Göteborgs Stad

Årsrapport för dataskyddsarbetet 2021

Göteborgs Spårvägar AB

2021-12-22

Innehåll

1 Dataskyddsarbetet

1.1 Att förvalta ett förtroende

Att få ta del av och hantera andra människors personliga uppgifter innebär att förvalta ett stort förtroende. Dataskyddsförordningen har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Lagen har höga sanktionsavgifter, men det är inte därför det är viktigt att lagen följs. Att personuppgifter hanteras lagenligt bör snarare vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Enligt lagstiftningen har dataskyddsombudet bland annat till uppgift att ge råd och information till den personuppgiftsansvarige i dataskyddsfrågor. Dataskyddsombudet har även till uppgift att övervaka efterlevnaden av dataskyddsförordningen hos personuppgiftsansvariga.

Dataskyddsombudet ska enligt lagstiftningen rapportera till högsta förvaltningsledning dvs. styrelse eller nämnd. Detta för att den högsta ledningen ska få den information som behövs för att kunna bedöma vilka prioriteringar som ska göras och vilka risker som organisationen är beredd att ta. Dataskyddsombudet fattar inte beslut åt verksamheten. Ytterst vilar ansvaret för att verksamheterna följer lagen på nämnd/styrelse. De råd och rekommendationer som ges av dataskyddsombudet syftar till att ge ledningen underlag för att kunna fatta väl underbyggda beslut.

1.2 Dataskyddsenhetens gemensamma arbete

Dataskyddsenheten har under det gångna året regelbundet skickat ut nyhetsbrev innehållandes omvärldsbevakning och information från enheten. Däremellan har enheten även informerat verksamheterna om förändringar i lagstiftning och praxis.

Enheten har också tillgängliggjort en digital grundutbildning som alla stadens bolag och förvaltningar har fått tillgång till, och som fritt kan användas av verksamheterna. Det har även arrangerats ett flertal lärarledda utbildningar, bland annat en grundutbildning och en utbildning riktad till yrkesgruppen kommunikatörer. Genom att hålla utbildningarna digitalt har flera hundra personer inom stadens verksamheter haft möjlighet att delta. Då intresset varit stort kommer dataskyddsenheten fortsätta anordna utbildningar inom olika ämnesområden.

För att skapa möjligheter för samarbete och erfarenhetsutbyte i dataskyddsfrågor har enheten under året anordnat två nätverksträffar för stadens dataskyddskontakter. Teman för nätverksträffarna har anpassats utefter de frågor enheten identifierat att många av stadens verksamheter arbetar med.

2 Kontrollarbetet

2.1 Ett systematiskt arbete

Dataskyddsenheten har under året tagit fram gemensamma rutiner för kontrollarbetet, med syfte att skapa ett enhetligt, transparent och systematiskt arbetssätt för Göteborgs Stads verksamheter. Kontrollerna följer en årsplan, nedan kallad ”Kontrollplan”.

Kontrollplanen skickades ut i januari 2021, med en redogörelse för planerade kontroller under året samt relevanta tidpunkter. Kontrollplanen redogjorde dels för två fördjupade kontroller, som valdes ut efter verksamhetens riskområden, dels återkommande fasta kontrollpunkter som årligen kommer att stämmas av för att se var verksamheten befinner sig i sitt dataskyddsarbete. Av kontrollplanen framgick också att en uppföljning kommer att ske av tidigare lämnade rekommendationer.

Under första halvåret har dataskyddsombudet genomfört de fördjupade kontrollerna. Under andra halvåret har dataskyddsombudet genomfört en kontroll av de fasta kontrollpunkterna samt gjort en uppföljning av tidigare lämnade rekommendationer i tidigare utförda kontroller.

2.2 Rättsutveckling som påverkat kontrollarbetet under året

Rättsutvecklingen under året har föranlett dataskyddsombudet att särskilt uppmärksamma behandlingen av personuppgifter som påverkats av nya rättsfall och rekommendationer. Ett antal händelser har också gjort att enheten har haft anledning att analysera stadens struktur rörande kommungemensamma interna tjänster.

2.2.1 Tredjelandsöverföringar (överföringar till länder utanför EU/EES)

I juli 2020 kom en dom från EU-domstolen kallad Schrems II-domen. Frågan i målet var om det avtal som fanns mellan EU och USA gav tillräckligt skydd för personuppgifter för att dessa lagligen skulle få överföras till USA. Frågeställningen i sig var väckt med anledning av den omfattande datainsamling som amerikansk lagstiftning möjliggör för amerikanska säkerhetsorgan av icke-amerikanska medborgares uppgifter. Rättsfallet rörde bulkinsamling av data ”in transit” men frågan är principiellt intressant eftersom i princip alla verksamheter som faller under amerikansk jurisdiktion kan förmås överlämna annans data, även i de fall denna finns utanför USA. Domstolen ogiltigförklarade avtalet och fastslog att det kan krävas omfattande säkerhetsåtgärder för att kunna överföra uppgifter till USA eller andra länder med liknande lagstiftning. Skyddsåtgärderna behövde i princip omöjliggöra för utländska myndigheter att kunna få del av uppgifterna, genom

exempelvis kryptering eller anonymisering. Domen har fått stor påverkan, och sedan den kom har därför frågan om tredjelandsöverföringar varit ständigt aktuell. Under året har också några vägledningar publicerats av Europeiska dataskyddsstyrelsen, EDPB, ett organ där samtliga länders tillsynsmyndigheter samverkar. Domen har inneburit att en översyn av aktuella personuppgiftsbehandlingar har behövt ske för att ta reda på om någon överföring sker till USA eller i vissa fall även annat land. Begreppet överföring är dessutom brett och inkluderar även att ge någon i USA åtkomst till uppgifter, även när uppgifterna befinner sig inom EU. Domstolen har uppmanat tillsynsmyndigheterna i respektive land att börja agera i frågan.

Kommentarer och rekommendationer

Om denna översyn ännu inte genomförts rekommenderar dataskyddsombudet att detta arbete prioriteras, så att verksamheten får en tydlig riskbild och kan vidta åtgärder eller fatta nödvändiga beslut.

2.2.2 Rätt beslutsnivå

Frågan om tredjelandsöverföringar har varit omfattande och har berört såväl användningen av olika system (M365, Google) som sociala medier, cookies, osv. Frågan är komplex eftersom stora investeringar gjorts under den tid som avtalet mellan EU och USA var i kraft och förutsättningarna nu ändrats. Det har också förelegat en osäkerhet om USA tänker ändra sin lagstiftning, om leverantörerna kommer att skapa nya koncernkonstellationer eller om nya förhandlingar mellan EU och USA kan leda till ett nytt avtal (vilket idag endast är möjligt om amerikansk lagstiftning först ändras). Mer än ett år har dock passerat sedan domen kom och några nya lösningar för att kunna överföra personuppgifter till USA i klartext finns fortfarande inte. Det innebär att det idag i de flesta fall saknas lagliga möjligheter för överföring av personuppgifter till USA. Om en verksamhet väljer att fortsätta att behandla personuppgifter utan att ha säkerställt en laglig överföring så innebär detta ett accepterande av risk för förtroendeskada, skadestånd och sanktionsavgift. Ett accepterande skulle även kunna förstås som att man medvetet väljer att bryta mot gällande lagstiftning och riskera de registrerades fri- och rättigheter.

Kommentarer och rekommendationer

Nämnd/styrelse är ansvarig för att verksamheten följer lagen. Nämnd/styrelse rekommenderas att säkerställa att beslut som innebär en avvikelse från gällande dataskyddslagstiftning fattas på behörig nivå.

2.2.3 Kommungemensamma interna tjänster

De kommungemensamma interna tjänsterna erbjuds och levereras idag av Intraservice. Vad som utgör en kommungemensam intern tjänst beslutas av

stadsdirektören, på delegation av kommunstyrelsen, efter samråd med förvaltnings- och bolagsledningar.

Enligt stadens styrande dokument så är det för många av stadens verksamheter obligatoriskt att använda tjänsterna. I vissa fall pekar styrande dokument ut exakt vilket system som utgörs av tjänsten, tex. M365, medan det i andra fall endast anges typ av tjänst. Intraservice roll innebär att upphandla och/eller teckna avtal med en underleverantör för stadens räkning. I styrande dokument anges att Intraservice ska betraktas som leverantör och därmed ett personuppgiftsbiträde (dvs. någon som behandlar personuppgifter för annans räkning) åt stadens bolag och förvaltningar.

Den personuppgiftsansvarige är den som bestämmer ändamål och medel med en behandling. I normala fall är det respektive bolag och nämnd som är personuppgiftsansvarig för de personuppgiftsbehandlingar som sker inom verksamheten. När det kommer till stadens kommungemensamma interna tjänster blir detta dock ofta problematiskt eftersom majoriteten av verksamheterna inte alltid har någon möjlighet att påverka ändamål och oftast inte har någon reell möjlighet att påverka medel för behandlingar som sker inom dessa tjänster. Utifrån detta uppstår frågor om vilket ansvar som Intraservice och kommunstyrelsen har för dessa tjänster, samt hur stadens struktur för kommungemensamma interna tjänster påverkar fördelningen av personuppgiftsansvaret för de behandlingar där dessa tjänster används. Oaktat vad som anges i styrande dokument skulle utgångspunkten, vid en rättslig prövning, vara vem som faktiskt hade rådighet att besluta om ändamål och medel.

Kommentarer och rekommendationer

Utifrån ett ansvarsperspektiv, då sanktionsavgifter riktas mot den som är personuppgiftsansvarig, samt eftersom frågan berör dataskyddsarbetet inom alla de förvaltningar och bolag som använder dessa tjänster, rekommenderar dataskyddsombudet att frågan om roller och ansvar utreds och tydliggörs i kommande styrmodell.

Flera av de kommungemensamma interna tjänsterna medför dessutom risker ur ett dataskyddsrättsligt perspektiv, särskilt kopplat till tredjelandsöverföringar. Dataskyddsenheten har uppmärksammat att det ofta är oklart i vilken utsträckning som stadens förvaltningar och bolag är medvetna om dessa risker och det egna ansvar man har för att hantera dem i rollen som personuppgiftsansvarig.

Förvaltningar och bolag rekommenderas säkerställa att de har tillgång till komplett och aktuell information/fakta om de tjänster som används, samt att de har kompetens att bedöma riskerna för sina behandlingar utifrån ett verksamhetsperspektiv.

2.3 Årets kontrollarbete

2.3.1 Fördjupade kontroller

De fördjupade kontrollerna har bestått av en kontroll av förvaltningens hantering av personuppgiftsincidenter under 2020, samt av en kontroll av hantering av anställdas personuppgifter via positioneringsteknik (GPS). Dessa genomfördes under våren och presenterades för styrelsen i augusti 2021.

Dataskyddsombudet har i rapporten avseende de fördjupade kontrollerna haft vissa anmärkningar och därför lämnat ett antal rekommendationer till verksamheten. Hur verksamheten har hanterat dessa rekommendationer har följts upp under hösten.

2.3.2 Fasta kontrollpunkter

För att ge verksamheten en bild av hur långt man har kommit i det systematiska dataskyddsarbetet har dataskyddsenheten tagit fram en enkät utifrån de fasta kontrollpunkterna. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Enkäten består av tolv punkter där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Verksamheten har fått besvara frågorna utifrån aktuellt läge inom verksamheten.

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten har utifrån svaren på den enkät som skickats ut från dataskyddsenheten fått ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[1]

Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt. Enkäten kommer att upprepas kommande år. Avsikten med detta arbetssätt är att både att få en bild av nuläget och att kunna åskådliggöra de förändringar som vidtas över tid. Enkäten har ej främst för avsikt att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

[1] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

Beskrivning av risknivåer

Risknivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

2.4 Resultat av fasta kontrollpunkter för Göteborgs Spårvägar AB

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Kommentarer och rekommendationer:

Bolaget har på nästan alla påståenden på denna punkt skattat sitt arbete högt. Det som anges som ett tydligt förbättringsområde är att ha rutiner för att regelbundet involvera dataskyddsombudet.

Dataskyddsombudet instämmer överlag i bolagets skattning men vill understryka att för att dataskydd ska anses vara en naturlig och integrerad del i det dagliga arbetet krävs det att man inom alla delar av verksamheten har tillräcklig kunskap om dataskydd. I detta ingår att ha tillräckliga kunskaper för att kunna flagga för när personuppgiftsbehandlingar sker på ett felaktigt eller osäkert sätt och när åtgärder kan behöva vidtas.

Utifrån skattningen rekommenderas att bolaget tar fram rutiner som säkerställer att dataskyddsombudet på ett mer systematiskt sätt informeras om och involveras i alla frågor rörande dataskydd.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Kommentarer och rekommendationer:

Bolagets skattning på denna punkt indikerar att verksamheten anser sig ha mycket goda förutsättningar för att identifiera och hantera personuppgiftsincidenter. Däribland har bolaget via sin skattning angett att det finns dokumenterade rutiner som ger goda förutsättningar för att upptäcka och utreda incidenter. I denna punkt ingår en skattning kring hur väl rutinen/rutinerna är kända för alla medarbetare inom verksamheten.

Utifrån skattningen rekommenderar dataskyddsombudet att bolaget tar fram rutiner som säkerställer att inträffade personuppgiftsincidenter rapporteras in till tillsynsmyndigheten inom den angivna tidsramen om 72 h. Bolaget rekommenderas också att ta fram en långsiktig plan och rutiner som säkerställer att medarbetare regelbundet ges utbildning och information om vad en personuppgiftsincident är och hur dessa ska hanteras.

Dataskyddsombudet genomförde under våren/sommaren 2021 en fördjupad kontroll avseende just hanteringen av personuppgiftsincidenter inom bolaget. Denna visade på vissa förbättringsområden och dataskyddsombudet gav i samband med detta några rekommendationer. Vidare kommentarer om den fördjupade kontrollen, de rekommendationer som lämnades och uppföljningen därav framkommer under avsnitt 2.6.2.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kommentarer och rekommendationer:

Bolaget har på denna punkt angivit genomgående låga värden i sin skattning vilket innebär att det utgör ett riskområde med omfattande risker där det omgående behöver vidtas åtgärder. Enkätsvaren visar till exempel att bolaget uppskattningsvis enbart har tecknat avtal med ca 25 % av de personuppgiftsbiträden som bolaget anlitar. Då avsaknaden av biträdesavtal utgör en hög risk för bolaget rekommenderar dataskyddsombudet att det omgående genomförs en kartläggning av behandlingar där biträden anlitas, och därefter tecknar personuppgiftsbiträdesavtal där det saknas.

Bolaget anger vidare att det saknas rutiner för att kontrollera anlitade biträden samt för att vid anlitande av nya biträden kontrollera deras underbiträden. Utifrån det ansvar som bolaget har vid användningen av biträden enligt artikel 28 GDPR (den s.k. ”omsorgsplikten”) föreligger här en risk för att bolaget inte kan uppfylla kraven enligt GDPR.

Dataskyddsombudets rekommenderar att det tas fram rutiner för att identifiera, kontrollera och reglera förhållandet med personuppgiftsbiträden och eventuella underbiträden. I denna bel behöver det också säkerställas att det inom bolaget finns tillräcklig kompetens för att bedöma om anlitade biträden och deras underbiträden uppfyller kraven enligt GDPR. Det rekommenderas också att bolaget tar fram rutiner som säkerställer att personuppgiftsbiträdesavtal regelbundet följs upp och att det då kontrolleras att överenskomna villkor uppfylls. Det behöver även tas fram rutiner för att säkerställa att andra nödvändiga överenskommelser eller avtal tecknas när det finns en gemensam eller delad hantering av personuppgifter.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Kommentarer och rekommendationer:

Bolagets samlade skattning på denna punkt visar att detta är ett omfattande riskområde som kräver åtgärder.

Utöver att det i de flesta fall är ett krav enligt förordningen att ha ett aktuellt och uppdaterat personuppgiftsregister, kan det också vara ett användbart hjälpmedel i verksamhetens dataskyddsarbete då det ger en överblick över de behandlingar som sker. Dataskyddsombudet rekommenderar bolaget att prioritera arbetet med personuppgiftsregistret. Bolaget rekommenderas också att ta fram en rutin för att kontinuerligt uppdatera registret för det fall det tillkommer behandlingar eller om behandlingar ändras.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Kommentarer och rekommendationer:

Bolagets svar indikerar att det inom denna kontrollpunkt finns omfattande risker som omgående kräver åtgärder. En avsaknad av överblick och tydlig styrning i hur dataskyddsarbetet bedrivs innebär stora risker eftersom man bland annat riskerar att fokusera sina resurser på fel frågor.

Ett systematiskt dataskyddsarbete bör bedrivas utifrån övergripande och långsiktiga strategier för verksamheten avseende både dataskydd och informationssäkerhet. Dataskyddsombudet rekommenderar därför att bolaget tar fram styrande dokument som reglerar personuppgifter och tar fram rutiner för att hålla dessa uppdaterade. Dessa dokument behöver också synliggöras för medarbetarna. Utifrån skattningen rekommenderar dataskyddsombudet att bolaget tar fram en informationssäkerhetspolicy som anger hur personuppgifter kan/får behandlas i exempelvis IT-system, datorer och mobila enheter. Bolaget rekommenderas också att samordna dataskyddsarbetet med informationssäkerhetsarbetet. Av vikt är även att säkerställa att verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet. Verksamheten rekommenderas också att ta fram rutiner för att regelbundet genomföra kontroller för att se hur dataskyddsförordningen efterlevs.

Dataskyddsombudet lämnar också en övergripande rekommendation om att i dokumenterade handlings- och/eller verksamhetsplan, rutiner och policys tydliggöra sin strategi för det övergripande dataskyddsarbetet. I detta ingår att beakta vilka resurser som behöver avsättas för att säkerställa dataskyddsarbetet. Här vill dataskyddsombudet skicka med att det är viktigt att se långsiktigt på detta arbete vilket innebär att bolaget inte bör förlita sig på punktinsatser genomförda av tillfälliga konsulter.

2.4.6 Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Kommentarer och rekommendationer:

Bolagets skattning i denna del indikerar att detta utgör ett förbättringsområde för bolaget. Skattningen indikerar att verksamheten inte anser att den allmänna kunskapsnivån ger goda förutsättningar i dataskyddsarbetet och att det saknas rutiner för att följa upp och bibehålla kunskapsnivån hos medarbetare.

En adekvat kunskapsnivå hos de medarbetare som i sitt arbete behandlar personuppgifter är en grundläggande förutsättning för dataskyddsarbetet i stort. Bolaget rekommenderas därför att genomföra utbildningsinsatser och ta fram en långsiktig utbildningsplan för att säkerställa medarbetarnas kunskapsnivå och bibehålla den över tid. I detta arbete kan bolaget få stöd från dataskyddsenheten

som regelbundet erbjuder utbildningar inom dataskydd, både sådana som är riktade till hela staden och verksamhetsspecifika.

2.4.7 Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Kommentarer och rekommendationer:

Vad gäller bolagets integritetspolicy besvaras dessa påståenden med mycket varierande skattningar. Det anges bl.a. att policyn uppfyller kraven enligt GDPR och att det finns dokumenterade rutiner för att informera medarbetare om hur deras personuppgifter behandlas. Påståendena kopplade till att tillhandahålla informationen till de registrerade och att kontinuerligt se över och uppdatera policyn, samt att den är nåbar från samtliga kanaler skattas lågt och utgör därför klara förbättringsområden.

Dataskyddsombudet instämmer delvis i bolagets skattning och vet att det pågått och pågår ett arbete med interna och externa integritetspolicys i verksamheten. Såvitt dataskyddsombudet kan se är detta dock ännu inte genomfört och den information som i skrivande stund finns att få via bolagets hemsida är i stora delar inaktuell. Bolaget rekommenderas att säkerställa att de registrerade på ett enkelt och tydligt sätt får tillgång till den information som de har rätt till enligt GDPR. Bolaget rekommenderas även att ta fram rutiner som anger både instruktioner kring när/hur policyn ska uppdateras och också utpekar vem/vilken roll inom bolaget som ansvarar för att detta görs.

2.4.8 Kontrollpunkt 8: Mejl och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för mejl och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kommentarer och rekommendationer:

Bolaget har på denna punkt angett mycket varierande värden med konsekvensen att man placerar sig inom riskområde tre. Dataskyddsombudet gör i vissa delar en avvikande bedömning än den som bolaget gör. Särskilt gäller detta skattningen kopplad till påståendet om att ha rutiner för att kontrollera att handlingar innehållandes personuppgifter gallras.

Vid kontakt med bolaget under det gångna året har det flera gånger angetts att bolaget har flertalet system innehållandes stora mängder personuppgifter som sannolikt borde gallras. Därför är det i viss mån förvånande att bolaget på denna punkt anger att detta inte på något sätt är ett förbättringsområde. Det är positivt att det finns en dokumenthanteringsplan med angivna gallringsfrister, men denna utgör bara ett viktigt verktyg så länge den faktiskt tillämpas. Utifrån dataskyddsombudets uppfattning rekommenderas bolaget att utföra kontroller i samtliga system som innehåller personuppgifter och kontrollera att dessa gallras.

Utifrån skattningen i övrigt står det även klart att bolaget behöver informationsklassificera sina personuppgiftsbehandlingar och säkerställa att de klassningar som gjorts är aktuella. Bolaget rekommenderas också att ta fram anvisningar för hur information i de olika informationsklasserna får hanteras och lagras. Bolaget rekommenderas också att säkerställa att de registrerade, vid kontakt med bolaget, får information om hur deras personuppgiftsbehandlingar hanteras.

Vid genomgång av kontrollpunkterna med bolaget framkom det att det pågår ett arbete med rutiner som berör detta område. Resultatet av detta förbättringsarbete kommer att illustreras i 2022 års rapport.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Kommentarer och rekommendationer:

Avseende konsekvensbedömningar skattar bolaget sitt arbete på flertalet påståenden mycket högt. Sammantaget går det att utläsa att det finns risker identifierade som bör åtgärdas men att dessa inte bedöms vara brådskande, omfattande eller allvarliga. Det som skattas lågt är hur stor andel av personuppgiftsbehandlingarna som kontrollerats utifrån höga risker samt hur stor andel behandlingar som det finns genomförda eller pågående konsekvensbedömningar för. I denna del instämmer dataskyddsombudet som under det senaste året fått lämna kommentarer på två konsekvensbedömningar, varav ingen, i skrivande stund, är slutförd.

Mot bakgrund av att bolaget fortfarande befinner sig i början av sitt arbete med konsekvensbedömningar är det dataskyddsombudets uppfattning att det oklart om det finns fog för den höga skattningen. Dataskyddsombudets bild är att bolaget håller på att utveckla sitt arbete och att de rutiner som finns ännu inte har fått chans att helt bli testade. Särskilt oklart är det gällande rutinen för att följa upp de åtgärder som beslutats i en konsekvensbedömning i och med att ingen konsekvensbedömning hittills färdigställts, och det därmed inte heller har funnits några åtgärder att följa upp.

Att genomföra konsekvensbedömningar är i många fall ett krav enligt GDPR och om detta inte genomförs riskerar man att missa att vidta åtgärder som behövs för att säkerställa de registrerades rättigheter. Vid en tillsyn kan det också innebära sanktionsavgifter från tillsynsmyndigheten. Arbetet med konsekvensbedömningar behöver inledas i ett tidigt skede vid nya eller förändrade behandlingar och vid införanden behöver man ta höjd för att arbetet kräver tid, resurser och korrekt kompetens.

Dataskyddsombudet rekommenderar att bolaget kartlägger de personuppgiftsbehandlingar som kan innebära en hög risk för registrerades fri- och rättigheter. Därefter bör en handlingsplan tas fram för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Kommentarer och rekommendationer:

Bolaget har på denna punkt skattat sitt arbete med i snitt medellåga värden. Dataskyddsombudet har ingen anledning att göra en annan bedömning än den som bolaget här gör. Dataskyddsombudet under det gångna året tillfrågats gällande ett IT-projekt/upphandling som innefattar personuppgiftsbehandlingar. Om detta beror på att det är det enda pågående projektet av detta slag inom bolaget eller om det beror på att dataskyddsombudet inte involverats är för dataskyddsombudet oklart.

Överlag är detta ett förbättringsområde för bolaget och man rekommenderas att ta fram tydliga processer för hur dataskydd ska integreras i dessa frågor. Bolaget rekommenderas också ta fram rutiner för att säkerställa att kravställningen anpassas efter reglerna om dataskydd i GDPR, vari det ingår att säkerställa att verksamheten följer reglerna som gäller för tredjelandsöverföringar.

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kommentarer och rekommendationer:

Bolaget har på denna punkt överlag skattat sitt dataskyddsarbete lågt. Sammantaget indikerar detta att bolaget inte anser sig ha överblick över sina IT-system och digitala verktyg, kontroll över hur det ges tillgång/behörighet till dessa och hur användandet följs upp och kontrolleras. Dataskyddsombudet delar denna bedömning och rekommenderar bolaget att kartlägga alla de IT-system och digitala verktyg som används och säkerställa att de har kontrollerats för följsamhet mot GDPR.

Bolaget skattar sitt arbete något högre vad gäller användning av kakor (cookies) på webbsidor. Här kan dataskyddsombudet konstatera att bolaget efter den genomgång av kontrollpunkterna som hölls med verksamheten, där dataskyddsombudet anmärkte på avsaknad av information, har tagit fram en s.k. "cookiebanner" som ger information om hur kakor (cookies) samlas in. Dataskyddsombudet har inte kontrollerat insamlingen av kakor eller den information som ges men anser det mycket positivt att bolaget agerat direkt efter att bristen påtalats.

2.4.11.1 Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Kommentarer och rekommendationer:

Sammantaget går det, utifrån skattningen, att utläsa bolaget anser sig ha goda förutsättningar för att hantera de registrerades rättigheter. Dataskyddsombudet har endast ett fåtal gånger blivit tillfrågad angående begäran från registrerade rörande deras rättigheter, men har inte heller några indikationer som tyder på att skattningen skulle vara missvisande eller felaktig.

Av skattningen kan det utläsas att det inom bolaget saknas en medvetenhet om de registrerades rättigheter och att det saknas en dokumenterad process för att hitta/få tillgång till efterfrågad information vi en begäran om registerutdrag. Därför rekommenderas bolaget att inkludera information om registrerades rättigheter i den utbildning som ges till medarbetare avseende dataskydd i övrigt. Det är också viktigt att den kartläggning som rekommenderas under kontrollpunkt 11 genomförs för att därigenom få överblick över vilka system och verktyg som det behöver göras sökningar i, för att sedan ta fram en process för att säkerställa en korrekt hantering av frågor rörande registerutdrag.

2.5 Särskilda iakttagelser

2.5.1 Tredjelandsöverföring och användningen av sociala medier

De flesta sociala medier som används inom staden är ägda av amerikanska organisationer som i sina avtalsvillkor anger att överföring till tredjeland sker. Eftersom en behandling av personuppgifter i sociala medier därmed innebär en otillåten tredjelandsöverföring har frågan om användandet av dessa plattformar varit, och fortsätter att vara, högaktuell. Dataskyddsenheten har tillsammans med stadsledningskontoret tagit fram rekommendationer till stadens förvaltningar och bolag för hanteringen av sociala medier. Denna rekommendation utgår ifrån att alla helst ska avstå från att behandla personuppgifter i sociala medier, såvida inte risk för otillåten tredjelandsöverföring kan uteslutas. Om en verksamhet väljer att fortsätta att behandla personuppgifter i sociala medier innebär detta ett accepterande av risk som det bör fattas ett beslut om på lämplig nivå.

Såvitt dataskyddsombudet vet har bolaget inte fattat något formellt beslut avseende användningen av sociala medier i verksamheten. Om verksamheten använder sociala medier och planerar att fortsätta med detta bör ett sådant beslut fattas.

2.6 Uppföljning

2.6.1 Uppföljning av genomförd kontroll 2018

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll 1 (2018): Organisatoriska förutsättningar för dataskyddsarbetet.

Kontrollen genomfördes under 2018 och det beskrevs då att bolagets dataskyddsorganisation stod i startgroparna. Bolaget rekommenderades att säkerställa att gå från förslagsfas till en genomförandefas. Bolaget rekommenderades också att vidareutveckla den externa integritetspolicyn.

Uppföljningen av denna kontroll har genomförts inom ramen för den skattning som bolaget gjorde via den utskickade enkäten. Den visade att det fortfarande finns vissa åtgärder som behöver vidtas för att säkerställa att bolaget har en tydlig och ändamålsenlig dataskyddsorganisation. Särskilt vad gäller att hitta rutiner för att på ett mer systematiskt sätt involvera dataskyddsombudet i frågor som rör dataskydd. Kommentarer och rekommendationer är lämnade under avsnitt 2.4.1 ”Kontrollpunkt 1: Dataskyddsorganisation”.

Kontroll 2 (2020): Granskning av utbildningsnivå i dataskydd

Kontrollen genomfördes under våren 2020 och presenterades för styrelsen maj samma år. Kontrollen presenterades i en rapport som var gemensam för Göteborgs Spårvägar AB, GS Buss AB och GS Trafikantservice AB. Resultatet av kontrollen

visade att bolagen vid denna tid inte genomfört några större utbildningsinsatser och att kunskapsnivån var varierande. Kunskapsluckor identifierades både gällande hantering av personuppgiftsincidenter och grundläggande delar av dataskyddslagstiftningen, t.ex. vem som är personuppgiftsansvarig och vad som utgör en personuppgift. Utifrån detta rekommenderades bolagen att ta fram en konkret utbildningsplan, kartlägga vilka yrkesgrupper som har störst behov av utbildning samt synliggöra nuvarande rutiner för hantering av personuppgifter. Bolagen rekommenderades också att fokusera på att ge anställda tillräcklig kunskap om personuppgiftsincidenter och hanteringen därav.

Uppföljningen av denna kontroll har genomförts både genom en fördjupad kontroll under våren/sommaren 2021 samt inom ramen för den skattning som bolaget gjorde via den utskickade enkäten. Dessa visar att det finns fortsatt förbättringsutrymme. Rekommendationer för det fortsatta arbetet lämnas under avsnitt 2.4.6 ”Kontrollpunkt 6: Utbildning” samt under nedanstående avsnitt (2.6.2, Kontroll 2).

2.6.2 Uppföljning av genomförda kontroll 2021

Verksamheten har fått en kort enkät med frågor om åtgärder har vidtagits med anledning av dataskyddsombudets lämnade rekommendationer för de genomförda kontrollerna under våren 2021.

Kontroll 1 (2021): Hanteringen av personuppgiftsincidenter 2020

Verksamheten gavs följande rekommendationer:

- 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.

Verksamheten har i svaret på de uppföljningsfrågor som skickades ut angett att ett antal åtgärder har vidtagits och/eller planeras. Bl.a. är processen för incidenter uppdaterad och dataskyddsorganisationen planeras att under 2022 utökas med dataskyddssamordnare för att minska personberoendet. Det har också genomförts informationsinsatser och bolagets intranät är uppdaterad med information om personuppgiftsincidenter. Det framgår inte att bolaget har genomfört eller planerar någon åtgärd kopplad till den sista rekommendationen om att ta fram en rutin för att regelbundet informera sina anställda. En rekommendation kopplad till detta framgår också under avsnitt 2.4.2 ”Kontrollpunkt 2: Personuppgiftsincidenter”.

Framåt rekommenderar dataskyddsombudet också att bolaget utvärderar sitt arbete med personuppgiftsincidenter för att säkerställa att rutinerna är effektiva och ändamålsenliga, samt ifall den utbildning och information som ges till chefer och medarbetare är tillräcklig. Ett mått för detta kan vara antalet inrapporterade personuppgiftsincidenter, som bör öka i takt med att medarbetarna får bättre kännedom om vad som utgör en incident och hur den ska hanteras. Fortsatt uppföljning av denna kontroll kommer framåt att ske inom ramen för ”Kontrollpunkt 2: Personuppgiftsincidenter”, förutsatt att inget särskilt föranleder en separat uppföljning.

Kontroll 2: Hantering av anställdas personuppgifter: Positioneringsteknik (GPS)

Verksamheten gavs följande rekommendationer:

- GSAB rekommenderades att genomföra en kartläggning av personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer, och bedöma huruvida behandlingarna kan motiveras med hänvisning till ändamål, nödvändighet och rättslig grund.
- GSAB rekommenderades att genomföra konsekvensbedömningar för identifierade personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer.
- GSAB rekommenderades att skriftligen informera de anställda om personuppgiftsbehandlingarna.

Verksamheten har i svaret på de uppföljningsfrågor som skickades ut angett att ett antal åtgärder har vidtagits eller påbörjats. Bl.a. har bolaget uppdaterat sitt regelverk gällande fordon- och fordonshantering, upprättat instruktion och tagit fram information. Bolaget har även påbörjat konsekvensbedömningar för personuppgiftsbehandlingen i ISA och överfallslarmet.

Eftersom inte alla rekommendationer har hanterats kvarstår de lämnade rekommendationerna i de delar där de ännu inte har behandlats eller slutförts. Mot bakgrund av de stora risker som är förknippat med den här typen av behandlingar, och eftersom arbetet ännu inte har slutförts, kommer dataskyddsombudet också att genomföra ytterligare uppföljning av denna kontroll under 2022.

2.7 Sammanfattande rekommendationer

För att på ett ännu mer praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en mer noggrann genomgång av enkätresultaten tillsammans med verksamheten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att den aktuella risknivå ska bibehållas.

2.7.1 Rekommendation för hantering av resultaten

Av enkätsvaren framgår att Göteborgs Spårvägar AB har kommit olika långt i dataskyddsarbetet inom de tolv kontrollpunkterna. Utifrån bolagets skattning är det fyra kontrollpunkter som sticker ut vad gäller risknivå. Dessa punkter är ”Biträdesavtal och andra överenskommelser” (kontrollpunkt 3), ”Personuppgiftsregister” (kontrollpunkt 4), ”Övergripande strategi för dataskydd” (kontrollpunkt 5) och ”IT-system och digitala verktyg” (kontrollpunkt 11) där det finns höga risker identifierade som bedöms vara omfattande och som kräver åtgärder. Dataskyddsombudet rekommenderar därför att bolaget prioriterar de rekommendationer som angetts under dessa fyra punkter.

Utifrån att det finns ytterligare kontrollpunkter med risker som kräver omgående åtgärder rekommenderas Göteborgs Spårvägar AB att i samråd med dataskyddsombudet ta fram en handlingsplan för arbetet med dessa under 2022.

3 Bilagor

3.1 Bilaga 1: Diagram över resultat av fasta kontrollpunkter, i jämförelse med Göteborgs Stads genomsnitt.