Göteborgs Stad

Årsrapport för dataskyddsarbetet 2021

Boplats Göteborg AB

2021-12-20

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 kontroll avseende personuppgiftsbehandlingsregistret och hantering av biträden 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 rekommendationer till verksamheten att vidta ändringar och tillägg. 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 Boplats

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 den interna dataskyddsorganisationen fungerar väl och att inga direkta risker är identifierade. Dataskyddsombudet instämmer i bolagets bedömning avseende den interna dataskyddsorganisationen utifrån den kontakt dataskyddsombudet haft med bolagets dataskyddsorganisation under året. Uppfattningen är att bolagets dataskyddskontakter får tillräckligt med tid och resurser till sitt förfogande för att kunna utföra ett kontinuerligt dataskyddsarbete, samt att dataskyddsperspektivet tas hänsyn till i många delar av verksamheten. Det kan ofta vara bristande kunskap om dataskyddsfrågor på andra poster inom verksamheten som gör att perspektivet fattas, men uppfattningen är att dataskyddskontakterna jobbar för att förbättra detta.

Dataskyddsombudet kontaktas regelbundet för att delta i frågor som rör skyddet av personuppgifter och uppmuntrar bolaget till att fortsätta på samma sätt. Även fast den interna kompetensen är god finns det, förutom det lagstadgade kravet, alltid en nytta av att lyfta frågor med dataskyddsombudet.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Kommentarer och rekommendationer:

Bolagets hantering av personuppgiftsincidenter granskades under hösten 2020 och dataskyddsombudet anser att bolagets skattning av kontrollpunkten stämmer bra överens med den hur det ser ut i praktiken. Utifrån de kommentarer som lämnades på granskningen har ett antal åtgärder vidtagits och i dagsläget finns inga större risker identifierade. Det finns rutiner på plats både för att upptäcka och utreda incidenter, men också för att bedöma om de ska anmälas eller inte samt hur de ska dokumenteras. Dataskyddsombudet har under året fått kännedom om en

personuppgiftsincident och instämde där i bolagets bedömning att inte anmäla den till tillsynsmyndigheten.

Eftersom bolagets rutiner säkerställer att medarbetarna och dataskyddsorganisationen vet hur de ska agera vid en incident och hur de bedömer incidenter, anser dataskyddsombudet att det finns goda förutsättningar för bolaget att hantera incidenter i enlighet med dataskyddsförordningen.

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 avseende användning av biträdesavtalsmall och stickprovskontroll av redan ingående avtal, i den fördjupade kontrollen under våren. Kontrollpunkten avser mer det löpande arbetet med biträden och avtal och här instämmer dataskyddsombudet i bolagets bedömning av nuläget. Det finns förbättringspotential på ett par punkter och bolaget har också åtgärdat de synpunkter som dataskyddsombudet lämnade i granskningen. Efterlevnadskontroll av anlitade personuppgiftsbiträden är ett effektivt verktyg för att kontrollera biträdena och att de uppfyller ställda krav. I ljuset av den senaste rättsutvecklingen rörande tredjelandsöverföring vill dataskyddsombudet skicka med att det är viktigt att bolaget kan bedöma hela kedjan av underbiträden vid anlitande av biträde som har underbiträden. Trots att man kanske inte har koll på hela kedjan kommer man som personuppgiftsansvarig att bli ansvarig.

I den mån bolaget har svårigheter att bedöma om andra överenskommelser/avtal behöver upprättas avseende gemensam/annan delad hantering av personuppgifter, bistår dataskyddsombudet gärna med råd.

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:

Dataskyddsombudet har under våren granskat bolagets personuppgiftsregister och instämmer i den bedömning som gjorts, och att inga direkta risker föreligger. Registret är i dagsläget uppdaterat och ska innehålla alla bolagets behandlingar. Dataskyddskontakterna har initierat att öka kunskapen om registret även på andra håll inom verksamheten vilket är bra. För att registret ska kunna användas på ett bra sätt i det löpande dataskyddsarbetet och säkerställa att det håller sig uppdaterat, krävs att man dokumenterar vem som ansvarar för det samt genomför regelbunden översyn.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Kommentarer och rekommendationer:

Bolaget har under denna punkt angett att man har en övergripande strategi för arbetet med dataskydd och att man arbetar systematiskt med att integrera dataskyddsfrågorna i informationssäkerhetsarbetet. Utifrån den höga skattningen kan dataskyddsombudet framåt att kontrollera de bedömningar som gjorts för att se hur långt bolaget kommit i arbetet. Bolaget anger att en liten del av verksamhetens informationstillgångar är identifierade och värderade utifrån K/R/T i enlighet med stadens styrande dokument, därför rekommenderas bolaget att åtgärda detta. I den mån man anordnar fysiska och digitala sammankomster, är det viktigt att ta fram rutiner för att efterleva kraven enligt dataskyddsförordningen. Dessa rutiner behöver också bolagets medarbetare som anordnar sammankomster få kännedom om, så att man säkerställer efterlevnaden i hela verksamheten.

Visserligen utför dataskyddsombudet kontroller för att säkerställa bolagets följsamhet mot dataskyddsförordningen, men det är också viktigt att bolaget gör sina egna kontroller för att säkerställa att man följer regelverket.

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 på kontrollpunkten visar att det finns vissa risker som behöver åtgärdas men att den allmänna kunskapsnivån inom verksamheten ändå ger goda förutsättningar i dataskyddsarbetet. Medarbetarna ges regelbundet möjlighet att

delta i externa utbildningar inom dataskydd och det genomförs regelbundet informationsinsatser för att utbilda och informera medarbetarna inom dataskydd. 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. 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 som kan vara relevanta för bolagets verksamhet i utbildningsplanen. Även bolagets anställda har möjlighet att delta i de utbildningar som Dataskyddsenheten erbjuder, men dataskyddsombudet kan också vid behov hålla enskilda riktade utbildningar. Bolaget rekommenderas att kartlägga och identifiera vilket utbildningsbehov verksamheten har och hur man kan tillgodose detta framöver.

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 och dataskyddsombudet instämmer bolagets bedömning. Bolaget har regelbundet sett över sin integritetspolicy och även involverat dataskyddsombudet i detta arbete. Det arbetet bör fortsätta för att bibehålla den höga skattningen. Dataskyddsombudet rekommenderar verksamheten att se över och dokumentera hur man informerar medarbetare om hur deras personuppgifter behandlas. Det kan vara vid anställningens ingående, en särskild integritetspolicy riktad till anställda eller när särskilda behandlingar påbörjas.

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 svarat genomgående relativt högt på påståendena under kontrollpunkt 8 vilket har inneburit en ett resultat på nivå fyra, som indikerar att inga risker är

identifierade. Dataskyddsombudet ser ingen anledning att ifrågasätta detta resultat, men har inte diskuterar varken frågor rörande mejl, dokumenthantering eller informationsklassning med bolaget och ser att uppföljning eventuellt behövs. I sammanhanget rekommenderas dock bolaget även att följa upp och kontrollera så att utförandet av den faktiska gallringen, i olika systemen och på bolagets lagringsytor, genomförs i enlighet med vad som anges i dokumenthanteringsplanen. Det är positivt att bolaget har informationsklassificerat alla verksamhetens personuppgiftsbehandlingar utifrån Göteborgs Stads riktlinje för informationssäkerhet.

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:

Syftet med konsekvensbedömningar är att förebygga risker och på så sätt även minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för de registrerades fri- och rättigheter. Skattningen visar att bolaget har ett behov av att säkerställa att en bedömning av risk har genomförts avseende samtliga av bolagets personuppgiftsbehandlingar och att en konsekvensbedömning genomförs i de fall en sådan behövs.

Dataskyddsombudet har under året inte rådfrågats i någon konsekvensbedömning som bolaget arbetat med, vilket gör det svårt för dataskyddsombudet att bedöma hur bolaget arbetar med konsekvensbedömningar. Även om bolagets skattning inte indikerar några omfattande risker är dataskyddsombudet bedömning att bolaget bör prioritera detta arbete för att säkerställa att skattningen är korrekt. Att genomföra konsekvensbedömningar är i många fall ett absolut krav 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 bör vara en del av den övergripande strategin för dataskyddsarbetet i verksamheten, och den interna dataskyddsorganisationen bör fungera på ett sätt som säkerställer att inga nya eller förändrade behandlingar påbörjas utan att en bedömning görs om behovet av en konsekvensbedömning.

Bolaget rekommenderas att se över vad förordningen ställer för krav på vad en konsekvensbedömning ska innehålla och vilka kriterier som gäller för att en personuppgiftsansvarig ska behöva genomföra en konsekvensbedömning. Vägledning finns också på tillsynsmyndighetens hemsida. Dataskyddsombudets uppfattning, efter diskussion med bolagets dataskyddskontakter, är att skattningen inte motsvarar hur arbetet med konsekvensbedömningar ser ut i praktiken.

Dataskyddsombudet vill i sammanhanget betona att det inte är enbart för nya former av behandlingar som bolaget behöver göra konsekvensbedömningar, utan att det även behöver genomföras konsekvensbedömningar för alla redan befintliga riskfyllda behandlingar. Det är även av vikt att bolaget har rutiner för att följa upp identifierade risker samt att beslut om accepterande av risker sker på behörig nivå.

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 sin organisation och sina rutiner högt och har inte identifierat några direkta risker. Dataskyddsombudet har under det gångna året inte involverats i någon upphandling som bolaget själva har hanterat. Om detta beror på att inga upphandlingar på detta område har skett under året är för dataskyddsombudet oklart, men utifrån detta kan dataskyddsombudet inte göra någon egen bedömning. Men i konversation med bolaget framkommer att dataskyddskontakterna är involverade i dessa frågor, vilket innebär att dataskyddsperspektivet finns med från början.

För att få mer kunskap om bolagets arbete, och hur man säkerställer att dataskyddsperspektivet finns med i arbetet med nya IT-projekt och vid upphandling, samt hur man i kravställningen har med kriterier för inbyggt dataskydd och dataskydd som standard, rekommenderas bolaget att involvera dataskyddsombudet i ett tidigt skede.

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, vilket innebär att det finns några risker men som inte kräver några omgående åtgärder. Dataskyddsombudet vill särskilt uppmärksamma bolaget på vikten av tilldelning av behörigheter och åtkomster i IT-system och att följa upp detta regelbundet. Det är viktigt att bolaget begränsar behörigheter så att de är anpassade

och begränsade till vad som är nödvändigt för arbetsuppgifterna. Att ha kontroll på behörigheter kan till exempel vara ett sätt att undvika incidenter. Bolaget rekommenderas också att ha rutiner för att systematiskt kunna följa upp och kontrollera att användningen av system och/eller andra digitala verktyg följer antagna rutiner/riktlinjer/policys etc.

Bolaget och dataskyddsombudet har diskuterat frågan om cookies på hemsidan och det pågår ett arbete där förbättringar behöver göras utifrån gällande lagstiftning.

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:

Sammantaget anser bolaget, utifrån skattningen, att det finns goda förutsättningar för att hantera de registrerades rättigheter. Dataskyddsombudet har inte blivit tillfrågad angående någon begäran från registrerade rörande deras möjlighet att utöva sina rättigheter, men har inte heller några indikationer som tyder på att skattningen skulle vara missvisande eller felaktig. I den mån bolaget använder sig av samtycke, är det bra att rutiner finns för att hantera ett tillbakadragande av samtycke.

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.

Efter dialog med bolagets dataskyddskontakter framkommer att man planerar att ta fram ett underlag rörande bolagets användning av sociala medier och publicering

av personuppgifter. Styrelsen kommer därefter att fatta ett beslut.
Dataskyddsombudet lämnar gärna råd/rekommendationer på underlaget.

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. Förutsättningarna för ett organisatoriskt arbetssätt rörande dataskydd förelåg redan 2018 och bolaget rekommenderades att fortsätta i samma banor. Vidare rekommenderades man att bearbeta sin informationstext samt kommunicera ut den på ett tydligare sätt.

Kommentarer och rekommendationer:

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): Granskning av hantering av personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

Den rutin som beskriver hur bolagets medarbetare ska hantera inträffade incidenter behövdes kompletteras med information om vilken information som ska lämnas till registrerade och att den ska lämnas skyndsamt. Ytterligare komplettering krävdes rörande hur personalen inom bolaget informerar ansvariga om en inträffad incident samt vad som händer vid en biträdessituation.

Kommentarer och rekommendationer:

Uppföljningen visar att rutinen har kompletterats med de punkter som dataskyddsombudet rekommenderat. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att punkten 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): Personuppgiftsbehandlingsregistret

Verksamheten gavs följande rekommendationer:
Bolaget rekommenderades att säkerställa att rätt rättslig grund var angiven på behandlingarna och att enbart en grund finns per behandling. Rutinen för registret behövde kompletteras med ansvar för uppdatering, vilka krav som dataskyddsförordningen ställer samt att regelbunden översyn ska ske.

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. Dataskyddskontakterna kommer att ha genomgång av registret med respektive ansvarig chef inom bolaget.

Kontroll 2 (2021): Biträden och andra överenskommelser

Verksamheten gavs följande rekommendationer:
Bolaget rekommenderades att se över mallen och lägga till möjligheten att bilägga instruktioner. Bolaget behövde utreda huruvida en rutin behövs för att hantera biträdesavtal där det också framkommer vem inom bolaget som är behörig att ingå personuppgiftsbiträdesavtal. Slutligen bör bolaget se över redan ingångna avtal, då de tecknades innan dataskyddsförordningen trädde i kraft och i vissa fall behöver kompletteras/ändras.

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.

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 resultaten

Av enkätsvaren framgår att man inom bolaget har kommit olika långt i olika delar av dataskyddsarbetet. Utifrån bolagets skattning är det ett par kontrollpunkter där man placerar sig inom risknivå 3 och där det följaktligen finns skäl att fokusera sina resurser. Utöver det rekommenderas bolaget se över hanteringen och arbetet med konsekvensbedömningar i enlighet med kommentarerna i “Kontrollpunkt 9: Konsekvensbedömning/samråd”. Genomgången av årsrapporten med bolagets

dataskyddskontakter visade att det saknades kunskap och förståelse om vad en konsekvensbedömning är och när en sådan ska genomföras. Dataskyddsombudets uppfattning är att det inom nämnda områden finns identifierade risker som kräver åtgärder.

3 Bilagor

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