Fördjupad kontroll 2022

Hantering av personuppgiftsincidenter under 2021

Bakgrund

Den fördjupade kontrollen gällande personuppgiftsincidenter har haft till syfte att undersöka om det finns förutsättningar för verksamheten att hantera personuppgiftsincidenter på ett korrekt sätt som följer dataskyddsförordningen och om bolagets rutiner/handlingsplaner får önskat genomslag i praktiken. Kontrollen har genomförts i två delar där del ett har bestått av att verksamheten har ombetts att skicka in dokumentation av rutiner/handlingsplaner för hanteringen av incidenter och dokumentation över inträffade incidenter under 2021. Del två har bestått av frågor kopplade till organisationens incidenthantering.

Iakttagelser från kontrollen

Personuppgiftsincidenter kan leda till allvarliga konsekvenser för registrerade personer och det är av stor vikt att de hanteras på ett korrekt sätt. Enligt dataskyddsförordningen ska vissa typer av personuppgiftsincidenter anmälas till tillsynsmyndigheten och i vissa fall ska även de registrerade informeras. Även de personuppgiftsincidenter som inte behöver anmälas till tillsynsmyndigheten ska dokumenteras.

IMY:s checklista vid personuppgiftsincidenter

Integritetsskyddsmyndigheten (IMY) har på sin hemsida publicerat en checklista för personuppgiftsansvariga att använda i sitt arbete med personuppgiftsincidenter. Den består bl.a. av vilka åtgärder personuppgiftsansvariga kan vidta i sitt proaktiva arbete med personuppgiftsincidenter och vad som behöver göras vid redan inträffade incidenter. IMY lyfter att det av rutinerna bör framgå hur en bedömning av riskerna för de registrerade ska gå till och i förlängningen om det behöver upprättas en anmälan till tillsynsmyndigheten. Det bör också framgå hur man bedömer om de registrerade ska informeras, hur det ska gå till och vad informationen ska innehålla.

Renova AB:s hantering av personuppgiftsincidenter

Rutiner och handlingsplaner

Renova AB (bolaget) har en rutin för hantering av personuppgiftsincidenter som gäller för alla anställda på bolaget. Rutinen innefattar en beskrivning av vad en personuppgiftsincident innebär och innehåller ett antal listade exempel. Det är vidare beskrivet hur anställda, vid misstänkta incidenter, ska hantera en personuppgiftsincident. Efter en intern rapportering om misstänkt incident ska dataskyddskontakt fastställa om incident inträffat och riskbedöma den. I rutinen framgår att incident manager på bolagets IT-avdelning, dataskyddskontakt och systemansvarig ska delta i riskbedömningen.

Vidare framgår när en incident ska anmälas till tillsynsmyndigheten och att dataskyddsombud i så fall ska informeras.

Därefter följer en beskrivning av i vilka fall som de registrerade ska informeras och vad informationen ska innehålla. Vidare fastslår rutinen att incidenten ska åtgärdas och att alla personuppgiftsincidenter ska dokumenteras.

Personuppgiftsincidenter under 2021

Av det inskickade underlaget framgår att bolaget under år 2021 haft en personuppgiftsincident.

Information till anställda

Bolaget har rutinen vid personuppgiftsincidenter och rapportering av personuppgiftincident tillgänglig på sitt intranät för bolagets anställda.

Dataskyddsombudets rekommendationer

Rutiner och handlingsplaner

Bolagets rutin innehåller exempel på händelser som utgör en incident, vilket är positivt. Förutsatt att anställda har grundläggande kunskaper i dataskydd kan beskrivningen vara till hjälp att identifiera en personuppgiftsincident. Det är även positivt att det finns beskrivet att en riskbedömning måste göras vid en misstänkt incident.

För att göra hanteringen ytterligare lättillgängligare för verksamheten kan det enligt dataskyddsombudet finnas skäl att utöka rutinen med fler konkreta beskrivningar av hur en incident och den medförande risken för de registrerade ska bedömas. Att tydliggöra detta skulle göra det enklare att upptäcka och hantera incidenter korrekt inom verksamheten.

Rutinen beskriver hanteringen av incidenter och vilka från bolaget som ska ingå i bedömningen av en incident. Dataskyddsombudet rekommenderar att rutinen kompletteras med ett förtydligande gällande vem som fattar beslut efter att den initiala riskbedömningen gällande om incidenten ska anmälas till Integritetsskyddsmyndigheten.

Personuppgiftsincidenter under 2021

Bolaget har angett att de haft en personuppgiftincident under 2021. Inom en verksamhet är det normalt att det sker ett flertal incidenter varje år och det är troligt att så även har skett hos bolaget, trots att det inte upptäckts, dokumenterats och bedömts. Ett felskickat mejl/brev är exempelvis den vanligast förekommande personuppgiftsincidenten, vilket inte hade varit förvånande om bolaget hade haft vid ett eller flera tillfällen under året 2021.

Information till anställda

Med beaktande av det endast finns en dokumenterad personuppgiftsincident ställer sig dataskyddsombudet tveksam till om anställda har tillräcklig kunskap om vad en incident är och hur anställda ska hantera uppkomna incidenter. Bolaget har sina rutiner tillgängliga på sitt intranät men av bolagets svar framgår inte att någon utbildning eller särskild information givits till anställda om vad en personuppgiftincident är eller hur anställda ska hantera dessa. Dataskyddsombudet rekommenderar att bolaget ser över att ytterligare utbilda sina anställda i vad en personuppgiftsincident kan vara och hur den ska hanteras, för att säkerställa att incidenter inte missas.

Vidare kan det också finnas behov av att med ett visst intervall påminna om vad en personuppgiftsincident är och hur man går tillväga om man misstänker att en sådan har inträffat.

Sammanfattning

- Komplettera rutinen med instruktioner/metod för hur en bedömning av incident samt risken för de registrerades fri- och rättigheter kan göras.
- Komplettera rutinen med vem som beslutar gällande att bedöma om en anmälan till Integritetskyddsmyndigheten ska göras.
- Se över medarbetares kunskap gällande vad som är en personuppgiftsincident.
- Utbilda medarbetare om personuppgiftincidenter och hantering av dessa.
- Se över behovet av en rutin/plan för att regelbundet informera medarbetare om personuppgiftsincidenter och den interna incidenthanteringen.

Bilagor

- Information om fördjupad kontroll 2022.
- Frågeunderlag fördjupad kontroll 2022, del 1 och del 2.