Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Intraservice

2023-01-09

Innehåll

1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) 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. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

2.2 Fördjupad kontroll

2.2.1 Kontroll av integritetspolicy 2022

Den fördjupade kontrollen har bestått av en kontroll av hur väl förvaltningen uppfyller informationsskyldigheten enligt GDPR. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten för den fördjupade kontrollen haft vissa synpunkter och därför lämnat ett antal rekommendationer till verksamheten att vidta vissa åtgärder.

Sammanfattade rekommendationer:

- Ta fram verksamhetsspecifik information (intern integritetspolicy) som fokuserar på de behandlingar som omfattar anställda.

- Utreda hur policyn bättre kan formuleras, t.ex. med hjälp av skiktad integritetspolicy, eller hur det annars kan säkerställas att information lämnas till de registrerade.
- Se över informationen om tredjelandsöverföring.
- Ange precis lagringstid för uppgifterna (inte ange "så länge det är nödvändigt för de berättigade ändamålen")
- Om samtycke används som rättslig grund rekommenderas det att informationen kompletteras med uppgifter om hur ett samtycke kan återkallas.
- Se över språket för att uppfylla kravet på ett klart och tydligt språk.
- Ta bort hänvisning till intranätet eftersom informationen där är ej åtkomlig för utomstående och inte kan fungera som ett komplement till integritetspolicyn.

2.2.2 Uppföljning av tidigare genomförda kontroller

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll (2021): Personuppgiftsbiträdesavtal och andra överenskommelser

Verksamheten gavs följande rekommendationer:

- Förvaltningen bör utforma och bilägga instruktioner till de personuppgiftsbiträdesavtal där det saknas.
- Förvaltningen bör ta fram rutin eller tydliggöra hur redan existerande stöddokument ska användas vid säkerställande/uppföljning av ett biträdes tekniska och organisatoriska säkerhetsåtgärder.
- Förvaltningen bör utreda behov av att ta fram rutin för avtalsuppföljning.
- Förvaltningen bör överväga att i så stor utsträckning som möjligt använda egen mall för personuppgiftsbiträdesavtal för att minimera risken för ofördelaktiga avtalsvillkor.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har identifierat ett antal åtgärder utifrån dataskyddsombudets årsrapport 2021. Förslaget innehåller en rekommendation till uppstart av ett projekt där åtgärder vidtas i sin helhet utifrån vad som tas upp i årsrapporten 2021. Kopplat till kontrollen av biträdesavtal och andra överenskommelser har förvaltningen identifierat följande projektaktiviteter som bör vidtas:

- En process för bedömning kring tecknande av personuppgiftsbiträdesavtal som inkluderar att en bedömning görs kring om det verkligen rör sig om en biträdesrelation, samt, tillser att ändamålsenliga avtal/processer definieras i de fall där det inte bedöms röra sig om en biträdesrelation (exempelvis när det rör sig om gemensamt personuppgiftsansvar).

- Processen behöver även inkludera aktiviteter tillhörande kontinuerlig översyn av personuppgiftsbiträdesavtal.
- En fastställd mall för personuppgiftsbiträdesavtal.

I uppföljningen anges att åtgärden enbart utgör ett förslag till hantering, och dataskyddsombudet har i skrivande stund (december 2022) ännu inte fått bekräftat ifall förvaltningsledningen har beslutat att det beskrivna projektet med tillhörande aktiviteter ska påbörjas. Utifrån detta, och då förvaltningen under 2022 inte vidtagit några åtgärder utifrån tidigare lämnade rekommendationer, gör dataskyddsombudet bedömningen att samtliga rekommendationer kvarstår och att fortsatt uppföljning därför krävs under 2023.

2.2.3 Särskild uppföljning gällande förvaltningens hantering av personuppgiftsincidenter

Dataskyddsombudet lämnade i Intraservices årsrapport 2021 särskilda rekommendationer gällande förvaltningens hantering av personuppgiftsincidenter, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, då den bristfälliga hanteringen bedömdes medföra höga risker för såväl den egna förvaltningen som övriga verksamheter inom staden.

Utifrån de rekommendationer som lämnades har förvaltningen identifierat att följande åtgärder behöver vidtas:

- Säkerställande av en ändamålsenlig personuppgiftsincident-hanteringsprocess som inkluderar:
- Process inkl. kriterier för hur/om de registrerade ska informeras,
- Kriterier och rutiner för när och hur en incident ska anmälas till tillsynsmyndighet,
- Att dataskyddsombudet, både i osäkra fall och vid större incidenter, ska rådfrågas och involveras.

Samt, inom ramarna för tjänsteleveransen;

- Processer och rutiner för att korta ned tiden mellan det att förvaltningen får kännedom om en incident till dess att personuppgiftsansvariga underrättas,
- Tydliga instruktioner för vilken information som ska kommuniceras till personuppgiftsansvariga.

I uppföljningen anges att åtgärden enbart utgör ett förslag till hantering, och dataskyddsombudet har i skrivande stund (december 2022) ännu inte fått bekräftat ifall förvaltningsledningen har beslutat att det beskrivna projektet med tillhörande aktiviteter ska påbörjas. Utifrån detta, och då förvaltningen under 2022 inte vidtagit några åtgärder utifrån tidigare lämnade rekommendationer, gör dataskyddsombudet bedömningen att samtliga rekommendationer kvarstår och att fortsatt uppföljning därför krävs under 2023.

Med anledning av de höga risker nuvarande incidenthantering medför för staden som helhet rekommenderas nämnden uppdra åt förvaltningen att prioritera arbetet med denna fråga under 2023.

Se fler rekommendationer under kontrollpunkt 2 avseende personuppgiftsincidenter (rubrik 2.4.2).

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

2.3.1 Metod och risknivåer

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar 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.[3]

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 Intraservice dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

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.

Dataskyddsombudets kommentarer:

Verksamhetens resultat visar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. I skattningen anges att det inom förvaltningen saknas en intern organisation för dataskyddsarbetet där roller och ansvar är definierade, att det saknas definierade rapporteringsvägar i dataskyddsfrågor, att den interna dataskyddsorganisationen inte har tillräckligt med resurser för att kunna bedriva ett systematiskt dataskyddsarbete samt att det saknas rutiner som säkerställer att dataskyddsombudet regelbundet kontaktas för att delta i frågor som rör skyddet av personuppgifter. Sammantaget, utifrån förvaltningens skattning och gjorda iakttagelser under året, är dataskyddsombudets bedömning att förvaltningen i praktiken saknar en intern dataskyddsorganisation. Utifrån gjorda iakttagelser är det för dataskyddsombudet även tydligt att det inte bedrivs något systematiskt dataskyddsarbete inom verksamheten.

Av den gjorda skattningen delar dataskyddsombudet i stort förvaltningens bedömning, med undantag från att dataskydd bedöms vara en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten. Dataskyddsombudet möter regelbundet medarbetare i förvaltningen som inte har kunskap om dataskydd och reglerna som de ska följa. Dataskyddsombudet anser att dataskyddsperspektivet ofta saknas eller kommer in alldeles för sent i processerna. De råd och rekommendationer som dataskyddsombudet lämnar saknar mottagare och omhändertas inte heller i organisationen. I sammanhanget har dataskyddsombudet också noterat att det inte enbart handlar om okunskap i dataskydd, utan även om andra lagar såsom kommunallagen, offentlighet och sekretesslagstiftningen (OSL), arkivlagstiftning m.fl., vilka är nära sammankopplade med dataskyddslagstiftningen och centrala för offentlig verksamhet.

Dataskyddsombudet kan vidare se att förvaltningen inte vidtagit några åtgärder med anledning av de rekommendationer som lämnades i årsrapporten 2021. I förvaltningens årsrapport lyftes då bl.a. avsaknaden av dataskyddskompetens inom verksamheten som en hög risk och förvaltningen rekommenderades utreda vilka interna resurser och kompetenser som behövs inom verksamheten, och hur dessa resurser kan organiseras och samverka för att säkerställa en fungerande dataskyddsorganisation. Kopplat till det rekommenderades förvaltningen även se

över dåvarande konsultberoende inom området, då detta bedömdes medföra en ostabilitet och osäkerhet inom organisationen.

Dataskyddsombudet bedömer att det är av högsta vikt att förvaltningen omgående tillsätter resurser för att kunna bygga upp en intern dataskyddsorganisation. Den nuvarande organisationen, på kansliet, bedöms vara kraftigt underdimensionerad och sakna nödvändiga resurser för att kunna utföra uppdraget, även om kompetens i dataskydd finns hos ansvariga medarbetare. Nuvarande organisation har under en längre tid också själva uppmärksammat att det saknas förutsättningar för att kunna bedriva ett systematiskt dataskyddsarbete med hänvisning till brist på tid och resurser inom förvaltningen som helhet. Förvaltningen rekommenderas därför omgående ge den interna dataskyddsorganisationen möjlighet att se över vilka resurser, vilken kompetens och vilka rutiner/anvisningar (kopplat till roller, ansvar) man behöver inom verksamheten för att kunna säkerställa dataskyddsperspektivet fullt ut. Utifrån nämndens uppdrag och ansvar kopplat till digitalisering och digital infrastruktur är det särskilt anmärkningsvärt att förvaltningen fortfarande inte kunnat säkerställa en ändamålsenlig dataskyddsorganisation, trots att flertalet förslag på dess utformning tagits fram sedan GDPR trädde i kraft våren 2018.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bör åtgärdas men de bedöms inte vara brådskande, omfattande eller allvarliga. Oaktat förvaltningens skattning gör dataskyddsombudet bedömningen att det inom kontrollpunkten föreligger höga risker som kräver omgående åtgärder. Utifrån gjorda iakttagelser bedöms riskerna vara kopplade till brister i rutiner såväl som kunskap hos medarbetare.

Dataskyddsombudet har enbart fått kännedom om en inträffad personuppgiftsincident för förvaltningen i egenskap av personuppgiftsansvarig under 2022. En förvaltning som hanterar den mängd personuppgifter som Intraservice gör borde rimligtvis ha ett flertal inträffade incidenter varje år. Avsaknaden av incidenter indikerar att kunskapen om vad som utgör en personuppgiftsincident behöver öka inom verksamheten. Att ha få rapporterade incidenter behöver inte per definition innebära att allt fungerar som det ska, utan kan snarare tvärtom innebära att medarbetare inte kan identifiera när en incident inträffar. Det är viktigt att inträffade incidenter rapporteras så att de kan utredas och åtgärder vidtas för att liknande incidenter inte ska inträffa på nytt.

Vid de tillfällen dataskyddsombudet har varit involverad i hanteringen av personuppgiftsincidenter under året har det tydligt framgått att det saknas

grundläggande kunskaper om dataskyddsförordningen hos incidentkoordinatorer såväl som hos de ansvariga för tjänsterna (inom vilka incidenter inträffat). Det har förekommit att dataskyddsombudet behövt argumentera för varför något utgör en incident, och dataskyddsombudet har upplevt att det vid tillfällen funnits en motvilja till att acceptera att något utgör en personuppgiftsincident. Denna motvilja utgör i sig en risk eftersom det medför att individer kan känna en ovilja att anmäla när något inträffar, utifrån risken att bli upplevd som besvärlig.

Förvaltningen rekommenderas därför att utvärdera arbetssätt, rutiner och den information som medarbetarna har fått till sig för att bedöma eventuella åtgärder eftersom (den förväntade) effekten hittills tycks ha uteblivit. Förvaltningen behöver säkerställa att det finns tillräcklig kunskap hos medarbetare och rutiner på plats som ger förutsättningar för att identifiera, utreda och i förekommande fall anmäla incidenter. Det är också viktigt att det finns en kultur där rapportering av incidenter uppmuntras, för att säkerställa att mörkertal och underrapportering inte förekommer. Oavsett om det handlar om kunskap, rutiner, arbetssätt eller är en kulturfråga behöver verksamheten identifiera var det brister för att kunna arbeta vidare med frågan, så att incidenter framledes identifieras, rapporteras, utreds och i förekommande fall anmäls till tillsynsmyndigheten.

Dataskyddsombudet rekommenderar vidare förvaltningen att omgående säkerställa att incidentkoordinatorer, såväl som andra ansvariga för hanteringen av incidenter, genom nödvändiga utbildningsinsatser får rätt förutsättningar för att kunna hantera uppdraget. Förslagsvis genom att möjliggöra för medarbetarna att delta vid dataskyddsenhetens utbildningar.

Dataskyddsombudet lämnade i förra årets rapport särskilda rekommendationer kopplat till förvaltningens hantering av personuppgiftsincidenter. En förbättring sedan förra året är att incidentkoordinatorerna i större utsträckning kontaktar dataskyddsombudet för hjälp att bedöma incidenter, vilket är positivt och bedöms stärka hanteringen.

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.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens bedömning och kvarstår i uppfattningen om att det finns mycket kvar att göra när det kommer till hanteringen av biträden och biträdesavtal. Som anges i uppföljningen av den fördjupade

kontrollen för 2021 (se avsnitt 2.2.2) har förvaltningen tagit fram en plan för åtgärder utifrån dataskyddsombudets årsrapport 2021. Då den framtagna planen ännu ej medfört att några konkreta åtgärder vidtagits är dataskyddsombudets bedömning att tidigare identifierade risker kvarstår.

Dataskyddsombudet ser särskilt en stor risk när det kommer till förvaltningens kompetens att bedöma hela kedjan av underbiträden vid anlitande av en ny leverantör. Under året har det vid ett flertal tillfällen uppstått situationer där förvaltningen inte fullgjort sin omsorgsplikt enligt artikel 28 GDPR på grund av att det inte gjorts några ordentliga utredningar/bedömningar vid anlitande av nya leverantörer. Konsekvensen av detta har bland annat blivit att man ej kunnat använda tjänster man avropat/upphandlat, samt att kunder (övriga förvaltningar/bolag) valt att inte använda, eller inte fortsätta använda, tjänster som förvaltningen erbjuder. Att inte ha koll på anlitade leverantörer medför alltså inte enbart en risk för de registrerade, utan påverkar även förvaltningens möjligheter att sälja tilläggs- och specialisttjänster negativt.

I tillhandahållandet av tjänster förekommer det i flera fall att Intraservice agerar personuppgiftsbiträde gentemot andra verksamheter i staden, vilket ställer krav på kunskap i frågor kopplat till biträdesrollen. Dels vilka skyldigheter förvaltningen har gentemot personuppgiftsansvariga, dels vilket ansvar förvaltningen har gentemot underbiträden. Då Intraservice som regel agerar som en ”mellanhand” mellan verksamheter i staden och leverantörer, behöver verksamheterna kunna lita på att Intraservice uppfyller sina skyldigheter som biträde. För Intraservice innebär det bland annat att tillhandahålla information om behandlingar och leverantörer till förvaltningar/bolag, så att de i sin tur kan uppfylla sin omsorgsplikt enligt artikel 28 GDPR. I egenskap av ”mellanhand” blir alltså Intraservice en del i den kedjan av biträden som personuppgiftsansvariga, liksom Intraservice självt, behöver bedöma. Här ser dataskyddsombudet att det föreligger en risk för förvaltningen.

Dataskyddsombudets iakttagelse är att ansvariga inte har förståelse för ovanstående och därför både ifrågasätter och nekar förvaltningar/bolags tillgång till tekniska underlag. Om Intraservice fortsätter att inte tillhandahålla, eller sekretessbelägga utan ordentlig hänvisning, underlag som förvaltningar/bolag behöver ta del av för att kunna göra sina bedömningar kommer det få påverkan på både Intraservices roll som biträde och förvaltningar/bolags bedömningar gällande förvaltningens lämplighet som leverantör.

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.

Dataskyddsombudets kommentarer:

Dataskyddsombudet har under året haft ingen eller begränsad tillgång till förvaltningens personuppgiftsregister och har därför ingen insyn i hur arbetet fungerar. Efter dialog med verksamheten gör dock dataskyddsombudet bedömningen att det kvarstår mycket arbete med det interna personuppgiftsregistret så väl som det förvaltningen är skyldig att ha i rollen som biträde. Avsaknaden av en intern dataskyddsorganisation i kombination med tidigare punktinsatser av konsulter bedöms ha medfört att förvaltningen nu inte har något hållbart och fungerande arbete med registret. Vidare innebär bristerna i nuvarande register att förvaltningen inte uppfyller sin skyldighet att föra register över personuppgiftsbehandlingar enligt artikel 30 GDPR.

Förvaltningen rekommenderas framåt att ta ett omtag med registret för att säkerställa att alla behandlingar finns registrerade och att informationen är komplett. För att få ett register som uppfyller kraven enligt artikel 30 GDPR behöver förvaltningen börja registrera och beskriva behandlingar, istället för att utgå från tjänster eller system som görs i nuvarande register. Det måste också finnas ett utpekat ansvar för att uppdatera registret och föra in nya behandlingar.

Förvaltningen rekommenderas att under 2023 prioritera arbetet med att säkerställa att samtliga personuppgiftsbehandlingar dokumenteras i personuppgiftsregistret.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Sammantaget visar svaren att det saknas en överblick och en tydlig styrning i hur dataskyddsarbetet bedrivs, vilket innebär en risk eftersom man då bland annat riskerar att fokusera sina resurser på fel frågor. Från skattningen kan det utläsas att förvaltningen saknar en övergripande strategi för dataskyddsarbetet såväl som ett systematiskt arbete med att integrera dessa frågor i övrigt informations-säkerhetsarbete. Dataskyddsombudet delar förvaltningens bedömning och ser att detta är en effekt av att förvaltningen saknar en intern dataskyddsorganisation, vilket gör att planering, uppföljning och kontinuerligt arbete med dataskyddsfrågor i förvaltningen brister. För dataskyddsombudet tycks det även lite motsägelsefullt att ange att det finns ett riskbaserat arbetssätt i dataskyddsfrågor samtidigt som förvaltningen saknar en dataskyddsorganisation. Även om enskilda medarbetare kan arbeta riskbaserat i sina uppdrag, ser dataskyddsombudet en risk i att det inte får genomslag i praktiken just på grund av att förvaltningen saknar en intern dataskyddsorganisation som kan omhänderta och arbeta strategiskt med frågan.

För att få styrning i dataskyddsfrågor rekommenderas förvaltningen att ta fram övergripande styrande principer (till exempel i form av en strategi) samt ett årshjul

för det interna dataskyddsarbetet. I dagsläget saknas en överblick av förvaltningens arbete som helhet, vilket dataskyddsombudet bedömer blir särskilt tydligt vid utveckling av nya tjänster såväl som vid vidareutveckling av befintliga. Under året har det förekommit situationer där dataskyddsombudet blivit involverad i liknande/nära identiska projekt från olika håll inom förvaltningen, utan att dessa haft kännedom om varandra. Utöver att avsaknad av styrning utgör en risk i sig, har dataskyddsombudet vid flera tillfällen kunnat konstatera att projekt verkar ha initierats och arbetats med utan att först ha kontrollerats utifrån ett juridiskt perspektiv. I förekommande fall handlar det, utöver GDPR, om offentlighet- och sekretesslagstiftning såväl som andra lagrum som styr offentlig verksamhet.

Utifrån gjorda iakttagelser gör dataskyddsombudet bedömningen att tjänsteutvecklingen inom förvaltningen hittills främst styrts av viljan till en ökad digitalisering och användningen av ny teknik, i stället för att ha utgått från de lagrum som styr den kommunala verksamheten. Som en konsekvens av detta har gällande lagstiftning snarare försökt anpassas till tjänsternas förutsättningar och möjligheter, än vice versa. Detta bedöms medföra risker i form av en fortsatt utveckling av osäkra tjänster som inte tillhandahåller ett tillräckligt skydd för de personuppgifter som behandlas vid användning av dem.

Då lagefterlevnad är en förutsättning för att förvaltningen ska kunna bidra till en hållbar digitalisering inom staden, är det av stor vikt att förvaltningsledningen i form av både ord och handling signalerar betydelsen av detta inom verksamheten. Dataskyddsombudet bedömer att det är nödvändigt med ett skifte i prioriteringar inom verksamheten, och att det framåt blir tydligt för medarbetare att lagefterlevnad ej är något valbart, vare sig det gäller att följa GDPR, OSL eller något annat lagrum.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens bedömning. Det finns stora brister i medarbetarnas kunskap i dataskyddsfrågor, såväl som grundläggande kunskap och specifik kunskap för de som till exempel jobbar med tjänster inom HR, ekonomi, digital infrastruktur, IT-säkerhet, upphandlingar mm. Dataskyddsombudet rekommenderar förvaltningen att kartlägga utbildningsbehovet och identifiera de grupper som är i störst behov av utbildning.

Förvaltningen har en del utbildningsmaterial på intranätet, men efter en genomgång av detta kan dataskyddsombudet konstatera att denna information är inaktuellt och behöver uppdateras. Materialet som finns tillgängligt togs fram i samband med införandet av GDPR år 2018 och utifrån den rättsutveckling som skett sedan dess

finns risker för att medarbetare vid genomläsning av detta får fel information. Eventuellt nytt underlag rekommenderas stämmas av med dataskyddsombudet.

Utifrån förvaltningens uppdrag ser dataskyddsombudet anledning att särskilt lyfta den risk verksamhetens bristande kunskap i dataskydd utgör för staden som helhet. Denna risk bedöms särskilt föreligga inom verksamhetsområde IT (digital infrastruktur) och vara nära sammankopplad med avsaknaden av en övergripande strategi för dataskydd. Dataskyddsombudet rekommenderar förvaltningen att göra en särskild utbildningsinsats för ledningsgrupp samt medarbetare inom digital infrastruktur, med syftet att säkerställa att samtliga får grundläggande kunskaper i dataskyddsförordningen.

Dataskyddsenheten bidrar gärna både med grundläggande utbildning och mer riktade insatser, men förvaltningen måste ge medarbetarna möjlighet och förutsättning att kunna delta. Framåt uppmuntras förvaltningen till att både använda dataskyddsenhetens e-utbildning ”Dataskydd på jobbet” som är tillgänglig för alla verksamheter i Göteborgs Stad, samt säkerställa att medarbetare deltar vid de lärarledda utbildningar som enheten håller i.

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.

Dataskyddsombudets kommentarer:

Dataskyddsombudets bedömer att det inom kontrollpunkten föreligger risker som kräver åtgärder. Den högsta risken utgörs av att nuvarande integritetspolicy inte bedöms uppfylla kraven på information enligt artikel 13 och 14 GDPR, och att bolaget därför inte lever upp till informationsplikten. Sammantaget bedömer dataskyddsombudet att förvaltningen utför många behandlingar som inte täcks av integritetspolicyn, varpå förvaltningen behöver se över vilka andra sätt man har att uppfylla sin informationsplikt.

För att förvaltningen ska kunna uppfylla sin informationsplikt rekommenderas verksamheten fortsätta arbeta med att se över integritetspolicyn och uppdatera den så att informationen uppfyller kraven enligt GDPR.

Förvaltningens integritetspolicy är årets fördjupade kontroll och ytterligare rekommendationer från dataskyddsombudet finns i bilaga 1 till årsrapporten.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post 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.

Dataskyddsombudets kommentarer:

Förvaltningen har uppgett övervägande låga svar på kontrollpunkten vilket innebär att det föreligger stora risker som kräver åtgärder, vilket dataskyddsombudet instämmer i. En uppdaterad dokumenthanteringsplan med gallringsrutiner är en förutsättning för att förvaltningen ska kunna säkerställa principen om lagringsminimering enligt GDPR. Dataskyddsombudet rekommenderar att förvaltningen prioriterar arbetet med att ta fram en heltäckande dokumenthanteringsplan och tar fram rutiner för gallringsbeslut samt informerar medarbetarna om dokumenthantering och gallring. Dataskyddsombudet och förvaltningens kansli har under året identifierat ett möjligt samarbete i frågor kopplat till dokumenthantering och GDPR för att stärka medarbetares kunskap inom området som helhet. Vidare arbete i frågan kommer ske under 2023.

Utifrån den gjorda skattningen kan det också utläsas att en hög risk utgörs av att förvaltningen inte har någon uppfattning om hur stor andel av verksamhetens personuppgiftsbehandlingar som har informationsklassificerats utifrån stadens riktlinje om informationssäkerhet. Då förvaltningen, i egenskap av tjänsteleverantör, ställer krav på andra verksamheter att detta ska gjorts innan tjänster börjar användas finner dataskyddsombudet det motsägelsefullt att samma krav ej ställs på den egna förvaltningen.

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.

Dataskyddsombudets kommentarer:

Skattningen på kontrollpunkten indikerar utifrån den övergripande risknivån att det finns omfattande identifierade risker som kräver omgående åtgärder. Förvaltningens resultat på kontrollpunkten är väsentligt lägre än förra året, och dataskyddsombudets bedömning är att årets skattning mer korrekt avspeglar hur det faktiska arbetet med konsekvensbedömningar ser ut inom förvaltningen.

Vidare noterar dataskyddsombudet att flera av svaren tycks vara motsägelsefulla och inte spegla de faktiska omständigheterna. Till exempel anges att verksamheten har en dokumenterad rutin för att genomföra och dokumentera konsekvensbedömningar samt regelbundet involverar dataskyddsombudet för att inhämta råd vid konsekvensbedömningar, men trots detta har inte en enda

konsekvensbedömning färdigställts under året. Det framgår även att förvaltningen inte har kontrollerat några av sina personuppgiftsbehandlingar utifrån höga risker för de registrerades fri- och rättigheter, och det saknas dessutom planering för hur verksamheten framåt ska genomföra konsekvensbedömningar för dessa behandlingar.

Sammantaget visar svaren att det inom förvaltningen saknas förutsättningar för att på ett korrekt sätt kunna genomföra en konsekvensbedömning som uppfyller kraven enligt GDPR.

I dagsläget upplevs konsekvensbedömningar genomförs ad hoc inom förvaltningen och någon översyn över antalet konsekvensbedömningar finns, så vitt dataskyddsombudet vet, inte. Vid de tillfällen dataskyddsombudet blivit tillfrågad i arbetet med en konsekvensbedömning och lämnat rekommendationer har det inte varit tydligt hur dessa omhändertas samt följs upp. Dataskyddsombudet bedömer också att förvaltningen har en stor "skuld" över konsekvensbedömningar som borde ha genomförts på redan pågående behandlingar, men på grund av avsaknaden av en intern dataskyddsorganisationen samt brister i register-förteckningen, är det ingen i förvaltningen som har överblick av hur stor denna skuld är.

Sammantaget anser dataskyddsombudet att det inom kontrollpunkten finns omfattande risker som omgående behöver åtgärdas. Dessa utgörs både av risker för de registrerade, eftersom behandlingar där deras personuppgifter ingår inte har bedömts och risker för förvaltningen i form av förtroendeskada eller sanktionsavgifter vid en eventuell tillsyn. Dataskyddsombudet rekommenderar därför att förvaltningen framåt prioriterar arbetet med att genomföra konsekvensbedömningar. För att få en överblick och kunna planera arbetet framåt rekommenderas förvaltningen att som ett första steg kontrollera verksamhetens personuppgiftsbehandlingar utifrån höga risker och bedöma för vilka behandlingar konsekvensbedömningar behöver genomföras.

Eftersom konsekvensbedömningsarbetet är ett sätt för förvaltningen att hantera de risker som föreligger med behandlingar, är dataskyddsombudets rekommendation att förvaltningen implementerar arbetet med konsekvensbedömningar i den övergripande strategin för dataskydd samt tillhörande årshjul.

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.

Dataskyddsombudets kommentarer:

Förvaltningen har skattat sig själva lågt på kontrollpunkten och dataskyddsombudet instämmer i bedömningen. Dataskyddsombudets uppfattning är att det saknas rutiner och arbetssätt kopplat till GDPR vid upphandlingar. Det har vid flera tillfällen under året kunnat konstaterats att dataskyddsperspektivet missats i samband med upphandlingar, till exempel i form av bristfälliga kravställningar, vilket fått konsekvensen att det uppstår problem när tjänsterna ska börja används då dess användning inte är förenlig med GDPR. Dataskyddsombudet upplever också att det saknas kunskap hos medarbetarna om vilka krav/frågor de bör lyfta in i upphandlingar och även hur de ska ta emot dataskyddsombudets rekommendationer i de fall dataskyddsombudet blir involverad. Bristen på rutiner gör också att varje projekt i princip behöver formulera sina egna krav och frågor till leverantörerna. Dataskyddsombuden rekommenderar att förvaltningen tar fram rutiner kopplat till upphandling som säkerställer att dataskyddsperspektivet omhändertas tidigt i processerna. Förvaltningen behöver även förtydliga för medarbetarna att dataskyddsombudet ska involveras i alla frågor som rör dataskydd, även vid upphandlingar, samt ta fram en plan för kommande upphandlingar så att dataskyddsombudet får tid och möjlighet att planera sitt eget arbete. Ett bra exempel på sådan planering har tillhandahållits av tjänsteområdet HR, som redan inför det nya året informerat dataskyddsombudet om när verksamheten behöver stöttning.

Sammantaget rekommenderas förvaltningen framåt se över hur det kan säkerställas att dataskyddsombudet involveras i ett tidigt skede i uppstart av nya IT-projekt, vid införande av nya system/tjänster eller i samband med upphandlingar.

Kopplat till kravställning och upphandling har dataskyddsombudet under året blivit informerad om att det inom förvaltningen pågår ett arbete med en kravkatalog. I detta arbete har dataskyddsombudet ombett att bli involverad utifrån att det kunnat identifieras brister i nuvarande kravställningar kopplat till personuppgiftshantering. Trots flertalet påtryckningar har ansvariga inom verksamhetsområde IT hittills inte involverat dataskyddsombudet i arbetet. Någon motivering till varför har ej getts. Utifrån tidigare identifierade risker ser dataskyddsombudet att det föreligger en hög risk att en kravkatalog som Intraservice tar fram själva utan att involvera rätt kompetenser, både kopplat till informationssäkerhet i staden (CISO), arkivfrågor (regionarkivet), personuppgiftshantering (DSO) och inom upphandling (INK) kommer vara bristfällig. Dataskyddsombudet vill därför särskilt poängtera att förvaltningen framåt behöver involvera rätt kompetenser för att såväl den egna förvaltningen som andra verksamheter i staden ska kunna ha nytta av kravkatalogen.

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.

Dataskyddsombudets kommentarer:

Enligt verksamhetens skattning finns kvarstående risker kopplat till avsaknaden av en heltäckande och uppdaterad dokumentation över samtliga IT-system och digitala verktyg som används inom organisationen, målgruppsanpassad information för digitala verktyg samt rutiner för att systematiskt följa upp och kontrollera att användningen av system och/eller andra digitala verktyg följer antagna rutiner/riktlinjer/policys. Vidare saknas även en dokumenterad och tydlig överblick över kommunikationskanaler och rutiner för att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster såsom gratisappar och sociala medier.

Om man ser till den gjorda skattningen gällande behörigheter uppger förvaltningen en fyra på att det finns rutiner för tilldelning av behörigheter och åtkomst till IT-system, men en etta på uppföljning av behörigheter. Här ser dataskyddsombudet en risk om uppföljning aldrig sker, eftersom personal byter eller avslutar tjänster regelbundet inom förvaltningen. Förvaltningen rekommenderas därför ta fram rutiner som säkerställer att behörigheter följs upp både vid ändring och avslut av tjänst.

Vidare uppger förvaltningen att det saknas rutiner för att systematiskt kunna följa upp och kontrollera att användningen av system/digitala verktyg följer antagna rutiner/riktlinjer/policys. Med tanke på antalet system och digitala verktyg som används i verksamheten rekommenderar dataskyddsombudet att förvaltningen åtgärdar bristen. Förvaltningen uppger också att det saknas heltäckande och uppdaterad dokumentation över samtliga IT-system, vilket är en förutsättning för att efterlevnad av rutiner för system/verktyg ska få effekt. En sådan dokumentation bör därför göras först för att förvaltningen ska få en översyn över vilka verktyg och system som används i verksamheten. Utifrån förvaltningens uppdrag bedöms det vara särskilt allvarligt att en komplett systemdokumentation saknas inom verksamheten.

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.

Dataskyddsombudets kommentarer:

Sammantaget genererar verksamhetens svar ett resultat som innebär att risker är identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder. Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades

rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar på förvaltningen. Dock bedömer dataskyddsombudet att eftersom den generella kunskapen om dataskydd behöver ökas, finns det sannolikt även brister i kunskapen om de registrerades rättigheter. Särskilt viktig är frågan om registerutdrag där förvaltningen uppger att det saknas en rutin/process för att kunna hitta/få tillgång till efterfrågad information. Eftersom en begäran om registerutdrag ska hanteras inom 30 dagar är det särskilt viktigt att förvaltningen har en rutin som medarbetarna har tillgång till.

Utifrån skattningen bedömer dataskyddsombudet att verksamhetens arbete med hantering av registrerades rättigheter behöver prioriteras under 2023, och rekommenderar förvaltningen att som ett första steg ta fram en rutin för att hantera en begäran om registerutdrag.

2.5 Särskilda iakttagelser under året

2.5.1 Utredning av Intraservices personuppgiftsansvar i nya styrmodellen

Sedan GDPR trädde i kraft i maj 2018 har förvaltningen för Intraservice som huvudregel betraktats som personuppgiftsbiträde för de tjänster som levereras till övriga verksamheter i staden. Inför den nya styrmodellen rekommenderades förvaltningen att, tillsammans med stadsledningskontoret, utreda ansvarsförhållandena då dataskyddsombudet såg en risk i att denna ”huvudregel” var felaktig. Därtill bedömdes ett sådant arbete vara nödvändigt då någon faktisk utredning av ansvarsförhållandena inte tidigare gjorts inom staden.

Även om dataskyddsenheten under 2022 fortsatt att lyfta att frågan om personuppgiftsansvar behöver utredas i den nya styrmodellen har något initiativ till utredning ej tagits av ansvariga förvaltningar. I en skrivelse till kommunstyrelsen den 30 september 2022 med anledning av det återremitterande ärendet ”Göteborgs Stads plan för digitalisering 2022-2025” (dnr 0617/21) redogjordes för bakgrunden samt för de iakttagelser och risker som dataskyddsombudet identifierat. Att fördelningen av personuppgiftsansvaret och hanteringen av dessa frågor inom staden inte har fungerat under de senaste åren är en väl etablerad sanning och något som ständigt lyfts i informationssäkerhets- och dataskyddssammanhang. Avsaknaden av tydliga svar i ansvarsfrågan och brist på samordning är en källa till stor frustration inom stadens förvaltningar och bolag och medför risker för registrerade.

Då stadsledningskontoret under 2022 ej tagit något initiativ till en gemensam utredning rekommenderar dataskyddsombudet nu i stället förvaltningen för Intraservice att, tillsammans med övriga tjänsteleverantörer, utreda rådande ansvarsförhållanden för de personuppgiftsbehandlingar som ingår i tjänster såväl som den digitala infrastrukturen.

2.6 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en 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.

Utifrån identifierade risker rekommenderar dataskyddsombudet att förvaltningen under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation
  : Säkerställ att det finns en intern dataskyddsorganisation, med roller och ansvar är tydligt definierade, som kan arbeta praktiskt med dataskyddsfrågor.
- Kontrollpunkt 5: Övergripande strategi för dataskydd
  : Ta fram övergripande styrande principer (till exempel i form av en strategi) samt ett årshjul för det interna dataskyddsarbetet. Signalera från ledningsnivå att lagefterlevnad inte är valbart, utan ett krav för en hållbar digitalisering.
- Kontrollpunkt 4: Personuppgiftsregister
  : Se över och komplettera registret med de behandlingar som saknas för att uppfylla förvaltningens skyldighet att föra register över personuppgiftsbehandlingar enligt artikel 30 GDPR.

3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022