Fördjupad kontroll 2021

Hantering av personuppgiftsincidenter under 2020

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 2020. 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.

Rutiner och handlingsplaner

Göteborgs Spårvägar AB (GSAB) har en instruktion för hantering av personuppgiftsincidenter och en beskrivning av hur processen ska se ut vid en inträffad incident. Instruktionen fastställdes i december 2020 och innehåller en beskrivning av vad en personuppgiftsincident är och ett antal listade exempel. Därutöver anges det till vem som incidenten ska anmälas och vad anmälan ska innehålla. Det anges även kontaktuppgifter till bolagets dataskyddskontakt. Av processbeskrivningen går det bl.a. att utläsa att det är dataskyddskontakten som har till ansvar att analysera ärendet om personuppgiftsincident, diarieföra, göra en riskanalys och bedöma om det ska anmälas till tillsynsmyndigheten eller ej, samt kontakta dataskyddsombudet.

Av frågeunderlaget som ingick i kontrollens andra del framgår att bolaget använder sig av en metod/mall för riskanalys för att underlätta bedömningen av personuppgiftsincidenter.

Av det inskickade underlaget framgår att bolaget under år 2020 har upptäckt två personuppgiftsincidenter varav en förefaller ha anmälts till tillsynsmyndigheten.

Dataskyddsombudets rekommendationer

Bolaget har en instruktion som inledningsvis redogör för vad en personuppgiftsincident innebär. Den innehåller exempel på händelser som utgör en incident, vilket är positivt. Förutsatt att anställda har grundläggande kunskaper i dataskydd bör denna beskrivning vara tillräcklig för att kunna identifiera en personuppgiftsincident. Det är även positivt att det finns tydligt utpekade kontaktvägar och ansvar vid en misstänkt incident.

Så som ansvaret är fördelat (mellan dataskyddskontakt och tjänsteman i beredskap) är det av stor vikt att den som är ansvarig vid en incident vet hur denne ska gå tillväga. Instruktionen för hur en personuppgiftsincident ska hanteras bör därför vara detaljerad och pedagogisk. De dokument som i dagsläget utgör GSAB:s incidenthantering behöver läsas parallellt och saknar i stora delar beskrivningar av hur de olika bedömningarna ska göras. För att göra incidenthanteringen mindre sårbar bör det vara möjligt för flera personer inom bolaget att, med hjälp av stödjande dokument, korrekt bedöma och rapportera en incident. För att detta ska vara möjligt bör det finnas beskrivet vad en incident är, vilka steg som ska tas och hur man bedömer risken för de registrerade. Bedömningen av risken är avgörande för att korrekt kunna bedöma om incidenten ska anmälas till tillsynsmyndigheten eller ej, samt om de registrerade ska informeras. Om personuppgiftsincidenten är så pass allvarlig att de registrerade ska informeras bör det även finnas beskrivet i vilket skede detta ska ske, vad informationen ska innehålla och hur informationen ska förmedlas. Eftersom alla incidenter ska dokumenteras (även de som inte bedömts vara så allvarliga att de ska anmälas till tillsynsmyndigheten) bör det även finnas rutiner för hur denna dokumentation ska gå till och vad den ska innehålla.

En del av denna information går att utläsa ur det underlag som bolaget redan har men för att någon annan än dataskyddskontakten ska ha möjlighet att korrekt hantera en incident bör det kompletteras, förtydligas och konkretiseras. Att det finns förutsättningar för någon annan än dataskyddskontakten är av vikt särskilt eftersom personuppgiftsincidenter ska hanteras skyndsamt och anmälan till tillsynsmyndigheten ska göras inom 72 timmar.

Med tanke på att personuppgiftsincidenter kan vara komplicerade och svårutredda bör det också finnas instruktioner kring att, i de fall det är lämpligt, kontakta andra roller inom bolaget för att på ett tillfredsställande sätt kunna utreda incidenten. Detta är något som antagligen ter sig självklart för dataskyddskontakten men kan behöva tydliggöras i en instruktion eller rutin om det skulle falla på någon annan att utreda och rapportera.

Att bolaget enbart har två upptäckta incidenter under år 2020 kan vid första anblick uppfattas som något positivt och en indikation på att saker och ting fungerar som de ska. Det kan emellertid också vara ett tecken på att anställda saknar tillräcklig kunskap om hur man identifierar en incident eller att dessa inte rapporteras in.

Av frågeunderlaget framgår att information om personuppgiftsincidenter ges genom återkommande utbildningar och att det redogörs för på intranätet. Genom verksamhetsledningssystemet är även processen för personuppgiftsincidenter tillgänglig för alla anställda. Det är positivt att bolaget jobbar aktivt med att utbilda medarbetarna

och att det finns information att tillgå. Det framgår emellertid inte att det finns en rutin eller handlingsplan som anger hur man säkerställer att informationen når alla de som behandlar personuppgifter och som behöver kunna identifiera en incident. Eftersom dataskydd i de flestas dagliga arbete är en perifer fråga kan det även 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 inträffat.

Sammanfattning

- Instruktionen bör kompletteras med en beskrivning av hur bedömningen av risken för de registrerades fri- och rättigheter ska göras
- Instruktionen bör kompletteras med instruktioner om när de registrerade ska informeras, vad informationen ska innehålla och hur den ska tillhandahållas
- Incidenthanteringen bör göras mindre personberoende genom att tydliggöra och konkretisera instruktionerna så att fler kan följa dem
- Bolaget bör ha en rutin för att regelbundet informera sina anställda om den interna incidenthanteringen och göra det till en obligatorisk del av introduktionen för nyanställda.

Bilagor

1. Del 1 fördjupad kontroll personuppgiftsincidenter
2. Del 2 fördjupad kontroll personuppgiftsincidenter

Fördjupad kontroll 2021

Hantering av personuppgiftsincidenter under 2020

Del 1: Dokumentation för er att skicka in till ert dataskyddsombud:

1. Rutiner/handlingsplaner/instruktioner för att hantera personuppgiftsincidenter
2. Dokumentation av inträffade personuppgiftsincidenter
    a. Dokumentation av incidenter som har anmälts till tillsynsmyndigheten
    b. Dokumentation av incidenter som endast har dokumenterats internt
3. Dokumentation av utredningar kring potentiella personuppgiftsincidenter

Underlaget ska ha inkommit till ert dataskyddsombud **senast den 4 mars 2021.**

Har du frågor, kontakta ditt dataskyddsombud.

Fördjupad kontroll 2021

Hantering av personuppgiftsincidenter under 2020

Del 2

Frågor att besvara:

1. Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida händelsen är en personuppgiftsincident eller ej.
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
2. Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida incidenten ska anmälas till tillsynsmyndigheten.
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
3. Hur ni säkerställer att era anställda vet vad en personuppgiftsincident är och hur de ska gå tillväga vid inträffade personuppgiftsincidenter.

Svaren ska ha inkommit till ert dataskyddsombud **senast den 16 april 2021.**

Har du frågor, kontakta ditt dataskyddsombud.