Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Fastighetskontoret

2022-12-23

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

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

dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i 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 biträdesavtal och andra överenskommelser 2022

Den fördjupade kontrollen har bestått av biträdesavtal och andra överenskommelser (kontrollpunkt tre). Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

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

- Fastighetskontoret bör utreda frågan om personuppgiftsansvar för samtliga personuppgiftsbehandlingar och teckna personuppgiftsbiträdesavtal eller överenskommelse om gemensamt personuppgiftsansvar för de behandlingar som ska regleras i enlighet med vad som anges i artikel 28 i GDPR.

- Förvaltningen bör ta fram skriftliga rutiner för samtliga delar av hanteringen av personuppgiftsbiträdesavtal och andra överenskommelser på dataskyddsområdet. Detta för att komma bort från sitt personberoende och kunna visa att verksamheten uppfyller ansvarsskyldigheten i artikel 5 i GDPR.

- Fastighetskontoret bör teckna ett personuppgiftsbiträdesavtal med Aaeron avseende Incit Expand som uppfyller kraven på ett personuppgiftsbiträdesavtal i enlighet med Artikel 28 i GDPR.

- Förvaltningen bör ta fram en rutin för att säkerställa att verksamheten kan kontrollera och följa upp nya underbiträden avseende biträdesrelationen med Securitas AB.

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 1 (2021): Hanteringen av personuppgiftsincidenter 2020.

Verksamheten gavs följande rekommendationer:

- Minska personberoendet genom att tydliggöra och konkretisera rutinen för incidenter så att fler inom förvaltningen har möjlighet och förutsättningar att hantera incidenter.
- Komplettera rutinen med instruktion/mall för hur incidenter ska dokumenteras.
- Komplettera rutinen med konkreta beskrivningar/instruktioner för hur en bedömning av risken för de registrerades fri- och rättigheter ska göras.
- Se över kunskapsnivån hos anställda och ta fram en plan för hur förvaltningen kan säkerställa att anställda hålls informerade.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit vissa åtgärder i enlighet med dataskyddsombudets rekommendationer. På grund av omorganisation och stor personalomsättning har dock inte samtliga åtgärder genomförts. Fastighetskontoret upphör vid årsskiftet och någon fortsatt uppföljning kommer därför inte att ske inom ramen för nuvarande organisation.

Kontroll 2 (2021): Positioneringsteknik (GPS)

Verksamheten gavs följande rekommendationer:

- Genomför kartläggning av personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer, och bedöm huruvida behandlingarna kan motiveras med hänvisning till nödvändighet och ändamål.
- Genomför konsekvensbedömningar för identifierade personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer.
- Säkerställ skriftlig information om behandlingen till anställda.

Och dataskyddsombudets kommentar:

Verksamheten har angett att de har vidtagit åtgärder i enlighet med lämnade rekommendationer. I svaren hänvisas till att förvaltningen tagit fram dokumentet ”Anvisning för körjournaler” som alla berörda särskilt får ta del av. Dokumentet innehåller information om alla de rutiner som fastighetskontoret har kring körjournaler som även inkluderar positioneringsteknik, inklusive stickprov.

Dataskyddsombudets bedömning är att den framtagna anvisningen, även om det är positivt att förvaltningen tagit fram den, inte i sig utgör en åtgärd enligt rekommendationerna. De rekommendationer som lämnades i den fördjupade kontrollen kvarstår därför, och förvaltningen rekommenderas därtill kontrollera huruvida behandlingen i form av ”stickprovskontroller” är förenlig med GDPR.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder vissa åtgärder i enlighet med dataskyddsombudets rekommendationer. På grund av omorganisation och stor personalomsättning har dock inte samtliga åtgärder genomförts. Fastighetskontoret upphör vid årsskiftet och någon fortsatt uppföljning kommer därför inte att ske inom ramen för nuvarande organisation.

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 Fastighetskontorets 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 verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

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

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:

Fastighetskontoret har kunskaps- och kompetensmässigt goda förutsättningar för att bedriva dataskyddsarbete. Det finns väletablerade rapporteringsvägar och fastställda roller. De brister som förvaltningen själva uppger handlar främst om bristen på integrering av dataskydd i förvaltningens dagliga arbete, samt otillräckliga resurser. Verksamheten har under året haft stor omsättning/nyrekrytering av personal vilket är en bidragande orsak. Dataskyddsombudets rekommendation är att den interna dataskyddsorganisationen tillförs tillräckliga resurser för att kunna bedriva ett systematiskt dataskyddsarbete. Förvaltningen behöver också utreda hur och verka för att de olika verksamhetsdelarna i högre utsträckning involveras i dataskyddsarbetet, för att säkerställa att dataskyddsorganisationen representeras av och når ut till samtliga delar.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Skattningen indikerar att det inte föreligger några höga risker inom kontrollpunkten Fastighetskontorets svar visar på att verksamheten har rutiner och arbetssätt på plats för att hantera personuppgiftsincidenter. Dataskyddsombudet gör ingen annan bedömning än verksamheten, men är av uppfattningen att förvaltningen behöver fortsätta arbeta med frågan genom kontinuerliga kunskapshöjande insatser hos medarbetarna.

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:

Kontrollpunkten är föremål för årets fördjupade kontroll. Med utgångspunkt i det som framkommit under den fördjupade kontrollen gör dataskyddsombudet en delvis annan bedömning av kontrollpunkten än den som förvaltningen själv har gjort. Fastighetskontoret rekommenderas därför att utreda frågan om personuppgiftsansvar för samtliga personuppgiftsbehandlingar och teckna personuppgiftsbiträdesavtal eller överenskommelse om gemensamt personuppgiftsansvar för de behandlingar som ska regleras i enlighet med vad som anges i artikel 28 i GDPR.

Förvaltningen rekommenderas också att ta fram skriftliga rutiner för samtliga delar av hanteringen av personuppgiftsbiträdesavtal och andra överenskommelser på dataskyddsområdet. Detta för att komma bort från sitt personberoende och kunna visa att verksamheten uppfyller ansvarsskyldigheten enligt artikel 5 i GDPR. För rekommendationer i sin helhet hänvisas till bilaga 2.

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 ingen anledning att göra en annan bedömning än den som förvaltningen gjort.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Dataskyddsombudet anser att förvaltningens skattning blir delvis missvisande. Flera av de delar som krävs för en övergripande strategi för dataskydd, i form av rutiner och styrande dokument, finns visserligen finns på plats. God kompetens finns också inom dataskyddsorganisationen. Däremot anser dataskyddsombudet att det saknas en tydlig och dokumenterad styrning.

Detta framgår också av förvaltningens egen skattning där verksamheten anger sig sakna en övergripande strategi och ett systematiskt arbetssätt för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet. Dataskyddsombudet ifrågasätter också delvis fastighetskontorets skattning om att förvaltningen arbetar riskbaserat. Utifrån detta rekommenderas fastighetskontoret att i dokumenterade handlings- och/eller verksamhetsplan, rutiner och policys tydliggöra sin strategi för det övergripande dataskyddsarbetet.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet har ingen anledning att göra en annan bedömning än förvaltningen. Fastighetskontoret rekommenderas likväl att genomföra regelbundna informationsinsatser för att utbilda och informera medarbete inom dataskydd, med syftet att höja/bibehålla den allmänna kunskapsnivån.

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:

Dataskyddsombudet delar inte fullt ut fastighetskontorets bedömning för kontrollpunkten, utan anser att integritetspolicyn behöver uppdateras och kompletteras då nuvarande integritetspolicy saknar information om hur de registrerades personuppgifter hanteras vid kontakt med myndigheten, till exempel vid frågor, samt information om att inlämnade uppgifter som regel utgör en allmän handling och därmed kan komma att behandlas utifrån dessa ändamål.

Fastighetskontoret rekommenderas därför vidta åtgärder för att säkerställa att policyn uppfyller kraven på information, samt att informationen är lättillgänglig oavsett i vilken digital kanal som den registrerades personuppgifter behandlas.

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 svar indikerar att befintlig dokumenthanteringsplan behöver uppdateras och rutiner för gallring behöver tas fram. Med tanke på att fastighetskontoret upphör vid årsskiftet är detta något som dataskyddsombudet anser bör prioriteras i den nya organisationen. Verksamheten rekommenderas också utföra kontroller i system och lagringsytor som innehåller personuppgifter och kontrollera att dessa gallras i enlighet med vad som anges i dokumenthanteringsplanen.

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:

Dataskyddsombudet har under året inte rådfrågats i någon konsekvensbedömning som förvaltningen arbetat med.

Dataskyddsombudet vill i sammanhanget betona att det inte är enbart för nya former av behandlingar som förvaltningen behöver göra konsekvensbedömningar, utan att det även behöver genomföras konsekvensbedömningar för riskfyllda befintliga behandlingar som redan är påbörjade Det är även av vikt att förvaltningen har rutiner för att följa upp identifierade risker.

Dataskyddsombudet delar inte heller uppfattningen att samtliga verksamhetens behandlingar med höga risker för de registrerade skulle ha konsekvensbedömts, till exempel framgår det av dataskyddsombudets uppföljning av tidigare års fördjupade kontroll att någon bedömning avseende GPS positionering inte har genomförts.

Verksamheten har även andra behandlingar kopplade bland annat till O365-miljön som inte konsekvensbedömts. Dataskyddsombudet delar därför inte verksamhetens bedömning och rekommenderar förvaltningen att utreda huruvida förvaltningen verkligen utför konsekvensbedömningar för samtliga behandlingar med höga risker.

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 på denna punkt skattat sin organisation och sina rutiner högt. Dataskyddsombudet har under det gångna året inte involverats i någon upphandling som förvaltningen själva har hanterat. Däremot har dataskyddsombudet involverats indirekt via IT-säkerhetsfunktionen på Intraservice när en del av fastighetskontorets verksamhet avsåg att upphandla/utveckla sitt användande av tjänsten/verktyget MMD. Dataskyddsombudets observation från det enda möte som hölls i frågan är att förvaltningens rutiner inte verkar ha följts i någon del utan att frågan initierats helt utan involvering av förvaltningens dataskyddskompetens eller dataskyddsombudet och att det var mer av en slump som dataskyddsombudet blev involverad i en behandling med stora potentiella risker för de registrerades friheter och rättigheter.

Det ger sammantaget fog för dataskyddsombudet att ifrågasätta förvaltningens egen skattning av kontrollpunkten. Rekommendationen till verksamheten är därför att i första hand se över behovet av informationsinsatser så att de rutiner som finns på området efterlevs.

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:

Förvaltningens skattning skiljer sig i flera delar väsentligt ifrån tidigare års och dataskyddsombudets bedömning är att den nu är mer realistisk. Verksamheten rekommenderas att framför allt utreda användningen av cookies, så att användningen av dessa på till exempel stadsutvecklingswebben (vars redaktion är placerad på fastighetskontoret) följer kraven enligt GDPR. Verksamheten behöver också ta fram rutiner för införande och användande av kostnadsfria tjänster som gratisappar och sociala medier.

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 anser förvaltningen, utifrån skattningen, att verksamheten har goda förutsättningar för att hantera de registrerades rättigheter. Dataskyddsombudet har inte blivit tillfrågad angående någon begäran från registrerade rörande deras möjlighet att utöva sina rättigheter och har inte heller några indikationer som tyder på att skattningen skulle vara missvisande eller felaktig.

2.5 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/bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation
  Fastighetskontoret rekommenderas tillse att den interna dataskyddsorganisationen tillförs tillräckliga resurser för att kunna bedriva ett systematiskt dataskyddsarbete

- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser
  Fastighetskontoret rekommenderas att utreda frågan om personuppgiftsansvar för samtliga personuppgiftsbehandlingar och teckna personuppgiftsbiträdesavtal eller överenskommelse om gemensamt personuppgiftsansvar för de behandlingar som ska regleras, i enlighet med vad som anges i artikel 28 i GDPR.

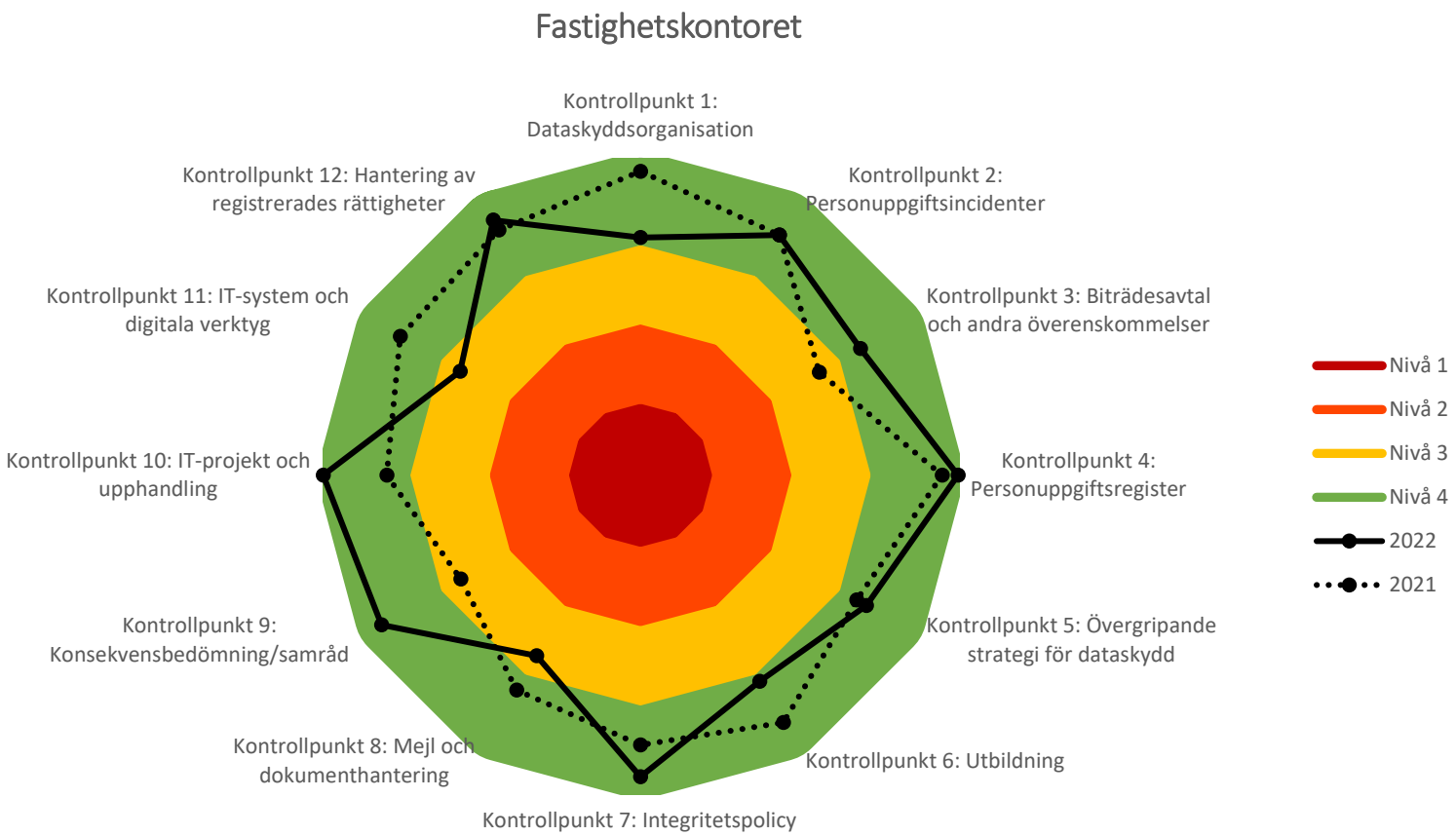
- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Förvaltningen rekommenderas kartlägga sina behandlingar med höga risker och genomföra konsekvensbedömningar i enlighet med artikel 35 i GDPR.

3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022

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



Fördjupad kontroll: Fastighetskontoret

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Bakgrund

Den fördjupade kontrollen av biträdesavtal och andra överenskommelser syftar till att kontrollera om organisationen uppfyller kraven i artikel 28.3 i dataskydds-förordningen (GDPR), om att relationen mellan personuppgiftsansvarig (PUA) och personuppgiftsbiträde (PUB) ska regleras skriftligen. Kontrollen har genomförts i två delar, del ett har bestått av ett antal frågor som besvarats av organisationen och del två har bestått av att dataskyddsombudet slumpvis valt ut tre avtal, som organisationen har tecknat, för att kontrollera om dessa uppfyller kraven i GDPR.

Iakttagelser från kontrollen

Den som är personuppgiftsansvarig ansvarar för att personuppgifter hanteras korrekt i alla led. Ansvaret gäller även om man anlitar underleverantörer. För att ha full kontroll över personuppgifterna krävs att ansvarsförhållandena regleras, vanligtvis genom att det upprättas ett personuppgiftsbiträdesavtal. Även andra ansvarsrelationer inom dataskyddsområdet kan behöva regleras i ett avtal eller överenskommelse. Till exempel kan ett gemensamt personuppgiftsansvar regleras genom ett datadelningsavtal, som ett sätt att uppfylla kraven i GDPR.

Rättslig reglering och vägledning

Det framgår av artikel 28 i GDPR att när uppgifter behandlas av ett personuppgiftsbiträde för den personuppgiftsansvariges räkning så ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller nationell rätt som är bindande för biträdet. Detta innebär att förhållandet inte nödvändigtvis behöver regleras i ett biträdesavtal, även om det i praktiken är det allra vanligaste. Oavsett hur man väljer att göra, så ska det av detta avtal eller rättsakt alltid framgå vad som är föremål för personuppgiftsbehandlingen, dess varaktighet, art och ändamål, vilken typ av personuppgifter som behandlas och vilka kategorier av registrerade som förekommer. Avtalet ska vara skriftligt och personuppgiftsbiträdet får endast behandla uppgifter på dokumenterade instruktioner från den personuppgiftsansvarige. Även formerna för ett gemensamt personuppgiftsansvar behöver regleras för den skull att en sådan situation uppstår. I artikel 26 i GDPR anges att de personuppgiftsansvarigas respektive ansvar ska fastställas genom ett inbördes arrangemang. Vanligtvis uppfylls detta krav genom att de personuppgiftsansvariga tecknar ett datadelningsavtal.

Dataskyddsombudets iakttagelser kommentarer och rekommendationer från kontrollen

Personuppgiftsbiträden

Fastighetskontoret uppger sig ha tecknat avtal med samtliga personuppgiftsbiträden som förvaltningen anlitar, med undantag för Intraservice. Fastighetskontoret uppger att i flera fall där Intraservice behandlar personuppgifter så saknas möjlighet att bestämma över ändamålet och medlen för behandlingen varför det inte är klarlagt att fastighetskontoret är personuppgiftsansvarig för alla dessa behandlingar. För flera behandlingar som dataskyddsombudet vet förekommer i form av kommungemensamma interna tjänster saknas uppgift om biträdesavtal. Detta är relaterat till det förvaltningen uppger angående svårigheten med att klarlägga huruvida man är personuppgiftsansvarig eller inte för sådana behandlingar.

Dataskyddsombudets utgångspunkt är dock att för samtliga personuppgiftsbehandlingar där förvaltningen i varje fall delvis bestämmer över sina egna ändamål och medel så är fastighetskontoret antingen ensamt eller delat personuppgiftsansvarig för dessa och i den mån Intraservice (eller annan aktör) behandlar personuppgifter för förvaltningens räkning så ska detta regleras i ett personuppgiftsbiträdesavtal. Är ansvaret delat ska det regleras i ett datadelningsavtal. I det fall ansvarsfördelningen är oklar bör fastighetskontoret, gärna i samarbete med andra förvaltningar, verka för att ansvarsfrågan inom Staden utreds, så att det står klart hur personuppgiftsansvaret ska regleras.

Biträdesavtal och instruktioner

Förvaltningen uppger att instruktioner har lämnats till samtliga biträden i enlighet med det standardiserade personuppgiftsbiträdesavtal (PUB-avtal) som används inom Göteborgs Stad. Vid inledandet av en ny personuppgiftsbehandling ska detta registreras i förvaltningens personuppgiftsbehandlingsregister och där ska det också anges huruvida behandlingen innebär att det krävs ett PUB-avtal. Förvaltningen verkar dock sakna en skriftlig rutin för att avgöra huruvida en behandling kräver att ett biträdesavtal tecknas och också hur detta ska ske rent praktiskt. Dataskyddsombudets rekommendation är att förvaltningen fastställer detta i en skriftlig och officiell rutin.

Kontroll och uppföljning

Fastighetskontoret uppger att det saknas rutiner för att följa upp de garantier som personuppgiftsbiträden lämnat avseende tekniska och organisatoriska åtgärder, detta motiverar förvaltningen med att enbart etablerade tjänsteleverantörer anlitas och att verksamheten ännu inte upplevt att ett behov av rutiner för uppföljning har funnits. Även om dataskyddsombudet kan ha en viss förståelse för synsättet så kvarstår faktum att den personuppgiftsansvarige har ett ansvar för att säkerställa att personuppgifter som

behandlas för dennes räkning hanteras på ett sätt som är förenligt med dataskyddsförordningen och som tillvaratar de registrerades rättigheter. För att kunna göra detta krävs det att rutiner finns på plats avseende hur den personuppgiftsansvarige ska kunna följa upp detta och med vilka tidsintervall som det ska ske. Dataskyddsombudets rekommendation är därför att Fastighetskontoret tar fram sådana rutiner.

Vad gäller avtalsuppföljning så saknas det också här skriftliga rutiner. Även om det inte varit aktuellt med några avslutade eller upphörande tjänster så är det viktigt att det finns en fastställd ordning som på förhand talar om hur frågan ska hanteras. En sådan hantering bör inte vara personbunden utan finnas dokumenterad i en skriftlig rutin. Dataskyddsombudet vill särskilt poängtera att avsaknaden av skriftliga rutiner i sig inte behöver betyda att verksamhetens hantering är dålig eller otillräcklig. En väsentlig del av personuppgiftsansvaret enligt GDPR består dock av att kunna visa att man följer förordningen och även hur man gör detta, den så kallade ansvarsskyldigheten.

Avsaknaden av skriftliga rutiner är också många gånger ett tecken på att en dataskyddsorganisation är personbunden. Dataskyddsombudets uppfattning är att fastighetskontoret har kompetenta personer som arbetar med dataskyddsfrågorna, men att förvaltningen bör minska personberoendet då det innebär en sårbarhet. Ett viktigt led i detta är fastställandet av skriftliga rutiner för hur arbetet med dataskyddsfrågor ska bedrivas, till exempel då det handlar om uppföljning och kontroll av biträdesavtal. Fastighetskontoret rekommenderas därför att ta fram sådana rutiner.

Själva tecknandet av avtal regleras i förvaltningens delegationsordning och dataskyddsombudet har inga synpunkter på den ordningen. Varje medarbetare får anses vara införstådd med att man som anställd bara har rätt att agera i enlighet med den delegationsordning som är fastställd.

Sammanfattningsvis kan konstateras att förvaltningen arbetar löpande med hanteringen kring personuppgiftsbiträdesavtal men att den skulle behöva formaliseras i skriftliga rutiner för att komma ifrån beroendet av några få kunniga nyckelpersoner.

Granskning av avtal

Som en andra del i den fördjupade kontrollen har Dataskyddsombudet också granskat tre slumpmässigt utvalda personuppgiftsbiträdesavtal som förvaltningen tecknat med leverantörer. Vad gäller fastighetskontorets avtal med Securitas så har dataskyddsombudet ett antal synpunkter. I avtalet framkommer att biträdet har rätt att anlita underbiträden, det anges visserligen att PUA ska informeras och har rätt att invända, men det är inte helt tydligt hur den processen ser ut. I avtalet förefaller det som att den enda information som lämnas av Securitas är att ändringen annonseras på en särskilt dedikerad hemsida. Vid tillämpandet av ett sådant förfaringssätt är det av stor vikt att förvaltningen har rutiner för att kontinuerligt kontrollera och följa upp de underbiträden som redovisas på hemsidan så att man kan göra invändningar mot underbiträden som inte uppfyller de krav som förvaltningen ställer. Det är också tydligt att den personuppgiftsansvariges instruktion till biträdet är framtagen av biträdet

(Securitas), det centrala är naturligtvis instruktionens innehåll. Men med tanke på att en bilagd instruktion är riktad från PUA till PUB så är det viktigt att det är den personuppgiftsansvariges instruktioner till biträdet och att det inte finns några oklarheter om det förhållandet. Förvaltningen rekommenderas därför att ta fram en rutin för att kontinuerligt kunna följa upp och kontrollera de underbiträden som anlitas av Securitas.

Vad gäller avtalet med Aareon avseende fastighetssystemet Incit expand så är det minst sagt knapphändigt, faktum är att det är tveksamt om man kan kalla det för avtal då det egentligen bara innehåller en instruktion, samt en allmän kommentar om GDPR ifrån Almega. I instruktionen som är framtagen av biträdet framgår inte heller var någonstans personuppgifterna behandlas eller vilka underbiträden som anlitas av biträdet. I instruktionen hänvisas i stället till ”bilaga biträdesavtal” på Aareons hemsida. Denna bilaga är dock inte möjlig att ni via hemsidan utan i stället behövs inloggning till Aareons supporttjänst. Företagets information om GDPR är högst rudimentär och förefaller inte ha uppdaterats sedan 2018. Dataskyddsombudets uppfattning är att det dokument som finns på plats inte uppfyller de krav på ett biträdesavtal som GDPR ställer. Dataskyddsombudets rekommendation är därför att fastighetskontoret tecknar ett avtal med Aaeron som uppfyller kraven i GDPR, med en adekvat instruktion.

Dataskyddsombudet har slutligen granskat fastighetskontorets personuppgiftsträdesavtal med Antura, avtalet är visserligen knapphändigt, men uppfyller ändå enligt dataskyddsombudets mening kraven på vad ett personuppgiftsbiträdesavtal ska innehålla. Dataskyddsombudet har inga övriga synpunkter.

Sammanfattande rekommendationer

- Fastighetskontoret bör utreda frågan om personuppgiftsansvar för samtliga personuppgiftsbehandlingar och teckna personuppgiftsbiträdesavtal eller överenskommelse om gemensamt personuppgiftsansvar för de behandlingar som ska regleras i enlighet med vad som anges i artikel 28 i GDPR.

- Förvaltningen bör ta fram skriftliga rutiner för samtliga delar av hanteringen av personuppgiftsbiträdesavtal och andra överenskommelser på dataskyddsområdet. Detta för att komma bort från sitt personberoende och kunna visa att verksamheten uppfyller ansvarsskyldigheten i artikel 5 i GDPR.

- Fastighetskontoret bör teckna ett personuppgiftsbiträdesavtal med Aaeron avseende Incit Expand som uppfyller kraven på ett personuppgiftsbiträdesavtal i enlighet med Artikel 28 i GDPR.

- Förvaltningen bör ta fram en rutin för att säkerställa att verksamheten kan kontrollera och följa upp nya underbiträden avseende biträdesrelationen med Securitas AB

Bilagor

1. Information om fördjupad kontroll 2022
2. Fördjupad kontroll 2022 Biträdesavtal och andra överenskommelser (del 1)

Bilaga 1

Fördjupad kontroll: Fastighetskontoret

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.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att svara på ett antal frågor kopplade till er hantering av Biträdesavtal och andra överenskommelser.
I del två kommer dataskyddsombudet att genomföra en stickprovskontroll genom att begära 3 slumpmässigt utvalda biträdesavtal ifrån ert PU- register.

Bilaga 2

Fördjupad kontroll 2022 - Biträdesavtal

Del 1

Hej! Vänligen besvara frågorna så utförligt och detaljerat som möjligt. Bifoga även relevanta dokument, underlag och aktuella rutiner som ni har tagit fram. Svaren skall ha inkommit till dataskyddsombudet senast den 7 mars 2022.
Har du frågor, kontakta ditt Dataskyddsombud.

1. Ange/bifoga lista över vilka ni har identifierat som personuppgiftsbiträden. **A)** Ange för vilka personuppgiftsbiträden som det finns personuppgiftsbiträdesavtal. **B)** Har ni gett instruktioner till de personuppgiftsbiträden som ni har avtal med, enligt art. 28.3 a dataskyddsförordningen? För det fall att ni tecknat biträdesavtal, men ej gett instruktioner, ange detta.

2. Finns det rutiner för bedömningen av om en leverantör eller annan motpart ska anses vara personuppgiftsbiträde? **A)** Om ja, bifogarutinen/rutinerna. **B)** Om nej, ange hur ni går till väga för att annars göra den bedömningen.

3. Finns det rutiner för att säkerställa och följa upp att personuppgiftsbiträden uppfyller de garantier som de har lämnat avseende tekniska och organisatoriska åtgärder? **A)** Om ja, bifoga rutinen/rutinerna. **B)** Om nej, ange hur ni annars går till väga för att göra den bedömningen.

4. Finns det rutiner för regelbunden avtalsuppföljning (t.ex. om tjänsten ändras eller avslutas) för personuppgiftsbiträdesavtalen? **A)** Om ja, bifoga rutinen/rutinerna. **B)** Om nej, ange hur ni säkerställer att era personuppgiftsbiträdesavtal är aktuella och uppdaterade?

5. Ange hur ni säkerställer att tecknande av personuppgiftsbiträdesavtal sker i behörig ordning.

6. Ange/bifoga lista över vilka övriga överenskommelser ni ingått, till exempel avseende gemensamt/delat personuppgiftsansvar.

7. Finns det rutiner för bedömningen om när ni behöver upprätta en överenskommelse om delat/gemensamt personuppgiftsansvar? **A)** Om ja, bifogarutinen/rutinerna. **B)** Om nej, ange hur ni går till väga för att annars göra den bedömningen.