Göteborgs Stad

Årsrapport för dataskyddsarbetet 2021

Renova AB

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 bolagets hantering av anställdas personuppgifter avseende uppgifter från positioneringsteknik.

I samråd med verksamheten har kontroll avseende bolagets hantering av anställdas personuppgifter av positioneringsteknik genomförts under oktober till november och presenteras i en separat rapport bilagd till denna årsrapport. I bilagan lämnas ett antal rekommendationer som dataskyddsombudet ämnar följa upp under 2022 utöver ytterligare fördjupade kontroller.

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 Renova 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 goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Genom att fortsätta stödja det goda arbetet ges den interna dataskyddsorganisationen möjlighet att förbättra arbetet ytterligare. För att öka bolagets möjligheter att kunna bedriva ett systematiskt dataskyddsarbete behöver den interna dataskyddsorganisationen ges tillräckligt med resurser.

Bolaget har under året identifierat behov som behöver punktinsatser och tagit in hjälp för att åtgärda det akuta behov som uppstått. Dataskyddsombudet ser risker med att detta gör att det löpande dataskyddsarbetet inte fungerar över tid, när enbart punktinsatser görs för att åtgärda brister. Bolaget behöver lägga upp en plan för det löpande arbetet där den interna dataskyddsorganisationen är involverad såväl som vid behov, externa resurser. Bolaget rekommenderas därför att se över hur man kan göra dataskyddsarbetet till en naturlig och integrerad del i det dagliga arbetet.

Det är också viktigt att bolaget säkerställer att alla medarbetare vet hur de ska hantera personuppgifter. Tydliga rutiner behöver också tas fram för att säkerställa att dataskyddsombudet involveras i dataskyddsarbetet.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Kommentarer och rekommendationer:

Bolaget bedriver ett bra arbete med att identifiera och hantera inträffade personuppgiftsincidenter. Dataskyddsorganisationen bör ges möjlighet att kontinuerligt se över och förbättra verksamhetens rutiner för hanteringen av personuppgiftsincidenter. Bolaget bör säkerställa att den dokumentation som förs vid inträffade incidenter uppfyller kraven enligt dataskyddsförordningen. Vidare är

det av yttersta vikt att medarbetarna inom bolaget har kunskap om vad en incident är och vad de ska göra om en incident upptäcks/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 har ett behov av att säkerställa att man kan bedöma om det uppstår en biträdesrelation vid anlitande av nya leverantörer samt kontrollera att det finns biträdesavtal på plats för alla situationer som kräver det. Om så inte är fallet, bör det åtgärdas snarast då det finns stora risker med att låta någon annan behandla personuppgifter å sina vägnar utan att det reglerats.

Verksamheten har behov av att säkerställa att personuppgiftsbiträdesavtal regelbundet följs upp för att kontrollera att överenskomna villkor uppfylls och att biträdet gör vad som överenskommits. Eftersom bolaget är personuppgiftsansvarigt är det också viktigt att man har rutiner och kompetens att bedöma hela kedjan av underbiträden. Detta är särskilt viktigt i ljuset av Schrems II-domen och problematiken med tredjelandsöverföring.

I den mån verksamheten 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.

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:

Ett aktuellt och uppdaterat personuppgiftsregister kan vara ett användbart hjälpmedel i verksamhetens dataskyddsarbete. Bolaget behöver säkerställa att all nödvändig information dokumenteras i personuppgiftsregistret så att registret

uppfyller de krav som ställs i dataskyddsförordningen. Dataskyddsombudet instämmer i bolagets bedömning i att registret behöver se över och uppdateras utifrån de behandlingar bolaget faktiskt har i dagsläget, då uppfattning är att behandlingarna förts in en gång och därefter inte kontrollerats. Det är också viktigt att en eller flera utpekade personer i bolaget ansvarar för registret och säkerställer att behandlingarna är korrekt angivna samt att registret kontinuerligt uppdateras. När det arbetet är gjort, kan registret med fördel användas i det löpande dataskyddsarbetet.

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. 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 verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet. Verksamheten behöver också regelbundet genomföra egna kontroller för att se hur dataskyddsförordningen efterlevs internt, det räcker inte enbart med de kontroller som genomförs av dataskyddsombudet.

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 bolagets medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Bolaget har behov av att ge medarbetarna möjlighet att delta i både interna och externa utbildningsinsatser för att höja den allmänna kunskapsnivån om dataskydd. Den lokala dataskyddsorganisationen bör ges rätt förutsättningar för att kunna genomföra informationsinsatser. För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser måste verksamheten kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter

genomförda utbildningar. Dataskyddsenheten erbjuder utbildningar men dataskyddsombudet kan även hålla riktade utbildningar vid identifierat behov,

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. Även de anställda måste informeras om hur deras personuppgifter behandlas, särskilt om en ny behandling påbörjas. Informationen ska vara enkel att nå för den registrerade. Bolaget rekommenderas att regelbundet se över policyn och uppdatera vid behov. Till exempel bör policyn uppdateras om överföring av personuppgifter till tredjeland, i de fall bolaget har någon sådan.

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:

Resultatet på kontrollpunkten visar att bolaget har identifierat en del risker som kräver åtgärder. 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. Det är också viktigt att se till så att alla medarbetare har kunskap om bolagets dokumenthantering och gallringsbestämmelser. Det finns även behov av att se över verksamhetens informationsklassificering av personuppgiftsbehandlingar och kontrollera så att detta görs i enlighet med Göteborgs Stads riktlinjer för informationssäkerhet. Bolaget måste även se till så att medarbetarna vet hur information ska hanteras beroende på informationsklassningen. 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 tex hänvisning i e-postsignaturen till verksamhetens integritetspolicy.

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. Det är därför mycket viktigt att bolaget ser till så att det finns rutiner för att identifiera riskfyllda personuppgiftsbehandlingar samt att konsekvensbedömningar genomförs innan sådana behandlingar påbörjas. Det är inte enbart för nya former av riskfyllda behandlingar som konsekvensbedömningar behöver göras utan det finns behov för bolaget att säkerställa att konsekvensbedömningar har genomförts för alla befintliga behandlingar där det föreligger en hög risk. Det behöver även finnas rutiner för att uppdatera en befintlig konsekvensbedömning vid förändringar.

Verksamheten 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. Dataskyddsombudet har under året inte blivit involverad i någon konsekvensbedömning, därför är siffran fyra på pågående konsekvensbedömningar svår att bemöta.

Det är även viktigt att bolaget ser över hur beslut om att acceptera risker i en konsekvensbedömning fattas och dokumenteras samt att det finns rutiner för att följa upp beslutade åtgärder. Verksamheten behöver också ta fram ett arbetssätt för att inhämta de registrerades synpunkter i vissa fall.

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 behov av att säkerställa att dataskyddsperspektivet finns med redan i anskaffandet av nya IT- och digitaliseringslösningar samt vid utvecklingen av

redan befintliga system och tjänster. 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. Verksamheten bör även ha som rutin att dataskyddsombudet involveras från start i dessa processer.

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 behöver säkerställa att de rutiner man har för tilldelning av behörigheter och åtkomster i IT-system är uppdaterade och korrekta, samt att behörigheter och åtkomster regelbundet följs upp. Det är ett bra sätt att säkerställa att medarbetarna enbart får tillgång till sådana personuppgifter som är nödvändiga för dem i sitt arbete.

Bolaget behöver kartlägga och sammanställa information om samtliga IT-system och digitala verktyg som verksamheten använder. Det behövs också en dokumenterad anskaffningsprocess för att säkerställa dataskyddsperspektivet vid införande av nya tjänster, system eller appar som inte kräver upphandling.

Det är viktigt att verksamheten utför kontroller så att IT-system och digitala verktyg används på rätt sätt. Därför är det även nödvändigt att verksamheten ser till att informera om korrekt användning.

Det finns även behov för bolaget att, i den mån man använder sig av cookies, säkerställa att användningen följer kraven enligt GDPR och korrekt information lämnas. Av att döma av den cookieruta som finns på hemsidan så uppfyller den inte kraven, då den registrerade inte får någon information om vilka personuppgifter som behandlas om man trycker på “jag förstår” knappen.

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:

Bolaget behöver öka medarbetarnas kunskap om de registrerades rättigheter och i vilka fall rättigheterna begränsas. Verksamheten behöver säkerställa att det finns rutiner för att hantera invändningar mot en personuppgiftsbehandling, då det är en rättighet den registrerade i vissa fall har när en personuppgiftsbehandling grundar sig på allmänt intresse, led i myndighetsutövning eller intresseavvägning. Personuppgiftsansvarig är skyldig att meddela den registrerade vid första kontakttillfället om sin rätt att invända till behandlingen.

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 uppger att man kartlagt vilka sociala medier som används, men att man inte har fattat något beslut avseende fortsatt användning efter Schrems II-domen. Dataskyddsombudet rekommenderar bolaget att undersöka vilken personuppgiftsbehandling som sker på dessa sociala medier, och om fortsatt användning ska ske bör detta beslut fattas på behörig nivå.

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 en organisation med ansvar och roller, där organisationen hade särkunskap inom juridik och IT. Bolaget fick rekommendationer kopplade till sin integritetspolicy, att ta fram plan för dataskyddsarbetet 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): Granskning av utbildningsnivå i dataskydd.

Granskningen genomfördes 2020 och bestod av ett antal frågor med syfte att undersöka den interna kunskapsnivån avseende dataskydd.

Verksamheten gavs följande rekommendationer:

- Kunskapsnivån bör förbättras genom utbildningar.
- Utbilda 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 2.4.6kontrollpunkt 6: Utbildning.

2.6.2 Uppföljning av genomförda kontroller 2021

Den fördjupade kontrollen genomfördes i oktober-november och uppföljning kommer därför ske under våren 2022.

2.7 Sammanfattande rekommendationer

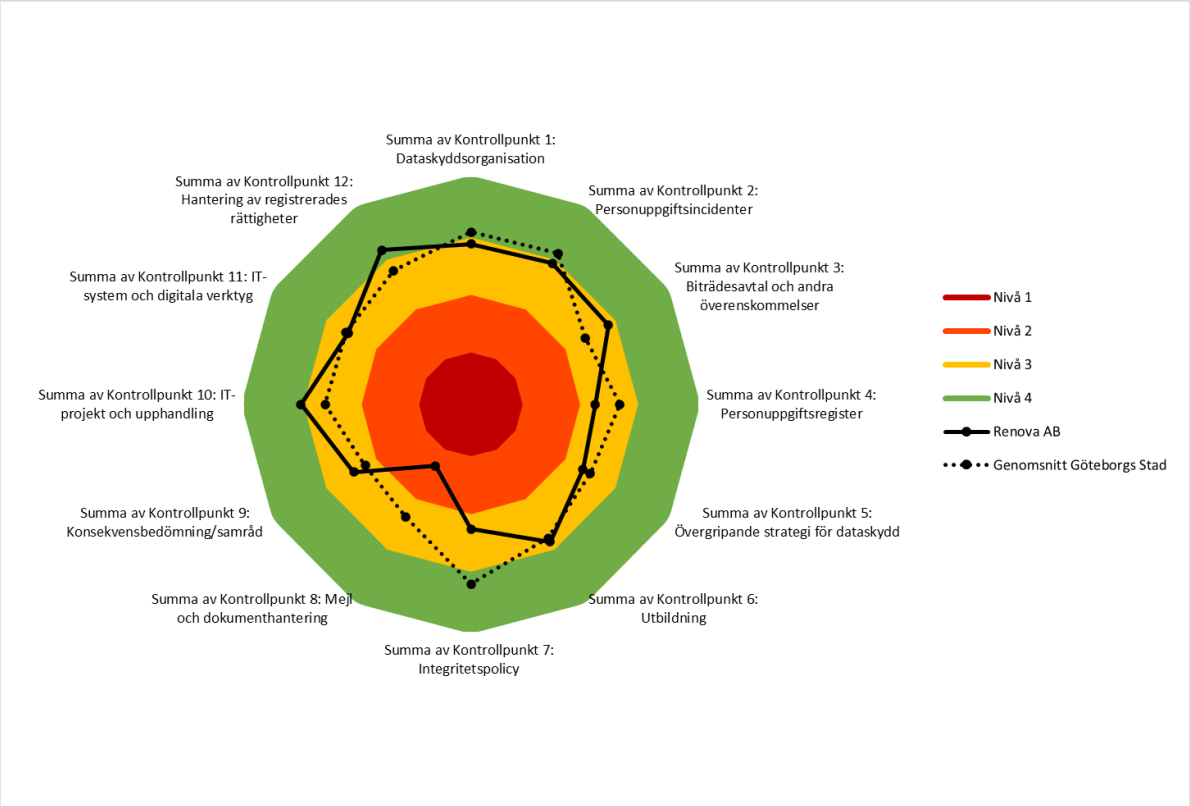
För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en mer noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar 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 en kontrollpunkt där man placerar sig inom risknivå två och där det följaktligen finns skäl att särskilt fokusera sina resurser. Dessa utgörs av ”Kontrollpunkt 8: Mejl- och dokumenthantering”. Inom dessa områden finns det identifierade risker som bedöms vara omfattande och som kräver åtgärder.

3 Bilagor

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



3.2 Fördjupad kontroll. Hantering av anställdas personuppgifter: GPS

Se separat bilaga för rapport avseende den fördjupade kontrollen.