

Till förbundsstyrelsen 240904

## **PM om Årsrapport GDPR och Granskningsrapport om incidenthantering**

Förbundets dataskyddsombud (DSO) har granskat förbundets arbetssätt. Detta PM innehåller kommentarer till hans förslag i de båda rapporterna Årsrapport 2023 och Granskningsrapport, inklusive förslag till tidsplan för fortsatta åtgärder.

### **A. Om Årsrapport 2023**

Årsrapporten inleds med information om syftet med årsrapporten, roller och ansvar i arbetet med GDPR-frågor.

**DSO:** Det verkar råda viss osäkerhet vad som ska ses som en begäran av rätt till rättelse respektive rätt till radering.

**Kommentar: utbildning har genomförts och rutinen har förtydligats.**

**DSO om granskning 2023 av information till registrerade:** Säkerställ att den information som ges kandidater, anställda och styrelsemedlemmar omfattar samtliga personuppgiftsbehandlingar av de registrerades personuppgifter före, under och efter anställningen/styrelseuppdraget,

**Kommentar: en översyn har skett och information kompletterats på flera sätt.**

**DSO:** upprätta en rutin för hantering av spontanansökningar och information till spontanansökare. Sådana ansökningar kan ju alltid komma in mejl-ledes till förbundet och behöver då hanteras

**Kommentar: en rutin har upprättats i samråd med DSO**

**DSO:** se över befintlig Integritetspolicyn och anpassa den för dess interna personuppgiftsbehandlingar (gällande anställda och styrelsemedlemmar), åtgärda felaktigheterna (som nämns under avsnitt 3.2) i Integritetspolicyn. stämna av Integritetspolicyn med artikel 13–14 samt addera relevanta delar

**Kommentar: uppdatering av Integritetspolicyn sker nu**

**DSO:** ta fram en ny fullständig informationstext för hemsidan för era externa behandlingar (gällande webbplats- och sociala mediebesökare, eventbesökare, kandidater med flera)

**Kommentar: en informationstext har tagits fram och lagts på hemsida**

**DSO:** gällande e-postsignaturen, att säkerställa att informationstexten

- beskriver att kontakt med samordningsförbundet innebär behandling av personuppgifter där förbundet är personuppgiftsansvarig,
- begränsar att förbundet får in känsliga personuppgifter via e-post, och
- innehåller en länk till kompletterande information och de registrerades rättigheter exempelvis till extern personuppgifts-/integritetspolicy på hemsidan

#### **Kommentar: texten har kompletterats i samråd med DSO**

**DSO:** i samband med prenumeration på nyheter från hemsidan, att säkerställa att "första lagersinformation" med hänvisning till kompletterande information och de registrerades rättigheter förslagsvis till extern personuppgifts-/integritetspolicy på hemsidan tillhandahålls de registrerade.

#### **Kommentar: texten har förtydligats i samråd med DSO**

**DSO konstaterade dessutom i Årsrapport 2021:** Eftersom förutsättningarna och antalet personuppgiftsbehandlingsprocesser kan ändras över tid, rekommenderas samordningsförbundet att årligen ompröva besluten att inte genomföra återstående åtgärder på åtgärdslistan...

Punkterna är:

- Överväg att upprätta rutiner för införande och underhåll av tekniska säkerhetsprodukter och -metoder.
- Överväg att upprätta rutiner för regelbunden testning av datasäkerhetsnivåer
- Överväg att ta fram en process för löpande riskvärdering av befintliga personuppgiftsbiträden. Särskilt vid behandling av känsliga uppgifter eller personnummer
- Överväg att utvärdera dataskydd och datasäkerhet för befintliga leverantörer. Särskilt vid behandling av känsliga uppgifter eller personnummer
- Komplettera befintlig process för att hantera klagomål med sådana rättigheter som följer av dataskyddsförordningen: begäran om åtkomst/utdrag; begäran om rättning av felaktiga personuppgifter; samt begäran om information
- Överväg att ta fram en dokumenterad strategi för uppföljning av förfrågningar och klagomål från registrerade

**Kommentar:** De båda sista punkterna har åtgärdats, i form av en Rutin vid förfrågan från registrerad. Rutinen har lagts in på hemsidan.

Motiv till att de övriga fyra punkterna i åtgärdslistan inte behöver åtgärdas är fortfarande tidsbrist. Säkerhetsnivån hålls hög även utan formella skrivna rutiner.

## **B. Granskningsrapport om förbundets hantering av personuppgiftsincidenter**

**DSO:** Säkerställ att det är tydligt för alla anställda och att de ska eskalera pågående samt misstänkta incidenter till förbundschefen.

**Kommentar:** Utbildning har genomförts och en tydligare rutin har införts.

**DSO:** 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

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 SF Södra Vätterbygden" med en kolumn för "Vilka personuppgifter har påverkats?".

**Kommentar till samtliga punkter: Klart**

**DSO:** Förbundet rekommenderas att involvera dataskyddsombudet när det råder tvekan vid bedömningen av huruvida en händelse ska klassas som en personuppgiftsincident.

**Kommentar: Utbildning har genomförts och överenskommelse gjorts om samråd vid tvekan**

**DSO:** Uppdatera artikel 30-registret genom att se över samtliga behandlingar och lämna kolumn L i registret tomt för de behandlingar som inte innehåller några känsliga personuppgifter

**Kommentar: Klart.**

**Förslag till beslut:**

att godkänna rapporten

att stå fast vid tidigare bedömning att de kvarvarande fyra punkterna som nämns i rapporten inte behöver åtgärdas. Motiv: tidsbrist.

Jönköping 2024-08-22

Peter Hedfors  
förbundschef