Göteborgs Stad

Beslutsunderlag
Utfärdat 2022-01-28
Diarienummer 0016/21

Handläggare
Katrin Gundersen
Telefon: 031-368 55 12
E-post: katrin.gundersen@gotalejon.goteborg.se

Årsrapport Dataskyddsenheten 2021

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- anteckna årsrapport från Dataskyddsenheten 2021.

Sammanfattning

De fördjupade kontrollerna har bestått av personuppgiftregistret och biträdesavtal och andra överenskommelser. Dessa har genomförts under våren och presenterades för styrelsen i juni 2021 i enligt med det som angivits i kontrollplanen. Dataskyddsombudet har i rapporterna avseende de fördjupade kontrollerna haft vissa anmärkningar och lämnat ett antal rekommendationer till verksamheten. Hur verksamheten hanterat de rekommendationer som lämnades i vårens fördjupade kontroll har följts upp under hösten.

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

Bedömning ur ekonomisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur ekologisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur social dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Samverkan

Ingen samverkan har genomförts

Bilagor

1. Årsrapport Dataskyddsenheten 2021

Ärendet

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 rekommendation som ges av dataskyddsombudet syftar till att ge ledningen underlag för att kunna fatta väl underbyggda beslut.

Beskrivning av ärendet

Dataskyddsenheten har under året tagit fram gemensamma rutiner för kontrollarbetet, med syfte att skapa ett enhetligt, transparent och systematiskt arbetssätt för Göteborgs Stads verksamheter.

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.

Förvaltningens /bolagets bedömning

Det är bolagets bedömning att resultatet från revisionen är rimlig och korrekt.

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2021

Försäkrings AB Göta Lejon

2021-12-21

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 rekommendation 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 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 Fördjupad kontroll

De fördjupade kontrollerna har bestått av personuppgiftregistret och biträdesavtal och andra överenskommelser. Dessa har genomförts under våren och presenterades för styrelsen i juni 2021 i enligt med det som angivits i kontrollplanen.

Dataskyddsombudet har i rapporterna avseende de fördjupade kontrollerna haft vissa anmärkningar och lämnat ett antal rekommendationer till verksamheten. Hur verksamheten hanterat de rekommendationer som lämnades i vårens fördjupade kontroll 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 Försäkrings AB Göta Lejon

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:

Bolagets skattning på kontrollpunkten visar att några risker finns angående verksamhetens interna dataskyddsorganisation, men inga som kräver akuta åtgärder. Bolaget har svarat varierande på de 6 frågorna under kontrollpunkten, både en nolla och en fyra bland annat. Det som bolaget framförallt saknar är definierade rapporteringsvägar som säkerställer att dataskyddsfrågorna når rätt nivå/befattning/roll inom verksamheten. Det saknas också rutiner för att säkerställa att dataskyddsombudet regelbundet kontaktas för att delta i frågor. Dataskyddsombudet instämmer i bolagets bedömning, eftersom man inte så ofta kontaktas i frågor rörande dataskydd.

På grund av detta är det svårt att bedöma hur det dagliga arbetet med dataskydd inom bolaget fungerar. För att dataskydd ska kunna anses vara en integrerad del av det dagliga arbetet krävs att det på samtliga nivåer inom bolaget finns en medvetenhet om dessa frågor, och insikter i vikten av att följa gällande dataskyddslagstiftning.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Kommentarer och rekommendationer:

Dataskyddsombudet granskade bolagets hantering av personuppgiftsincidenter under hösten 2020 och anser att bolaget har bra koll på hanteringen. Rutiner finns på plats både för att upptäcka och utreda incidenter, men också för att bedöma om de ska anmälas eller inte och hur de ska dokumenteras. Av de incidenter som kommit dataskyddsombudets kännedom har ingen varit av den karaktären att den har behövt anmälas till tillsynsmyndigheten. Därför vet inte dataskyddsombudet om svaret (0) på frågan av hur stor andel incidenter som har rapporterats i tid till tillsynsmyndigheten är baserat på att inga av incidenterna har varit av den digniteten att de behövts rapporteras, eller att det innebär att man haft sådana incidenter men

rapporterat för sent. I vilket fall påpekade dataskyddsombudet vikten av att förtydliga den korta tidsfrist som dataskyddsförordningen medger vid en inträffad incident i den tidigare granskningen, och detta har nu förtydligats i bolagets rutin. Det som brister hos bolaget är att systematiskt följa upp inträffade incidenter samt att regelbundet informera och utbilda den egna personalen om vad som ska göras när en incident inträffar. En uppföljning är en naturlig del i det systematiska dataskyddsarbetet och bör göras för att upptäcka eventuella mönster eller kunskapsluckor inom verksamheten som gör att det sker upprepade incidenter. Utbildning eller information om just incidenter kan också ingå i den övergripande utbildningen i dataskydd som ges till bolagets anställda.

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:

Dataskyddsombudet har granskat bolagets hantering av biträdesavtal och andra överenskommelser i den fördjupade kontrollen under våren avseende biträdesavtalsmall och stickprovskontroll på redan ingångna avtal. Dataskyddsombudet instämmer i bolagets bedömning av kontrollpunkten då det finns förbättringspotential på ett par punkter och i enlighet med de rekommendationer som lämnades i delårsrapporten. Någon efterlevnadskontroll av anlitade personuppgiftsbiträden har dataskyddsombudet inte sett, varpå det är svårt att bedöma bolagets hantering av detta. I den mån bolaget anser sig ha svårigheter att bedöma om andra överenskommelser/avtal behöver upprättas avseende gemensam/annan delad hantering av personuppgifter, internt eller externt, bör dataskyddsombudet kontaktas för rådgivning.

Bolaget har satt en trea på frågan om hur stor andel personuppgiftsbiträdesavtal som bolaget har tecknat med personuppgiftsbiträden och här vill dataskyddsombudet uppmärksamma bolaget på riskerna med att ha biträden där man inte har reglerat personuppgiftsbehandlingen. Om biträdet agerar utanför ett personuppgiftsbiträdesavtal och dess tillhörande instruktioner, finns risk att de själva istället ska ses som personuppgiftsansvariga för behandlingen i fråga. I de fall avtal saknas, blir det svårt att avgöra vem som egentligen är ansvarig.

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 skattning på kontrollpunkten visar att inga direkta risker föreligger i bolagets hantering med sitt personuppgiftsregister. Bolaget har svarat en fyra på tre av fem påstående under kontrollpunkten, vilket innebär att bolaget anser sig ha bra koll på vilka behandlingar som finns i registret, att de uppfyller alla krav samt att det finns en dokumenterad ansvarsfördelning. Efter dataskyddsombudet granskning under de fördjupade kontrollerna, instämmer dataskyddsombudet i den bedömningen. Det som behöver förbättras är framförallt kunskapen om hur själva systemet där registret finns fungerar, så att bolaget på ett enklare sätt kan använda registret i det dagliga dataskyddsarbetet. Enligt uppföljningen har bolaget bokat en utbildning med leverantören av systemet, vilket är positivt för framtiden. Slutligen saknar också bolaget en helt fungerande rutin för att kontinuerligt uppdatera registret med behandlingar som tillkommit eller förändrats. Registret är ett hjälpmedel som ska hållas levande, det går således inte att bara fylla i en gång och sedan låta vara. Dataskyddsombudet hoppas att bolaget efter utbildning kommer kunna använda registret mer i sin verksamhet och dra nytta av dess funktioner.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Kommentarer och rekommendationer:

Bolagets skattning på kontrollpunkten visar att några risker finns angående verksamhetens interna dataskyddsorganisation, men inga som kräver akuta åtgärder. Bolaget har under denna punkt angett att en tvåa på att man har en övergripande strategi för arbetet med dataskydd och att man arbetar systematiskt med att integrera dataskyddsfrågorna i informationssäkerhetsarbetet. Man anger samma siffra på att man har antagit ett riskbaserat arbetssätt och att det finns rutiner som hjälper till att säkerställa de styrande dokument som inom bolaget reglerar att personuppgiftsbehandlingar hålls uppdaterade. Eftersom dataskyddsombudet inte involveras i någon större utsträckning, är det svårt att bilda sig en uppfattning om dessa punkter. Generellt brukar ett systematiskt dataskyddsarbete och övergripande strategi för detta generera frågor på löpande band, varpå dataskyddsombudet ser anledning att följa upp på detta under kommande år.

Regelbundna interna kontroller är ett effektivt sätt för verksamheten att, utöver de granskningar som genomförs av dataskyddsombudet, säkerställa efterlevnaden av dataskyddsförordningen.

2.4.6 Kontrollpunkt 6: Utbildning

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

Kommentarer och rekommendationer:

Bolaget har under denna punkt angett enbart treor och en fyra, vilket tyder på en bra nivå inom bolaget avseende just utbildning och att inga risker är identifierade. Dataskyddsombudet har själv hållit en grundläggande utbildning i dataskydd där uppfattningen var att relativt många ifrån verksamheten deltog – men eftersom det var digitalt var det svårt att få en exakt siffra. Utöver det bjöds dataskyddsombudet in att hålla utbildning för styrelsen på deras strategidagar, men detta blev av oklar anledning inställt. När bolaget har identifierat ett behov av utbildning är det viktigt att det tas fram en plan för att säkerställa att det tillgodoses över tid.

Det är oavsett positivt att bolaget har identifierat ett behov av utbildning och tar hjälp av dataskyddsombudet. Det är rekommenderat att bolaget säkerställer att utbildningsbehovet tillgodoses även på lång sikt samt att det inkluderar alla delar av dataskydd (så som till exempel incidenthantering).

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 påstående med flera höga värden vilket tyder på att inga risker är identifierade. Dataskyddsombudet har inte i dagsläget någon anledning att tvivla på bolagets bedömning, men rekommenderar ändå bolaget att se över integritetspolicyn regelbundet. Dataskyddsombudet har inte granskat bolagets integritetspolicy i detalj, men kan vid en snabb överblick konstatera att policyn inte är särskilt uttömmande. Den är generellt hållen och beskriver inga särskilda situationer. I den mån bolaget hänvisar till sin integritetspolicy för beskrivning av hur man behandlar personuppgifter, är det bra om den beskriver även specifika behandlingar.

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:

Bolagets skattning på kontrollpunkten visar att några risker finns angående verksamhetens arbete med mejl- och dokumenthantering, men inga som kräver akuta åtgärder. Bolaget har svarat genomgående relativt högt på påståendena under kontrollpunkt 8. Dataskyddsombudet ser ingen anledning att ifrågasätta detta resultat, men har inte diskuterar varken frågor rörande mejl, dokumenthantering eller informationsklassning med bolaget och ser ett behov av att följa upp detta.

Bolaget har vissa punkter att förbättra, bland annat att de registrerade ska få information direkt i samband med upprättande av kontakt, t.ex. i signatur, om hur deras personuppgifter behandlas. Här kan dataskyddsombudet direkt konstatera att detta har saknats hos de personer som dataskyddsombudet varit i kontakt med hos bolaget. Där kan en enkel åtgärd vara att lägga in en länk till integritetspolicyn i mailsignaturen.

Även om de flesta personuppgiftsbehandlingar har informationsklassificerats bör bolaget se till så att alla behandlingar görs det, samt att det finns anvisningar som styr hur information i olika informationsklasser får hanteras och vilka lagringsytor som får användas.

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:

Bolagets skattning på kontrollpunkten visar att det finns stora risker angående verksamhetens arbete med konsekvensbedömningar som kräver akuta åtgärder. Eftersom bolaget inte har involverat dataskyddsombudet i något arbete rörande konsekvensbedömningar under det senaste året, kan ingen bedömning avseende verksamhetens arbete med konsekvensbedömningar göras. Att bolaget sätter en trea på att involvera dataskyddsombudet vid konsekvensbedömningar och en tvåa på att involvera dataskyddsombudet vid riskanalyser, är svårt att bemöta hur det fungerar i praktiken. Bolaget uppger att man har rutin för att genomföra och

dokumentera konsekvensbedömningar vilket dataskyddsombudet ser som positivt, då det är något som många verksamheter saknar. Huruvida materialet uppnår kraven på en godkänd konsekvensbedömning blir något att följa upp framöver. Att ha en riskbedömningsmetod är också en väsentlig del av konsekvensbedömningsarbetet och en förutsättning för att kunna bedöma huruvida en konsekvensbedömning behöver göras, om den behöver samrådas med IMY samt för att bolaget ska kunna acceptera risker i behandlingar.

Dataskyddsombudet vill uppmärksamma bolaget på att resultatet på kontrollpunkten visar på att det finns vissa förbättringsmöjligheter i arbetet med konsekvensbedömningar. Att det varken finns några pågående eller beslutade konsekvensbedömningar betyder troligtvis inte att verksamheten inte har några behandlingar som innebär hög risk, då de allra flesta verksamheter brukar ha i alla fall någon sådana. Verksamheten uppmanas därför se över vilka behandlingar man har och huruvida en konsekvensbedömning behöver göras. Därtill behöver bolaget ta fram rutin för att kunna acceptera risker som en konsekvensbedömning visar, annars missar man syftet med ett sådant verktyg.

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:

Resultatet på kontrollpunkten visar på att bolaget kan förbättra hur de arbetar med IT-projekt och upphandling utifrån ett dataskyddsperspektiv. Bolaget har angett en tvåa på 4 av 5 påståenden, vilket tyder på att dataskyddsperspektivet kanske inte är så prioriterat vid upphandling. Ökad kunskap om inbyggt dataskydd och dataskydd som standard kan förbättra bolagets möjligheter att säkerställa dessa krav även vid uppstart av IT-projekt och upphandling av nya system.

Dataskyddsombudet har inte under det gångna året blivit involverad i något IT-projekt eller vid införande av nya tjänster där personuppgifter kan komma att hanteras, och kan inte avgöra om det beror på att inga sådana har startats under året eller om bolaget har brustit i att involvera dataskyddsombudet.

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 gjort en ganska blandad bedömning avseende IT-system och digitala verktyg. Det som dataskyddsombudet reagerar på framför allt är att man sätter en tvåa på att det finns dokumenterade rutiner för tilldelning av behörigheter och åtkomster i IT-system, men en trea på att man följer upp medarbetarnas behörigheter och åtkomst. De två punkterna borde stämma överens med varandra, för det torde vara svårt att följa upp något man inte har en rutin för. Det är viktigt att bolaget begränsar behörigheter så att de är anpassade och begränsade till vad som är nödvändigt för arbetsuppgifterna. Regelbunden uppföljning av detta bör ske för att säkerställa att gamla behörigheter inte ligger kvar.

Att bolaget enbart satte en etta på målgruppsanpassad information för digitala verktyg som används och tillhandahålls kunder/brukare/elever behöver åtgärdas. I den mån bolaget har några sådana verktyg, bör man för att kunna uppfylla sin informationsskyldighet, också anpassa informationen.

2.4.12 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:

Bolagets skattning på kontrollpunkten visar att några risker finns angående verksamhetens hantering av registrerades rättigheter, men inga som kräver akuta åtgärder. Dataskyddsombudet anser att det är positivt att medvetenheten om de registrerades rättigheter uppskattas som en trea av verksamheten, samt att man angett en fyra på två av punkterna under kontrollpunkten. Kunskapen kan förbättras avseende hur rättigheterna begränsas och hur situationerna ska hanteras.

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.

Bolaget har uppgett att man inte utrett frågan för att ta något beslut på behörig nivå, utan att man fortsätter att använda LinkedIn som tidigare. Någon ändring kommer inte ske i nuläget, utan man inväntar beslut ifrån Staden. Dataskyddsombudet vill påpeka att varje personuppgiftsansvarig själv ansvarar för att fatta beslut och att Staden (Göteborgs Stad) inte kan fatta beslut som gäller för alla personuppgiftsansvariga.

2.6 Uppföljning

2.6.1 Uppföljning av genomförda kontroller 2018 - 2020

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 bestod av ett antal frågor med syfte att undersöka förutsättningarna för det interna dataskyddsarbetet. Av kontrollen framgick att bolaget hade utsett en dataskyddskontakt med meriterande kunskaper för rollen. Bolaget fick rekommendationer kopplade till sin integritetspolicy och man rekommenderades att säkerställa att dataskyddsombudet och bolaget planerar sitt samarbete för att ge goda förutsättningar för detta arbete.

Uppföljningen av denna kontroll har genomförts inom ramen för den skattning som bolaget gjorde via den utskickade enkäten. Den visade att det fortfarande finns åtgärder som behöver vidtas för att säkerställa att bolaget har en tydlig och funktionell dataskyddsorganisation med tillräckliga resurser som kan säkerställa dataskyddsperspektivet. Rekommendationer för det fortsatta arbetet lämnas under avsnitt 2.4.1 ”Kontrollpunkt 1: Dataskyddsorganisation”.

Kontroll 2 (2020): Hantering av personuppgiftsincidenter

Kontrollen genomfördes under 2020 och bestod av ett antal frågor med syfte att undersöka verksamhetens hantering av personuppgiftsincidenter.

Verksamheten gavs följande rekommendationer:

- Förtydliga den korta tidsfrist (72 timmar) som dataskyddsförordningen anger för anmälan av incident till tillsynsmyndigheten.
- Säkerställ att alla medarbetare informeras om rutinen.
- Se över formuleringar angående dataskyddsombudets roll.
- Förtydliga när de registrerade ska informeras.

- Dokumentera incidenter i ett separat dokument.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat.

2.6.2 Uppföljning av genomförda kontroller 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): Personuppgiftsregistret

Verksamheten gavs följande rekommendationer:

- Ta fram rutin för användning av registret.
- Förtydliga vem inom bolaget som är ansvarig för översyn och uppdatering av registret.

Kommentarer och rekommendationer:
Verksamheten har angett att de har vidtagit samtliga åtgärder i enlighet med lämnade rekommendationer. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att punkten behöver följas upp separat.

Kontroll 2 (2021): Biträdesavtal och andra överenskommelser

Verksamheten gavs följande rekommendationer:

- Uppdatera mallen med biträdets skyldighet att bistå vid förhandssamråd.
- Säkerställ att det går att lämna instruktioner i samband med biträdesavtal.

Kommentarer och rekommendationer:
Bolaget har angett att de har vidtagit åtgärder för några av de lämnade rekommendationerna. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att punkten behöver följas upp separat.

2.7 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en mer noggrann genomgång av enkätresultaten. 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 denna risknivå ska bibehållas.

2.7.1 Rekommendation för hantering av resultatet

Av enkätsvaren framgår att man inom bolaget har kommit olika långt i olika delar av dataskyddsarbetet. Utifrån bolagets skattning är det en kontrollpunkt där man placerar sig inom risknivå två och där det följaktligen finns skäl att särskilt fokusera sina resurser. Den är ”Kontrollpunkt 9: Konsekvensbedömning/samråd”. Inom det området finns det identifierade risker som bedöms vara omfattande och som kräver åtgärder. Även inom övriga kontrollpunkter lämnas rekommendationer för olika typer av åtgärder av skiftande brådskande karaktär. Prioritering mellan dessa bör göras i samråd med dataskyddsombudet.

3 Bilagor

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