Fördjupad kontroll 2022

Kontrollpunkt 2: 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 bland annat 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.

Business Region Göteborg AB:s hantering av personuppgiftsincidenter

Rutiner och handlingsplaner

Business Region Göteborg 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. Ansvarig chef ska sammankalla avdelningschefen för verksamhetsstöd, ansvarig för incidenthantering på IT-avdelningen, dataskyddskontakt och systemansvarig för aktuellt system för att riskbedöma incidenten. Rutinen innehåller även information om att bolagets dataskyddombud ska involveras gällande bedömning av risk och lämplig hantering. Rutinen fastslår inte vem som beslutar om att anmäla en incident till Integritetsskyddsmyndigheten men ansvarig för anmälan är dataskyddskontakten och det framgår i rutinen vad anmälan ska innehålla.

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 inte haft några personuppgiftsincidenter.

Information till anställda

Bolaget har haft en generell utbildning med samtliga anställda om dataskyddsförordningen och under utbildningen haft en genomgång gällande vad en personuppgiftsincident är. Bolaget har utöver den generella utbildningen haft en utbildning gällande bolagets hantering av personuppgiftincidenter, vilken riktade sig främst till systemansvariga, systemägare och andra berörda vid hantering av incident. På bolagets intranät finns information om vad en incident kan vara och uppmaning att rapportera till bolagets funktionsbrevlåda vid upptäckt av misstänkt incident. Rutinen för hantering av personuppgiftsincidenter finns också tillgänglig på bolagets intranät.

Dataskyddsombudets rekommendationer

Rutiner och handlingsplaner

Bolaget har en rutin som inledningsvis redogör för vad en personuppgiftsincident innebär. Den innehåller ett par 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. För att anställda ska få en bredare bild av vad som utgör incidenter rekommenderas bolaget komplettera nuvarande rutin med exempel som innefattar personuppgifter som inte är av särskilt skyddsvärd eller känslig karaktär. Även felskickade e-postmeddelanden innehållandes sådana personuppgifter kan utgöra en incident. Vidare är det positivt att det finns tydligt beskrivet att en riskbedömning måste göras vid en misstänkt incident och att det finns en utpekad grupp som ska omhänderta en incident. Det är också positivt att det inte är personbundet, utan knutet till en viss tjänst.

För att göra hanteringen mer lättillgänglig för verksamheten kan det enligt dataskyddsombudet finnas skäl att utöka rutinen med fler konkreta beskrivningar av vad en personuppgiftincident är samt mer 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. Eftersom personuppgiftsincidenter ska hanteras skyndsamt och anmälan till tillsynsmyndigheten ska göras inom 72 timmar bör det finnas möjlighet och förutsättningar även för andra inom bolaget att på ett korrekt sätt hantera incidenter. Sammantaget rekommenderar dataskyddsombudet att bolaget konkretiserar sin rutin och kompletterar den med en instruktion eller stödmaterial/metod som anger hur en incident och risken för de registrerade kan bedömas.

Personuppgiftsincidenter under 2021

Bolaget har angett att de inte haft någon 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 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

Vad gäller information till anställda, och hur det säkerställs att anställda vet vad en personuppgiftsincident är och hur dessa ska hanteras är det positivt att bolaget har jobbat aktivt med frågan och att det finns information att tillgå. Det framgår emellertid inte av underlaget att det finns en rutin för att säkerställa att informationen om personuppgiftsincidenter når alla som behandlar personuppgifter och som behöver kunna identifiera en incident. Den riktade utbildningen gällande personuppgiftincidenter har nått de anställda som kanske framför allt hanterar IT-system. Utöver dessa personer kan det finnas anställda som i sitt arbete kan tänkas upptäcka eller själva orsaka en incident, utan vetskap om att så är fallet. Med beaktande av att det inte finns några dokumenterade personuppgiftsincidenter ställer sig dataskyddsombudet tveksam till om anställda har tillräcklig kunskap om vad som utgör en incident. Dataskyddsombudet rekommenderar därför att bolaget ytterligare utbildar 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 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.
- Utbilda medarbetare om personuppgiftincidenter och hantering av dessa.
- Se över behovet av en rutin/plan för att kontinuerligt informera de anställda om personuppgiftsincidenter och den interna incidenthanteringen.

Bilagor

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