Göteborgs Stad

Årsrapport för dataskyddsarbetet 2021

Göteborgsregionens Fritidshamnar 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 av personuppgiftsbehandlingsregistret och hantering av anställdas personuppgifter, samtycke som rättslig grund. Dessa har genomförts under våren och presenterades för styrelsen i september 2021 i enligt med det som angivits i kontrollplanen.

Dataskyddsombudet har i rapporterna avseende de fördjupade kontrollerna haft vissa anmärkningar och därför 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 Göteborgsregionens Fritidshamnar 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 skattat högt på kontrollpunkten avseende dataskyddsorganisationen, en trea och resten fyror. Detta innebär att bolaget anser sig ha goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Ett sådant resultat innebär att bolaget inte ser några direkta risker med hur det interna dataskyddsarbetet fungerar och att man har säkerställt dataskyddsperspektivet i alla bolagets verksamhetsdelar. För att dataskydd ska kunna anses vara en integrerad del av det dagliga arbetet krävs att det på samtliga nivåer inom bolaget finns kunskap och medvetenhet om dataskydd och att frågor flödar enligt förutbestämda vägar. Det krävs också formella beslut i frågor rörande dataskydd och att dessa tas på rätt nivå för att ge riktning och vägledning åt bolaget i övrigt. Dataskyddsombudet ser risker med att bolaget skattar sig själva högt på kontrollpunkten, då det kan försätta bolaget i falsk trygghet om att det inte finns några förbättringspunkter i verksamheten. Även om bolaget är litet och har relativt få personuppgiftsbehandlingar, behandlar man trots det personuppgifter till både anställda och kunder. Det har under senaste året påbörjats nya behandlingar där dataskyddsombudets uppfattning inte varit att dataskyddsperspektivet var omhändertaget eftersom bolaget missat vissa viktiga aspekter. Dataskyddsombudets uppfattning är att det inom bolaget – liksom alla verksamheter – finns förbättringspotential angående hur den interna dataskyddsorganisationen fungerar.

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 gav därefter ett antal rekommendationer till bolaget för att

förbättra deras hantering av incidenter. Bolaget har inte återkommit med exakt vilka åtgärder man vidtagit med anledning av dessa rekommendationer, och dataskyddsombudets bedömning är därmed att den skattning bolaget gjort på kontrollpunkten är svår att bemöta. Rekommendationer som lämnades i granskningen var bland annat att bolaget behövde säkerställa att riskbedömningen sker på ett korrekt sätt samt att incidenterna dokumenteras enligt förordningens krav. För att inga risker ska föreligga behöver bolaget åtgärda de lämnade kommentarerna. Rutinen var också vid tiden för granskningen alldeles ny i verksamheten, varpå det då var svårt att få en uppfattning om hur väl förankrad den var i verksamheten. Det är därför viktigt att bolaget säkerställer att den kommuniceras ut till alla anställda, för att de ska veta vad en incident är och vad de gör när de misstänker/upptäcker en.

Dataskyddsombudet har inte fått kännedom om några incidenter under det senaste året, 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. Dataskyddsombudet vill uppmärksamma vikten av att incidenter anmälas i tid till tillsynsmyndigheten, och en förutsättning för det är att alla medarbetare inom bolaget har kunskap om vad en incident är och vad de ska göra när en sådan inträffar.

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 anger att man tecknat biträdesavtal med nästan alla personuppgiftsbiträden verksamheten har, vilket dataskyddsombudet anser positivt. I arbetet med biträden är det också viktigt att man, i enlighet med ansvarsprincipen i dataskyddsförordningen, kan säkerställa hela kedjan av biträden samt att man kontinuerligt kontrollerar att biträdena fortfarande uppfyller de villkor som ställts. Även redan ingångna avtal behöver följas upp och kontrolleras med jämna mellanrum. I och med att bolaget inte har involverat dataskyddsombudet i frågor rörande biträden och biträdesavtal, ser dataskyddsombudet ett behov av att följa upp frågan. Dataskyddsombudet har bett att få ta del av det biträdesavtal bolaget uppger man har planerat att ingå eller ingått under året, men ännu inte fått det, varpå det är svårt att bedöma hur bolaget faktiskt agerar i dessa situationer.

Dataskyddsombudet har rekommenderat bolaget att i den särskilda situationen specifikt undersöka hela kedjan och säkerställa att ingen olaglig tredjelandsöverföring sker, eftersom leverantörens själva på sin hemsida uppger att tredjelandsöverföring kan ske. Därmed finns det risker i bolagets hantering av biträdesavtal.

Bolaget saknar också rutiner för att kontinuerligt genomföra efterlevnadskontroller av biträden för att säkerställa att de villkor som ställts fortfarande uppfylls. Bolaget rekommenderas åtgärda detta.

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 den bedömning som gjordes då var att bolaget behövde ta ett omtag av registret för att uppfylla förordningens krav. Vid den tidpunkten hade bolaget inte ett register som uppfyllde kraven – det saknades bland annat information om ändamål, kategorier av personuppgifter och tekniska säkerhetsåtgärder. Sedan dess har ett par behandlingar förts in i registret, men långt ifrån alla som bolaget har. De rekommendationer som lämnades, utöver att bolaget behövde se över själva registret, var att ta fram en rutin för hantering av registret, vem som är ansvarig för det, när och hur översyn ska ske samt en beskrivning av hur registret kan användas i det dagliga dataskyddsarbetet. Bolaget har inte återkommit med några vidtagna åtgärder på dessa rekommendationer, varpå dataskyddsombudet har svårt att se att den höga skattningen som bolaget satt på påståendena stämmer överens med hur det faktiskt fungerar. Att från att inte ha haft ett register för några månader sedan till att sätta en fyra på att använda registret som en del i det löpande dataskyddsarbetet, är enligt dataskyddsombudets bedömning inte realistiskt.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Kommentarer och rekommendationer:

Ett systematiskt dataskyddsarbete bör bedrivas utifrån övergripande strategier för verksamheten avseende både dataskydd och informationssäkerhet. Eftersom

bolaget angett en fyra på övergripande strategi för arbetet med dataskydd, borde det indikera att dataskydd är involverat och prioriterat i alla bolagets verksamhetsdelar och processer. Det borde också innebära att bolaget har en rutin för att bedöma risker av behandlingar, konsekvensbedömningsarbetet, incidentuppföljning med mera. Dataskyddsombudets uppfattning är att bolaget inte har rutin i alla dessa delar av dataskyddsarbetet.

Det är därför av stor vikt att bolaget säkerställer att styrande dokument som reglerar personuppgifter hålls uppdaterade. Det behöver dessutom finnas en informationssäkerhetspolicy som anger hur personuppgifter kan behandlas i exempelvis IT-system, datorer och mobila enheter. Av vikt är även att säkerställa att alla verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet. Eftersom bolaget enbart skattat en tvåa på den punkten, rekommenderar dataskyddsombudet bolaget att åtgärda detta.

Verksamheten behöver också regelbundet genomföra kontroller för att se hur dataskyddsförordningen efterlevs. Dataskyddsombudet har inte fått ta del av några sådana kontroller, och kan komma att följa upp på både det och de andra påståendena under kontrollpunkten.

Bolaget har också angett en fyra på att man har rutiner för att säkerställa efterlevnad enligt dataskyddsförordningen vid anordnande av fysiska och digitala sammankomster vilket innebär att bolaget anser att man har sådana rutiner på plats för alla typer av sammankomster. Sådana rutiner måste också spridas till dem som anordnar sammankomsterna, för att säkerställa en enhetlig efterlevnad av förordningen. Eftersom bolaget inte involverat dataskyddsombudet i detta arbete kan dataskyddsombudet inte bedöma om rutinerna säkerställer efterlevnad, men kan komma att granska det framöver.

2.4.6 Kontrollpunkt 6: Utbildning

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

Kommentarer och rekommendationer:

För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Bolaget har bedömt att utbildningsnivån inom bolaget är så bra att inga åtgärder behöver vidtas. Dataskyddsombudets uppfattning är att för att en verksamhet ska kunna sätta fyra på alla påståenden på kontrollpunkten, så ska alla anställda fått heltäckande och regelbunden utbildning som uppfyller de krav som identifieras beroende på anställningstyp och ansvarsuppgifter. Dataskyddsombudet har inte fått kännedom om bolaget har kartlagt vilket behov av utbildning som finns för verksamheten som helhet och för särskilda positioner. En sådan plan för utbildning

påpekades av dataskyddsombudet redan 2020 vid den granskning av utbildningsnivån som genomfördes då.

Dataskyddsombudet har hållit en grundläggande utbildning i dataskydd för bolaget, men har ingen insyn i övrigt om vilka utbildningar bolaget har gått. Att man har erbjudit sina anställda en utbildning i grundläggande dataskydd är en bra början, men eftersom dataskydd är ett rättsområde som ständigt utvecklas är det viktigt att behovet säkerställs över tid.

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:

Integritetspolicyns syfte är att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. Bolaget behöver säkerställa att policyn uppfyller kraven på information och att informationen är lättillgänglig oavsett i vilken del av verksamheten den registrerades personuppgifter behandlas. Integritetspolicyn behöver också regelbundet uppdateras, till exempel står det fortfarande Datainspektionen fastän tillsynsmyndigheten bytt namn till Integritetsskyddsmyndigheten. Dataskyddsombudet har inte granskat integritetspolicyn i detalj men kan komma att göra det framöver. Bolaget rekommenderas även att säkerställa att medarbetarna i bolaget informeras om hur deras personuppgifter behandlas, vilket är särskilt viktigt när nya 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:

Det är av stor vikt att bolaget säkerställer att det finns en dokumenthanteringsplan som omfattar alla verksamhetsdelar och att det finns rutiner för när handlingar med personuppgifter gallras. Eftersom bolaget satt en trea på påståendet, uppfattar dataskyddsombudet det som att det saknas en del verksamhetsdelar och processer i nuvarande dokumenthanteringsplan. Dokumenthanteringsplanen ska också

innehålla aktuella gallringsrutiner och bolaget måste också säkerställa att den utlovade gallringen faktiskt sker. Det är också viktigt att se till så att alla medarbetare har kunskap om bolagets dokumenthantering och gallringsbestämmelser.

Eftersom bolaget enbart satt en etta på hur stor andel av verksamhetens personuppgiftsbehandlingar som har informationsklassats, finns det ett stort behov av att se över verksamhetens informationsklassificering av personuppgiftsbehandlingar och kontrollera så att detta görs i enlighet med Göteborgs Stads riktlinjer för informationssäkerhet. Verksamheten måste även se till så att medarbetarna vet hur information ska hanteras beroende på informationsklassningen. När en fullständig informationsklassning är gjord bör bolaget också ta fram rutiner eller anvisningar som förklarar hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas för informationen.

Vidare är det också viktigt att verksamheten informerar de registrerade direkt i samband med upprättande av kontakt om hur deras personuppgifter hanteras, vilket görs enkelt genom t.ex. hänvisning i e-postsignaturen till verksamhetens integritetspolicy. Slutligen bör de dokumenterade rutiner som bolaget uppger sig ha för hantering av personuppgifter i e-post, vara heltäckande och kommunicerad till alla medarbetare.

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. Bolaget har bedömt att hanteringen och genomförandet av konsekvensbedömningar inom bolaget är så bra att inga risker är identifierade och att inga åtgärder behöver vidtas eftersom skattningen totalt hamnade på grönt (3.2). Detta skulle innebära att bolaget vet hur de ska hantera behandlingar med hög risk och att genomförandet av konsekvensbedömningar sker rutinmässigt utan störningar. Eftersom dataskyddsombudet inte har blivit involverad eller tillfrågad avseende några konsekvensbedömningar ifrågasätts denna skattning. Bolaget har satt en etta på att man har framtagna och beslutade konsekvensbedömningar, samt en fyra på att det finns pågående konsekvensbedömningar, och att dataskyddsombudet bör involveras i dessa. Dataskyddsombudet ifrågasätter också hur det kan finnas pågående konsekvensbedömningar, när man samtidigt svarat att man inte har någon dokumenterad rutin för att genomföra och dokumentera konsekvensbedömningar. Att bolaget dessutom satt en fyra på att man har en rutin eller dokumenterat

arbetssätt för att uppdatera en befintlig konsekvensbedömning vid förändringar i behandlingar, ifrågasätts hur det är möjligt.

Vid genomgång av årsrapporten med bolaget framkommer det att dataskyddskontakten missuppfattat kontrollfrågan och saknar kunskap om vad en konsekvensbedömning egentligen är. Därför är resultatet på kontrollpunkten missvisande för den faktiska hanteringen avseende konsekvensbedömningar. Bolaget har i dagsläget inte genomfört någon konsekvensbedömning. Dataskyddsombudet rekommenderar bolaget att börja med att ta fram en rutin för att bedöma risker för behandlingar, för att därefter kunna genomföra riskanalyser och konsekvensbedömningar. Att genomföra konsekvensbedömningar är i många fall ett krav, och felaktig hantering eller icke genomförda konsekvensbedömningar kan innebära sanktionsavgifter ifrån tillsynsmyndigheten.

Bolaget måste se till så att dataskyddsombudet involveras och får möjlighet att lämna synpunkter i de fall beslut fattas att inte genomföra en konsekvensbedömning, men också får möjlighet att lämna råd vid en konsekvensbedömning.

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:

Bolagets skattning på kontrollpunkten innebär att bolaget anser att det inte finns några risker kopplade till hanteringen av IT-projekt och upphandling. Dataskyddsombudet anser att det trots det finns anledning för bolaget att aktivt jobba med att säkerställa att dataskyddsperspektivet finns med redan i uppstart av IT-projekt och upphandlingar. Vid upphandlingen av nya system/tjänster så behöver det tas med i kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard. Bolaget bör också ta fram en rutin för att genomföra risk-/behovsanalys för att kunna säkerställa att grundläggande principer enligt dataskyddsförordningen följs. Verksamheten bör även ha som rutin att dataskyddsombudet involveras från start i dessa processer. Dataskyddsombudets uppfattning är att bolaget inte på regelbunden basis genomför uppstart och upphandling av projekt, varpå det kanske i dagsläget inte föreligger faktiska risker men vid en framtida situation finns det många krav som behöver uppfyllas. Därför är det viktigt att bolaget redan nu säkerställer rutiner för hantering av IT-projekt och upphandling.

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:

Bolagets skattning på kontrollpunkten innebär att de inte har identifierat några risker eller förbättringsmöjligheter avseende IT-system och digitala verktyg. Dataskyddsombudet anser att det trots det finns anledning för bolaget att aktivt jobba med att säkerställa dataskyddsperspektivet redan i anskaffandet av nya IT-system och digitala verktyg. Dataskyddsombudet vill uppmärksamma bolaget på att kraven finns även vid uppstart/användning av system som inte kräver upphandling. Eftersom bolaget anger att man har rutiner och dokumenterat det mesta, kan uppföljning och kontroll ske av dataskyddsombudet.

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:

Även på denna kontrollpunkt skattar bolaget högt och identifierar inga risker i hanteringen av registrerades rättigheter. Att ha kunskap och medvetenhet om de registrerades rättigheter är väsentligt för det interna dataskyddsarbetet och efterlevnad mot förordningen. Bolaget har satt en nolla, d.v.s. ”vet inte/kan inte besvara frågan” angående hantering av registerutdrag inom 30 dagar. Dataskyddsombudet har svårt att bedöma om det beror på att man inte fått någon begäran eller om man inte lyckats hålla tidsfristen.

Dataskyddsombudet har granskat verksamhetens hantering av anställdas personuppgifter baserat på samtycke, och kommit fram till att bolaget inte använder sig av samtycke. I dialog med dataskyddskontakten har det också framkommit att man inte använder sig av samtycke heller i relation till andra registrerade än anställda. Därför är det inte konstigt att man inte har rutin för att hantera ett tillbakadragande av samtycke. I den mån man skulle grunda en behandling på samtycke, är det dock ytterst viktigt att man kan administrera samtycket ock ett tillbakadragande.

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.

Verksamheten har inte informerat dataskyddsombudet om hur man arbetar med personuppgifter på sociala medier. Verksamheten rekommenderas därför att kartlägga vilka sociala medier som används och huruvida det publiceras personuppgifter där, för att sedan ta ett beslut om fortsatt publicering.

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 hösten 2018. I den framgick att det fanns en organisation med ansvar för dataskyddsarbetet och att organisationen var väl representerad på ledningsnivå.

Verksamheten gavs följande rekommendationer:

- Förtydliga rollbeskrivningarna för vad vice VD och dataskyddskontakt ska göra.
- Informera dataskyddsombudet mer regelbundet.
- Förbättra och komplettera integritetspolicy.

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 för att kunna säkerställa

dataskyddsperspektivet. Rekommendationer för det fortsatta arbetet lämnas under avsnitt 2.4.1 ”Kontrollpunkt 1: Dataskyddsorganisation”.

Kontroll 2 (2020): Granskning av utbildningsnivå i dataskydd.

Verksamheten gavs följande rekommendationer:

- Förbättra de anställdas kunskapsnivå inom dataskydd genom fler utbildningsinsatser.
- Ta fram en konkret plan för utbildningsinsatser och identifiera behov.
- Skapa rutin för att informera/utbilda nyanställda.
- Informera och öva på personuppgiftsincidenter.

Kommentarer och rekommendationer:

Uppföljning av denna kontroll har skett genom att frågan varit en del av de fasta kontrollpunkterna. Resultat, kommentarer och rekommendationer framgår därför av punkten 2.4.6 kontrollpunkt 6: Utbildning.

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): Hanteringen av personuppgiftsregistret

Verksamheten gavs följande rekommendationer:

- Ta fram ett register (alt använd DraftIt) där behandlingar kan fyllas i och alla obligatoriska krav finns med.
- Dokumentera alla behandlingar.
- Gör en översyn över vilka behandlingar som finns dokumenterade i det gamla registret.
- Ta fram en rutin som beskriver hur översyn av registret sker, när detta ska ske och vem som är ansvarig.
- Använd registret i det dagliga dataskyddsarbetet.

Kommentarer och rekommendationer:
Verksamheten har angett att de har vidtagit åtgärder för några av de lämnade rekommendationerna. Anledningen till att inte åtgärder har vidtagits enligt samtliga rekommendationer framkommer inte. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att punkten behöver följas upp separat. Övriga rekommendationer kvarstår.

Kontroll 2 (2021): Hantering av anställdas personuppgifter: samtycke

Verksamheten gavs följande rekommendationer:

- Säkerställ korrekt rättslig grund för behandlingar.

- Uppdatera den information som lämnas till anställda.

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. Vissa kontrollpunkter har skattats högt, vilket utifrån dataskyddsombudets uppfattning inte riktigt överensstämmer med bolagets faktiska hantering av punkterna. I vissa fall beror skattningen på ett kunskapsglapp eller att man inom bolaget inte riktigt kommit så långt i sitt dataskyddsarbete. På "Kontrollpunkt 8: Mejl och dokumenthantering", "Kontrollpunkt 9: Konsekvensbedömning/Samråd" samt "Kontrollpunkt 3: biträdesavtal och andra överenskommelser" finns ett antal risker identifierade som bolaget bör åtgärda.

3 Bilagor

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