



# Årsrapport för dataskyddsarbetet 2021

**Gryaab**

2021-12-20

# Innehåll

<b>1</b>	<b>Dataskyddsarbetet</b>	<b>4</b>
1.1	Att förvalta ett förtroende	4
1.2	Dataskyddsenhetens gemensamma arbete	4
<b>2</b>	<b>Kontrollarbetet</b>	<b>5</b>
2.1	Ett systematiskt arbete	5
2.2	Rättsutveckling som påverkat kontrollarbetet under året	5
2.2.1	Tredjelandsöverföringar (överföringar till länder utanför EU/EES)	5
2.2.2	Rätt beslutsnivå	6
2.2.3	Kommungemensamma interna tjänster	7
2.3	Årets kontrollarbete	8
2.3.1	Fördjupad kontroll	8
2.3.2	Fasta kontrollpunkter	8
2.4	Resultat av fasta kontrollpunkter för Gryaab	10
2.4.1	Kontrollpunkt 1: Dataskyddsorganisation	10
2.4.2	Kontrollpunkt 2: Personuppgiftsincidenter	10
2.4.3	Kontrollpunkt 3: Biträdesavtal och andra överenskommelser	11
2.4.4	Kontrollpunkt 4: Personuppgiftsregister	11
2.4.5	Kontrollpunkt 5: Övergripande strategi för dataskydd	12
2.4.6	Kontrollpunkt 6: Utbildning	12
2.4.7	Kontrollpunkt 7: Integritetspolicy	13
2.4.8	Kontrollpunkt 8: Mejl och dokumenthantering	13
2.4.9	Kontrollpunkt 9: Konsekvensbedömning/samråd	14
2.4.10	Kontrollpunkt 10: IT-projekt och upphandling	15
2.4.11	Kontrollpunkt 11: IT-system och digitala verktyg	15
2.4.12	Kontrollpunkt 12: Hantering av registrerades rättigheter	16
2.5	Särskilda iakttagelser	16
2.5.1	Tredjelandsöverföring och användningen av sociala medier	16
2.6	Uppföljning	17
2.6.1	Uppföljning av genomförda kontroller 2018 - 2020	17
2.6.2	Uppföljning av genomförda kontroller 2021	18
2.7	Sammanfattande rekommendationer	19

<b>3</b>	<b>Bilagor .....</b>	<b>20</b>
3.1	Bilaga 1: Diagram över resultat av fasta kontrollpunkter, i jämförelse med Göteborgs Stads genomsnitt. ....	20

# 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 kommundemensamma interna tjänster.

#### 2.2.1 Tredjelandsoverföringar (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 personuppgiftsbehandlingsåtgärder 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 bolagsledningarna.

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 personuppgiftsregistret och hantering av biträdesavtal och andra överenskommelser. Dessa har genomförts under våren och presenterades för styrelsen i juni 2021 i enlighet med det som angivits i kontrollplanen.

Dataskyddsombudet har i rapporterna avseende de fördjupade kontrollerna haft vissa anmärkningar och lämnat 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.<sup>1</sup>

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.

---

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



## Beskrivning av risknivåer

Riskenivåer	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 Gryaab

### 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 inga direkta risker föreligger som kräver åtgärder. Dataskyddsombudet instämmer i bedömningen och anser att bolaget har en god intern dataskyddsorganisation. Det finns goda förutsättningar för att bedriva ett effektivt och fungerande dataskyddsarbete. Den interna dataskyddsgruppen består av tre personer med olika kompetens som regelbundet träffas och diskuterar dataskyddsfrågor. Bolaget rekommenderas säkerställa att beslut fattas på behörig nivå och att det finns definierade rapporteringsvägar för hur dataskyddsfrågor ska informeras om inom bolaget. Slutligen rekommenderas bolaget att säkerställa att det finns särskilda befattningar/roller med utpekat ansvar och mandat att fatta beslut i olika typer av dataskyddsfrågor.

### 2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter



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

#### Kommentarer och rekommendationer:

Dataskyddsombudet granskade bolagets hantering av personuppgiftsincidenter under hösten 2020 och anser att bolaget har bra koll på hanteringen. Rutiner finns på plats både för att upptäcka och utreda incidenter, men också för att bedöma om de ska anmälas eller inte och hur de ska dokumenteras. Under det senaste året har dataskyddsombudet inte fått kännedom om någon incident, så det går inte att bedöma huruvida bolaget gjort korrekta bedömningar avseende anmälan till tillsynsmyndigheten. En av rekommendationerna i granskningen 2020 var att bolaget bör förtydliga i rutinen hur och när dataskyddsombudet ska informeras och rådfrågas vid inträffande av en incident. Eftersom dataskyddsombudet ska anges som kontaktperson vid anmälan till tillsynsmyndigheten, är det av största vikt att incidenten kommer till dataskyddsombudets kännedom. Därför är det viktigt att detta framkommer i rutinen.

Bolaget rekommenderas också att fortsätta utbilda och påminna medarbetarna i bolaget om vad en incident är och hur de ska hantera en misstänkt/inträffad incident.

### 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:

Bolagets hantering av biträdeavtal och andra överenskommelser granskades under vårens fördjupade kontroll och för de rekommendationer som lämnades har åtgärder vidtagits. Kontrollen avsåg bolagets mall för avtalsskrivande samt en stickprovskontroll på tre befintliga avtal.

Bolaget rekommenderas se över befintliga biträdesrelationer och säkerställa så att avtal finns på plats för att reglera förhållandet. Det bör även finnas instruktioner till varje avtal som mer i detalj beskriver hur personuppgifterna får behandlas. Det bör också finnas en rutin för att bedöma huruvida det uppstår en biträdessituation vid anlitan av leverantör eller kund. Bolaget saknar i dagsläget rutin för att göra efterlevnadskontroller på biträdena, vilket är viktigt för att säkerställa att de följer förordningen och de krav som ställs på dem i avtalet. Slutligen är det viktigt, särskilt i ljuset av Schrems II-domen, att bolaget har kompetens och praktisk möjlighet att säkerställa kontroll av hela kedjan av biträden. Som personuppgiftsansvarig är man ansvarig för hela kedjan, och ska kräva in relevanta avtal och information rörande underbiträden som biträdet har.

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:

Dataskyddsombudet har under våren granskat bolagets personuppgiftsregister och instämmer i den bedömning som gjorts. Registret är i dagsläget uppdaterat och innehåller bolagets alla behandlingar. 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. För att bibehålla den höga skattningen bör bolaget regelbundet se över registret och säkerställa att det är uppdaterat.

### 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. 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. Bolaget behöver också regelbundet genomföra kontroller för att säkerställa att dataskyddsförordningen efterlevs. Bolaget rekommenderas också ta fram dokumenterade rutiner för att säkerställa efterlevnad mot kraven i dataskyddsförordningen vid anordnande av fysiska/digitala sammankomster. Det är också viktigt att sådana rutiner kommer till alla medarbetares kännedom.

### 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 ger regelbundet medarbetarna möjlighet att delta i både interna och externa utbildningsinsatser som höjer 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 har bolaget kartlagt vilka utbildningar och andra kompetenshöjande insatser som behövs samt att man följer 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 bolagets 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. Dataskyddsombudet instämmer i bolagets bedömning av kontrollpunkten men rekommenderar ändå bolaget att se över integritetspolicyn regelbundet. Till exempel så hänvisar man i dagsläget till Datainspektionen, fastän den svenska tillsynsmyndigheten bytte namn till Integritetsskyddsmyndigheten vid årsskiftet 2020/2021. Dataskyddsombudet har inte granskat bolagets integritetspolicy i detalj i dagsläget. I den mån bolaget hänvisar till sin integritetspolicy för beskrivning av hur man behandlar personuppgifter i särskilda fall, är det bra om den beskriver även specifika behandlingar. Integritetspolicyn bör uppdateras med information om tredjelandsoverföring, i de fall bolaget har någon sådan.

Slutligen är det viktigt att bolaget säkerställer att integritetspolicyn är enkel att nå från alla bolagets kommunikationskanaler, t.ex. sociala medier.

## 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. Det är också viktigt att se till så att alla medarbetare har kunskap om bolagets dokumenthantering och gallringsbestämmelser. Det finns ett 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. 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. Den skattning bolaget gjort visar att arbetet med konsekvensbedömningar fungerar bra, men att några risker är identifierade. Dataskyddsombudet instämmer inte helt i den skattning som bolaget har gjort, utan anser att det praktiska arbetet med konsekvensbedömningar inte fungerar fullt så väl. Efter dialog med dataskyddskontakterna framkommer också att man till viss del missuppfattat kontrollpunkten och saknar kunskap om vad en konsekvensbedömning är enligt förordningen och när en sådan ska göras.

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.

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. Bolaget måste också ha en rutin som säkerställer att beslut om att acceptera 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 skattning innebär att inga större risker har identifierats som behöver åtgärdas, och dataskyddsombudet ser ingen anledning att ha en avvikande åsikt. Dataskyddsombudet har dock inte blivit involverad i några IT-projekt eller upphandlingar det senaste året, varpå insyn saknas i bolagets hantering. Det är viktigt att bolaget säkerställer dataskyddsperspektivet även vid upphandling samt arbetar systematiskt och kontinuerligt för att bedöma risker för personuppgiftsbehandlingar vid upphandling och utveckling. Bolaget rekommenderas säkerställa att inbyggt dataskydd och dataskydd som standard säkerställs vid upphandling. Framöver rekommenderas bolaget involvera dataskyddsombudet mera.

## 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 visar att vissa risker är identifierade som kräver åtgärder. Det handlar framför allt om att bolaget bör ta fram dokumenterade rutiner för tilldelning av behörigheter och åtkomster i IT-system samt regelbunden uppföljning, eftersom det säkerställer att medarbetares tillgång till personuppgifter är anpassade och begränsade utifrån vad som är nödvändigt.

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. Vid användning av analyskakor som kräver samtycke ska en korrekt s.k. cookiebanner tas fram.

## 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 kan öka medarbetarnas kunskap om de registrerades rättigheter och i vilka fall rättigheterna begränsas, t.ex. genom att ha med det i utbildningar. Bolaget behöver säkerställa att det finns rutiner för att hantera invändningar mot en personuppgiftsbehandling och för att hantera situationen då ett samtycke från en registrerad dras tillbaka. Vid användning av samtycke är det viktigt att bolaget har koll på administreringen av samtycken och att det finns rutin för att hantera 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.

Bolaget har arbetat med frågan angående fortsatt användning av sociala medier under hösten. Dataskyddsgruppen planerar att ta fram en konsekvensbedömning avseende den registrerades risker medan kommunikationsavdelningen tar fram ett material som styrelsen ska fatta beslut på. Kommunikationsavdelningens material rekommenderar styrelsen att fatta beslut om fortsatt användning av sociala medier. Dataskyddsombudet kommer att lämna en officiell kommentar som kommer biläggas ärendet samt kommentarer till konsekvensbedömningen.



## 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.

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades bygga upp organisation och metod för arbetet med det interna dataskyddsarbetet. I och med att organisationen var ny, fanns det inte mycket för dataskyddsombudet att kommentera på. Bolaget rekommenderades konkretisera kontakten med dataskyddsombudet så snart dataskyddskontakten kommit tillrätta i sin roll.

#### Kommentarer och rekommendationer:

Uppföljningen av denna kontroll har genomförts inom ramen för den skattnings som bolaget gjorde via den utskickade enkäten. Den visade att det fortfarande finns några 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.

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades förbättra den allmänna kunskapsnivån inom dataskydd genom att genomföra flera utbildningsinsatser. Utbildningsinsatserna bör även följas upp. Bolaget rekommenderades särskilt fokusera på de som hanterar känsliga personuppgifter samt 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.

Kontroll 3 (2020): Hantering av personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades komplettera sin rutin med den korta tidsfrist som gäller för anmälan av en incident samt hur ett biträde kommunicerar en inträffad incident till bolaget. Bolaget rekommenderades ta fram en rutin för riskbedömning och säkerställa att den information som lämnas till de registrerade följer kraven i

förordningen, samt lämnas vid rätt tidpunkt. Rutinen behövde också kompletteras med när dataskyddsombudet ska informeras.

#### 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.

### **2.6.2 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 biträdesavtal och andra överenskommelser**

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades att uppdatera rutinen med biträdes skyldighet att gå med på och bistå vid granskning och inspektioner. Bolaget rekommenderades också att ta fram rutin för att kunna följa upp så att biträden uppfyller sina åtaganden enligt avtalet.

#### Kommentarer och rekommendationer:

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

#### **Kontroll 2 (2021): Personuppgiftsregistret**

Verksamheten gavs följande rekommendationer:

Bolaget rekommenderades att komplettera registret med kontaktuppgifter till personuppgiftsbiträden då det i vissa behandlingar saknades. Bolaget rekommenderades också ta fram en rutin för arbetet med registret som innehåller information om de obligatoriska kraven samt ansvar och roller för registret inom bolaget.

#### 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 framförallt ”Kontrollpunkt 3: Biträdesavtal och andra överenskommelser” som kräver omfattande åtgärder. Men även övriga punkter som hamnade på risknivå 3 behöver åtgärder som kan vara omfattande. Dataskyddsombudet rekommenderar även bolaget att se över arbetet med konsekvensbedömningar under ”Kontrollpunkt 9: Konsekvensbedömningar/Samråd”.

# 3 Bilagor

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



