Fördjupad kontroll 2021

Hantering av personuppgiftsincidenter under 2020 (Göteborgs Stads Kollektivtrafik AB)

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.

Göteborgs Stad Kollektivtrafik AB:s hantering av personuppgiftsincidenter

Rutiner och handlingsplaner

Göteborgs Stads Kollektivtrafik AB (GSK) har till dataskyddsombudet skickat in de beskrivningar och instruktioner som medarbetare har tillgång till. Detta underlag består av en beskrivning av vad en personuppgiftsincident är samt några listade exempel. Därutöver anges det till vem som incidenten ska anmälas och kort om vad anmälan ska innehålla. Dataskyddskontakten har till uppgift att analysera ärendet och bedöma om det utgör en personuppgiftsincident eller ej. Dataskyddskontakten har sedan till uppgift att diarieföra ärendet, genomföra en risk- och konsekvensanalys samt bedöma om händelsen innebär en incident och om det ska upprättas en anmälan till tillsynsmyndigheten. Dataskyddskontakten ska även informera dataskyddsombudet, återkoppla till berörda samt chef och utifrån risk- och konsekvensanalysen ska även orsaken till incidenten åtgärdas. Bilagd till denna instruktion finns även en processkarta som i korta ordalag beskriver hur en personuppgiftsincident ska hanteras.

Av frågeunderlaget som skickats in till dataskyddsombudet i del två av den fördjupade kontrollen angavs även att om en medarbetare misstänker en personuppgiftsincident ska denne kontakta sin chef som samlar in grundläggande information om incidenten. Chefen kontaktar sedan dataskyddskontakt.

Inträffade personuppgiftsincidenter under 2020

Av det inskickade underlaget framgår att bolaget under år 2020 har upptäckt en personuppgiftsincident. Denna har anmälts till tillsynsmyndigheten.

Information om incidenthantering till anställda

I frågeunderlag angavs även att frågan om GDPR har en stående punkt på bolagsledningsmötena varannan vecka och att tanken varit att det även ska finnas med på agendan för arbetsplatsträffar (APT). Det är enligt bolaget på detta som man säkerställer att medarbetare vet vad en personuppgiftsincident, hur man ska gå tillväga om en sådan misstänks samt hur man säkerställer att alla vet var information om detta finns att finna.

Dataskyddsombudets rekommendationer

Rutiner och handlingsplaner

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 för de flesta delar av incidenthanteringen finns utpekade kontaktvägar och ansvar vid en misstänkt incident.

Ansvaret vid en misstänkt incident är på olika sätt uppdelat inom bolaget. Medarbetare har ett ansvar för att rapportera misstänkta incidenter, chefer att utreda och dela information vidare. Därefter faller det till stor del (under kontorstid) på dataskyddskontakten att ansvara för den efterföljande hanteringen. Övrig tid är det tjänsteman i beredskap som har ansvaret. Utifrån denna uppdelning kan det konstateras att alla medarbetare behöver ha kunskap om vad en incident är. Chefer behöver ytterligare kunskap om de på ett tillfredsställande sätt ska kunna samla relevant information om incidenten. Dataskyddskontakt och de som kan utgöra tjänsteman i beredskap behöver därtill ha kunskap om hur en bedömning av risk ska göras för att kunna avgöra om en incident ska anmälas till tillsynsmyndigheten och ifall de registrerade ska informeras.

Det framgår när dataskyddskontakten och tjänsteman i beredskap har ansvar, men det framgår inte vem som har ansvar om dataskyddskontakten skulle vara frånvarande under kontorstid vid t.ex. sjukdom eller semester. Mot bakgrund av att incidenter ska hanteras skyndsamt och anmälan till tillsynsmyndigheten ska göras inom 72 timmar bör det finnas möjlighet och förutsättningar för flera inom bolaget att på ett korrekt sätt hantera incidenter. För att säkerställa att incidenter hanteras rätt, i rätt tid och att bedömningar görs på ett konsekvent och korrekt sätt bör det finnas detaljerade, pedagogiska och dokumenterade instruktioner. Den instruktion som i dagsläget utgör GSK:s incidenthantering är kortfattad, i vissa delar otydlig eller felaktig och saknar instruktioner för hur och när bedömningar ska göras. Som framgår ovan finns det även luckor i ansvarsfördelningen.

Dataskyddsombudet rekommenderar därför att bolaget kompletterar och tydliggör instruktionen och därmed gör det möjligt för fler personer inom bolaget att korrekt bedöma och rapportera en incident. Dataskyddsombudet rekommenderar att det i instruktionen tydliggörs vilka steg som ska tas vid en misstänkt incident och hur man bedömer risken för de registrerade. 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 anmälts till tillsynsmyndigheten) bör det även finnas rutiner för hur denna dokumentation ska gå till och vad den ska innehålla.

Inträffade personuppgiftsincidenter under 2020

Att bolaget enbart har en upptäckt incident under år 2020 kan initialt 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. Bolaget har under slutet av 2020 genomfört en utbildningsinsats för medarbetarna där de fått information om personuppgiftsincidenter. Dataskyddsombudet rekommenderar att bolaget bevakar frågan om inrapporterade incidenter och eventuellt ser över behovet av ytterligare informationsinsatser.

Information om incidenthantering till anställda

Att information om dataskydd/GDPR är en stående punkt på bolagsledningens möten är positivt och visar att bolaget arbetar aktivt med frågan om dataskydd. Att det även är tänkt att tas upp på APT är positivt, förutsatt att det faktiskt sker. Det framgår inte att det finns en dokumenterad rutin för hur man säkerställer att informationen når alla anställda eller ifall det är en del av introduktionen för nyanställda. GSK rekommenderas därför att ta fram en plan för att säkerställa detta. Det kan även finnas anledning att med viss regelbundenhet påminna de anställda om vad en personuppgiftsincident är och vad man ska göra om man misstänker att en har inträffat. Mot bakgrund av det låga antalet upptäckta incidenter under 2020 är detta något bolaget bör ta med sig framåt i sitt dataskyddsarbete.

Sammanfattning

- Instruktionen bör tydliggöras och kompletteras med en beskrivning av hur bedömningen av risken för de registrerades fri- och rättigheter ska göras.
- Instruktionen bör kompletteras med beskrivning av när de registrerade ska informeras, vad informationen ska innehålla och hur den ska tillhandahållas.
- Bolaget bör ha en rutin/plan 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.