5: grundläggande principer inklusive ansvarsskyldigheten,
- artikel 24.1: krav att kunna visa att organisationen lever upp till kraven i dataskyddsförordningen,
- skäl 85–86 och artiklarna 33 och 34: regler för hantering av personuppgiftsincidenter.

3.1 Definitionen av en personuppgiftsincident

En personuppgiftsincident innebär enligt artikel 4 (12) i dataskyddsförordningen ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”.

3.2 Regler för hantering av personuppgiftsincidenter

3.2.1 När ska en incident anmälas?

I enlighet med artikel 33 i GDPR ska en personuppgiftsincident anmälas till behörig tillsynsmyndighet om det inte är osannolikt att incidenten medför risk för fysiska personers fri- och rättigheter. Den personuppgiftsansvariga ska utan onödigt dröjsmål och inte senare än 72 timmar efter att den fått vetskap om personuppgiftsincidenten anmäla den till Integritetsskyddsmyndigheten (IMY). I de fall anmälan inte inkommer till IMY inom 72 timmar ska en motivering till förseningen lämnas av den personuppgiftsansvarige.

3.2.2 Kraven på anmälan och intern dokumentation

Anmälan till IMY ska åtminstone beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftstyper som berörs. Anmälan ska likväl förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas samt innehålla en beskrivning av de

sannolika konsekvenserna av personuppgiftsincidenten. Vidare ska anmälan beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten och när det är möjligt åtgärder för att mildra dess potentiella negativa konsekvenser. Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

Personuppgiftsansvarig ska enligt artikel 33.5 dokumentera alla personuppgiftsincidenter och dess omständigheter internt. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera att reglerna presenterade ovan följs.

3.2.3 Att informera de registrerade

I de fall personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers fri- och rättigheter ska den personuppgiftsansvariga utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. Enligt artikel 34 GDPR ska en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas, beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten samt beskrivning av de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, lämnas till den registrerade.

Undantag från informationskravet gäller bland annat om den personuppgiftsansvarige

- har gjort uppgifterna oläsbara exempelvis genom kryptering,
- har vidtagit ytterligare åtgärder som säkerställer att den höga risken för registrerades fri- och rättigheter sannolikt inte längre kommer att uppstå, eller om
- det skulle inbegripa en oproportionell ansträngning (i så fall ska i stället allmänheten informeras).

4. Granskningen

4.1 Svarsformuläret

Förbundet har svarat på dataskyddsombudets frågor om dess incidenthantering i utskickat svarsformulär. Av svaren framgår i huvudsak att förbundet tagit fram en incidenthanteringsplan (Rutin vid personuppgiftsincident enligt dataskyddsförordningen GDPR), en intern incidentlogg och att de anställda utbildats både vad gäller vad en personuppgiftsincident är och om dess hantering i enlighet med interna rutiner. Vidare har förbundet uppgett att alla biträdesavtal innehåller information om hur biträdet ska informera den personuppgiftsansvarige om biträdet upptäcker en personuppgiftsincident. Viss osäkerhet verkar dock råda angående huruvida förbundet agerar som personuppgiftsbiträde och gemensamt personuppgiftsansvarig i något fall.

Dataskyddsombudets slutsatser

Dataskyddsombudet ser positivt på att såväl interna styrdokument som loggföringsdokument tagits fram och att pub-avtalen innehåller information om hur biträdet ska informera

förbundet om biträdet upptäcker en personuppgiftsincident. Dataskyddsombudet har inga synpunkter på förbundets svar med anledning av dessa. För innehållet i rutin och intern logg se avsnitt 4.2 nedan. Vi tar upp och diskuterar förbundets eventuella ställning som personuppgiftsbiträde eller gemensamt personuppgiftsansvarig vid kommande utbildningstillfälle.

Tabell 2 *Antal dokumenterade personuppgiftsincidenter per år*

Antal dokumenterade personuppgiftsincidenter per år		
2021	**2022**	**2023**
0	**1**	**0**

Kommentar

Frågan är om fler incidenter skett som inte upptäckts eller om verksamheten faktiskt bara har haft en personuppgiftsincident (under 2022). Verksamheten är visserligen liten med endast ett fåtal anställda och en kärnverksamhet utan någon betydande personuppgiftsbehandling, men eftersom det krävs väldigt lite för att kvalificera en händelse som en personuppgiftsincident är det inte osannolikt att verksamheten har haft fler incidenter som inte identifierats. En av anledningarna kan vara att samtliga i organisationen inte har tillräcklig kunskap för att kunna identifiera en incident.

Det finns inget uttryckligt krav i dataskyddsförordningen på att involvera dataskyddsombudet vid utredning och bedömning av en personuppgiftsincident. Däremot ska dataskyddsombudet enligt artikel 38 i dataskyddsförordningen på ett korrekt sätt och i god tid delta i alla frågor som rör skyddet av personuppgifter. Finnvedens samordningsförbund rekommenderas därför att involvera dataskyddsombudet när det råder tvekan vid bedömningen av huruvida en händelse ska klassas som en personuppgiftsincident.

4.2 Rutin vid personuppgiftsincidenter och intern logg

Förbundet har upprättat ”Rutin vid personuppgiftsincident enligt dataskyddsförordningen GDPR” uppdaterad den 31 oktober 2023. Rutinen beskriver vad en personuppgiftsincident är samt hur förbundet ska upptäcka, hantera och dokumentera personuppgiftsincidenter. Vidare har förbundet tagit fram ”Logg för personuppgiftsincidenter i Finnvedens SF”.

Resultat

Resultatet av granskningen av incidenthanteringsinstruktionen samt den interna loggen visar följande.

1. *Det praktiska ansvaret för hantering av personuppgiftsincidenter*

   Det framgår av rutinen att förbundschefen ansvarar för den praktiska hanteringen av personuppgiftsincidenter.

   a. Inga synpunkter.

2. *Att alla incidenter ska rapporteras vid kommande AU- och styrelsemöte*

   Det är positivt att förbundet rapporterar inträffade personuppgiftsincidenter till dess högsta ledning. Jag delar även förbundets ställningstagande att ”Om incidenten är allvarlig ska förbundets ordförande informeras omedelbart”, samt att denne ska ta ställning till om extra AU- eller styrelsemöte bedöms behövas med anledning av det inträffade. Att direkt informera förbundets ordförande vid allvarliga incidenter och att rapportera alla incidenter till styrelsen (vid kommande AU-eller styrelsemöte), borgar dels för effektiv hantering av akuta problem, dels för att potentiella strukturella brister kan identifieras och avhjälpas på sikt.

   a. Inga synpunkter.

3. *Anställda*

   Rutinen saknar en tydlig beskrivning av samtliga anställdas ansvar avseende personuppgiftsincidenter. En personuppgiftsincident kan inträffa och upptäckas i hela organisationen, varför det är av största vikt att samtliga anställda kan identifiera en incident och vet hur de ska ta den vidare. Förbundet har visserligen en liten organisation och det borde falla sig naturligt att kontakta förbundschefen när man upptäckt en incident eller misstänker att en händelse kan utgöra en incident. Utifrån ansvarsskyldigheten är det dock viktigt att i riktlinjen klargöra att alla anställda har ett ansvar att eskalera incidenter och att ha en rutin för hur de anställda ska gå till väga när de upptäcker en misstänkt incident.

   a. Säkerställ att det i rutinen är tydligt för alla anställda och att de ska eskalera pågående samt misstänkta incidenter till förbundschefen. Det kan vara svårt för alla anställda att själva bedöma om en händelse utgör en incident eller inte, varför även misstänkta fall bör lyftas till förbundschefen vilken i sin tur kan eskalera frågan till dataskyddsombudet vid behov.

4. *Anmälan av incident till tillsynsmyndighet*

   För att underlätta eventuell anmälan till tillsynsmyndigheter bör så mycket uppgifter som möjligt om incidenten vara med i rapporteringen från den som upptäcker incidenten och informerar förbundschefen. Självklart kan vidare utredning och kompletteringar behövas och fler uppgifter kan behöva hämtas in i utredningen av incidenten. Så mycket (relevant) information som möjligt initialt från den som upptäcker incidenten underlättar dock en effektiv utredning och möjliggör att hålla tidsfristen om anmälan inom 72 timmar från dess den personuppgiftsansvarige fått vetskap om incidenten.

   I samband med klargörande av de anställdas ansvar (se ovan) bör det därför klargöras vilka uppgifter om incidenten som ska uppges i den interna rapportering till förbundschefen.

   a. Nedan information bör uppges vid intern rapportering av misstänkt eller pågående incident:
      i. beskrivning av personuppgiftsincidentens art.

ii. om möjligt, de kategorier av och det ungefärliga antalet registrerade som berörts
iii. om möjligt, de antal personuppgifter som incidenten omfattar
iv. beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten
v. beskrivning av de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten och
vi. när det är möjligt åtgärder för att mildra incidentens potentiella negativa konsekvenser.

b. Dataskyddsombudet noterar att rutinen förespråkar att särskild blankett på IMY:s hemsida ska användas för det fall anmälan aktualiseras, vilket jag inte har några invändningar emot. Däremot framkommer även att nämnda blankett ska skickas via post. Mot bakgrund av den korta tidsfristen för anmälan till IMY samt användarvänligheten rekommenderas förbundet att
    i. ändra rutinen och uppmana till att skicka in anmälan direkt via IMY:s hemsida eller ladda ner blanketten och skicka den per e-post.

5. *Alla personuppgiftsincidenter ska dokumenteras*

Det framgår av rutinen att incidenter ska dokumenteras i ett särskilt dokument: ”Logg för incidenter”. Det framgår däremot inte av rutinen vem som ansvarar för att dokumentering sker. Därför rekommenderas förbundet att

a. komplettera rutinen med information om vem som ansvarar för att dokumentering.

I ”Logg för incidenter” finns tydliga kolumner för vilka uppgifter om incidenten som dokumentationen omfattar. Enligt EDPB:s riktlinjer ska följande uppgifter, som minimum, finnas med i den interna dokumentationen: orsaker till incidenten, vad som hände, *vilka personuppgifter som påverkades*, incidentens effekt och konsekvens samt eventuella åtgärder vidtagna av den personuppgiftsansvarige. Kolumnerna i förbundets logg uppfyller dessa krav, frånsett vilka personuppgifter som påverkats av incidenten, varför det rekommenderas att

b. komplettera loggen med en kolumn för ”Vilka personuppgifter har påverkats?”.

6. *Information till registrerade*

Rutinen innehåller information om att registrerade ska informeras vid incident som sannolikt leder till en hög risk för den registrerades rättigheter och friheter. Av ansvarsfördelningen anges det i rutinen att förbundschefen ansvarar för att meddela sådan information. Däremot saknar rutinen information om att sådan information i så fall ska ges utan onödigt dröjsmål i enlighet med dataskyddsförordningens krav, varför förbundet rekommenderas att

a. säkerställa att det i rutinen framgår att information till registrerade ska lämnas *utan onödigt dröjsmål*.

7. Rutinens disposition

Hanteringen av personuppgiftsincidenter kan ses som en ”trestegsraket”. Alla incidenter ska dokumenteras internt (1). Föreligger risk för de registrerade ska incidenten anmälas till IMY (2) och bedöms denna risk som hög ska även de registrerade informeras (3). Rutinens disposition är in nuläget enligt följande. Den inleds med definitionen av en personuppgiftsincident, vilket jag tycker är klokt. Härefter följer rubriken ”Hur ska individer som drabbas informeras?” och sedan ”Hur ska incidenter rapporteras till Integritetsskyddsmyndigheten IMY?”. Enligt dataskyddsombudet är det mer pedagogiskt att efter rubriken ”Vad är en personuppgiftsincident?” ha avsnittet om anmälan till IMY och därefter rubriken om eventuell information till de drabbade (undantagsfall). Förbundet rekommenderas därför att

a. överväga att se över dispositionen av rutinens olika avsnitt till att bättre stämma överens med kronologin i bedömningen av en personuppgiftsincident.

4.3 Artikel 30-registret

Att hålla ett uppdaterat behandlingsregister är inte bara ett uttryckligt lagkrav utan även ett sätt för den personuppgiftsansvarige att leva upp till ansvarsskyldigheten i art. 5.2 i GDPR och visa att behandlingarna sker i enlighet med GDPR. Informationen i art. 30-registret, under förutsättning att den är korrekt och tillräcklig, ger den personuppgiftsansvarige en överblick över alla personuppgiftsbehandlingar som sker inom organisationen och underlättar organisationens fortsatta dataskyddsarbete. Dataskyddsombudet har, ombedd av förbundschefen, översiktligt granskat förbundets artikel 30-register. En djupare granskning av detsamma gjordes visserligen 2022. Art.30-registret är dock ”inget man blir klar med” utan ska ses som ett levande dokument som löpande behöver uppdateras, kompletteras och ”rensas” i takt med att personuppgiftsbehandlingar tillkommer och upphör.

Resultat

Vid en översiktlig kontroll noteras att registret är välifyllt (inga tomma kolumner förekommer), att det innehåller de behandlingar som det utifrån dataskyddsombudets kunskap om verksamheten rimligen kan förväntas innehålla samt att det uppdaterats så sent som den 20 december 2023. Dataskyddsombudet noterar dock att kolumn L ”Undantag i artikel 9” fyllts i med lagrum i artikel 9 dataskyddsförordningen för någon behandling som inte verkar omfatta känsliga personuppgifter. Undantag enligt artikel 9 krävs endast för behandling av särskilda kategorier av personuppgifter (känsliga personuppgifter). Kolumnen ska således endast fyllas för de behandlingar där förbundet behandlar känsliga personuppgifter. Vidare noteras att förbundet i behandlingen ”Deltagaruppgifter från insatser” angett att det avser avidentifierade uppgifter om deltagare. För det fall personerna över huvud inte är identifierbara torde det inte utgöra personuppgifter, därav ingen personuppgiftsbehandling och i sådant fall inget behov att ha med den i artikel 30-registret. Det är därför tveksamt om denna ska tas upp som behandling i registret.

Förbundet rekommenderas att

- Se över samtliga behandlingar och lämna kolumn L i registret tomt för de behandlingar som inte innehåller några känslig personuppgifter och
- Utreda huruvida behandlingen ”Deltagaruppgifter från insatser” omfattar personuppgifter (om de direkt eller indirekt är hänförliga till en identifierad eller identifierbar levande person) och om inte överväga att ta bort denna behandling från behandlingsregistret.