Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Stadsbyggnadskontoret

2022-12-20

Innehåll

1 Dataskydd i kommunal verksamhet 3

1.1 Göteborgs Stads dataskyddsombud 3

2 Granskning av dataskyddsarbetet 2022 4

2.1 Dataskyddsombudets kontrollfunktion 4

2.2 Fördjupad kontroll 4

2.2.1 Kontroll av biträdesavtal och andra överenskommelser 2022 4

2.2.2 Uppföljning av tidigare genomförda kontroller 5

2.3 Årlig kontroll av dataskyddsarbetet 6

2.3.1 Metod och risknivåer 6

2.4 Stadsbyggnadskontorets dataskyddsarbete 2022 6

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation 7

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter 7

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser . 8

2.4.4 Kontrollpunkt 4: Personuppgiftsregister 8

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd 8

2.4.6 Kontrollpunkt 6: Utbildning 9

2.4.7 Kontrollpunkt 7: Integritetspolicy 9

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering 10

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd 10

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling 11

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg 11

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter 12

2.5 Sammanfattande rekommendationer 12

3 Bilagor 13

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 därför lämnat ett antal rekommendationer till verksamheten att vidta åtgärder.

- Förvaltningen bör snarast teckna personuppgiftsbiträdesavtal i samtliga fall där verksamheten bedömer att en biträdessituation föreligger.

- 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 man uppfyller ansvarsskyldigheten i artikel 5 i GDPR.

- För de fall som biträdesavtal finns men instruktion saknas bör Stadsbyggnadskontoret snarast utfärda skriftliga instruktioner till biträdet.

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 2 (2021): Positioneringsteknik (GPS).

Verksamheten gavs följande rekommendationer:

- Stadsbyggnadskontoret rekommenderas kartlägga sina behandlingar där positioneringsteknik används och/eller förekommer.
- Samt därefter, i aktuella fall, genomföra konsekvensbedömningar för dessa behandlingar.

Och följande kompletterande rekommendationer

- Genomför konsekvensbedömningar för identifierade personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer.
- Ta fram rutiner för användningen av positioneringsteknik inom förvaltningen.
- Ta fram skriftlig information om behandlingen till anställda.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Förvaltningen uppger att på grund av en pressad arbetssituation till följd av den omorganisation som stadsbyggnadskontoret är en del av har andra prioriteringar behövt göras. Stadsbyggnadskontoret 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 Stadsbyggnadskontorets 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:

Dataskyddsombudet delar verksamhetens bedömning. Det finns visserligen fortfarande ett personberoende och mycket vilar på förvaltningens dataskyddskontakt. Dataskyddsombudets bedömning är ändå att förvaltningen arbetat aktivt med frågan och har en betydligt mer robust dataskyddsorganisation nu jämfört med förra året. Förvaltningen involverar fler delar av verksamheten i arbetet och har vidtagit åtgärder för att aktivt få med hela organisationen i dataskyddsfrågorna. Dataskyddsombudet har ingen annan rekommendation än att förvaltningen ska fortsätta på den positiva inslagna vägen och säkerställa att dataskyddsorganisationen tillförs tillräckliga resurser.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet gör i allt väsentligt samma bedömning för denna kontrollpunkt som i 2021 års rapport. Skattningen indikerar visserligen att det inte föreligger några höga risker och dataskyddsombudet delar den bedömningen. Samtidigt har förvaltningen, i jämförelse med andra verksamheter inom Göteborgs Stad få personuppgiftsincidenter, vilket kan vara ett tecken på att kunskapen hos anställda behöver öka, det kan naturligtvis också vara ett tecken på ett mycket väl fungerande arbete, oavsett detta så rekommenderas förvaltningen att fortsätta arbeta med att stärka medarbetarnas kunskaper om personuppgiftincidenter och hur de ska hanteras. Förvaltningen har, som sagt var, få rapporterade incidenter, men det är likväl viktigt att verksamheten arbetar systematiskt med att följa upp de incidenter som inträffar.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Dataskyddsombudets kommentarer:

Stadsbyggnadskontorets svar visar att det finns omfattande risker som behöver åtgärdas omgående. Kontrollpunkten har även varit föremål för dataskyddsombudets fördjupade kontroll (se bilaga 2), inom ramen för denna har förvaltningen rekommenderats att snarast teckna personuppgiftsbiträdesavtal i samtliga fall där verksamheten bedömer att en biträdessituation föreligger, ta fram skriftliga rutiner för samtliga delar av hanteringen av personuppgiftsbiträdesavtal och andra överenskommelser på dataskyddsområdet, bland annat efterlevnadskontroller av biträden, samt utfärda instruktioner till biträden för de fall att det saknas.

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. Men för att Stadsbyggnadskontoret ska kunna bibehålla sin goda status är det viktigt att verksamheten fortsätter att arbeta aktivt med sitt personuppgiftsregister.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Denna kontrollpunkt knyter an till kontrollpunkt 1 – dataskyddsorganisation. Dataskyddsombudets uppfattning är att förvaltningen kontinuerligt och aktivt arbetat med sin övergripande strategi och att man successivt höjer nivån. Det förbättringsområde som kvarstår handlar om förekomsten av interna kontroller för att säkerställa efterlevnaden av GDPR. Dataskyddsombudets rekommendation är därför att förvaltningen under 2023 mer aktivt börjar arbeta med sådana kontroller där det bedöms lämpligt.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet gör ingen annan bedömning än förvaltningen avseende skattningen för kontrollpunkten, men förvaltningen rekommenderas fortsätta med kontinuerliga utbildningsinsatser och att ta fram rutiner för att kunna följa upp och bibehålla kunskapsnivån hos de medarbetare som genomgått utbildning.

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 instämmer i stort i förvaltningens bedömning, men noterar att nuvarande integritetspolicy saknar information om till exempel användningen av cookies, eller att sådant som skickas in till förvaltningen blir allmänna handlingar och därmed kan komma att behandlas utifrån särskilda ändamål knutna till detta. Stadsbyggnadskontoret rekommenderas därför säkerställa att policyn uppdateras så att den uppfyller kraven på information enligt GDPR.

Då stadsbyggnadskontoret angett att policyn inte är nåbar från samtliga digitala kanaler rekommenderas förvaltningen även vidta åtgärder för att göra informationen 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:

Dataskyddsombudet delar förvaltningens bedömning och är av uppfattningen att Stadsbyggnadskontoret har en mycket hög kompetensnivå inom området i form av sin dataskyddskontakt och andra medarbetare. Förvaltningen har väl utarbetade dokument, riktlinjer och rutiner för samtliga delar som omfattas av kontrollpunkten.

Förvaltningen rekommenderas dock att i likhet med förra året följa upp och kontrollera så att utförandet av den faktiska gallringen, systemen och på lagringsytor, genomförs i enlighet med vad som anges i verksamhetens dokumenthanteringsplan.

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:

Förvaltningens svar visar på stora risker som kräver omgående åtgärder. Svaren visar på ett stort behov av att säkerställa att en bedömning av risk har genomförts för samtliga av förvaltningens personuppgiftsbehandlingar.

Dataskyddsombudets bedömning är att kompetensen att systematiskt arbeta riskbaserat och med konsekvensbedömningar finns på förvaltningen, men att arbetet har släpat efter och att det saknas nödvändiga rutiner. Stadsbyggnadskontoret rekommenderas därför att framgent prioritera detta arbete och att i första hand kartlägga sina behandlingar och därefter påbörja ett arbete med att genomföra konsekvensbedömningar för samtliga behandlingar med höga risker.

Verksamheten behöver också i detalj ta fram nödvändiga rutiner på området för att identifiera personuppgiftsbehandlingar med höga risker, säkerställa att en bedömning genomförts innan en behandling med höga risker inleds, inhämta dataskyddsombudets synpunkter, rutiner för genomförande av

konsekvensbedömning och för att hålla en genomförd bedömning uppdaterad. Verksamheten behöver också rutiner för beslut om riskacceptans och inhämtandet av de registrerades synpunkter.

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. Om detta beror på att inga upphandlingar på detta område har skett under året är oklart, men utifrån detta kan dataskyddsombudet inte göra någon annan bedömning än förvaltningens egen i frågan.

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:

Dataskyddsombudets rekommendation är snarlik den som lämnades i 2021 års rapport. Det vill säga att oaktat förvaltningens skattning så är dataskyddsombudet av uppfattningen att det föreligger en risk för att stadsbyggnadskontoret använder tjänster som av olika skäl saknar tillräcklig säkerhet vad gäller dataskydd. Denna bedömning grundar sig bland annat i det faktum att konsekvensbedömningar saknas för majoriteten av verksamhetens personuppgiftsbehandlingar. Stadsbyggnadskontoret rekommenderas därför att kartlägga alla de IT-system och digitala verktyg som används inom förvaltningen och kontrollera dess följsamhet mot GDPR.

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:

Dataskyddsombudet har inte blivit kontaktad av någon registrerad under året och har inte heller någon anledning att ifrågasätta förvaltningen egen skattning av kontrollpunkten. Med det sagt så behöver arbetet med att informera anställda och hålla en hög kunskapsnivå inom organisationen, om de registrerades rättigheter, bedrivas som ett kontinuerligt pågående arbete. Förvaltningen rekommenderas därför att löpande arbeta för att säkerställa att medarbetare på samtliga nivåer inom verksamheten har tillräckliga kunskaper om de registrerades rättigheter.

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 3: Biträdesavtal
  Teckna personuppgiftsbiträdesavtal i samtliga fall där verksamheten bedömer att en biträdessituation föreligger

  Ta fram skriftliga rutiner för samtliga delar av hanteringen av personuppgiftsbiträdesavtal och andra överenskommelser på dataskyddsområdet.

- Kontrollpunkt 9: Konsekvensbedömning samråd
  Kartlägga och påbörja arbetet med att genomföra konsekvensbedömningar för samtliga behandlingar med höga risker.

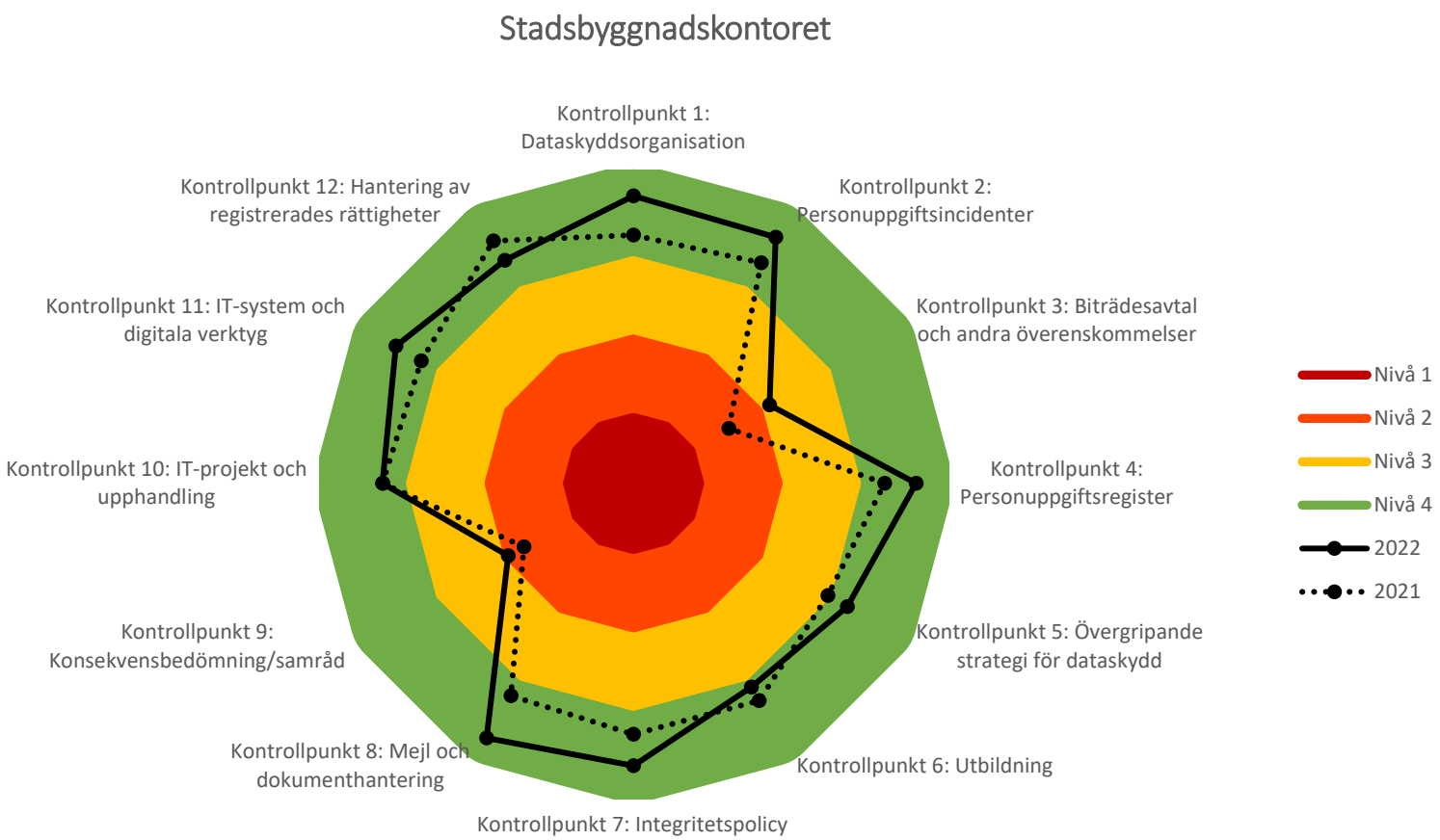
  Ta fram nödvändiga rutiner för samtliga delar av konsekvensbedömningsområdet.

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: Stadsbyggnadskontoret

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

Stadsbyggnadskontoret har i sitt svar till dataskyddsombudet bifogat en förteckning där det framgår att förvaltningen tecknat biträdesavtal med 12 personuppgiftsbiträden, för dessa saknas instruktioner i tre av fallen. Förvaltningen uppger samtidigt att det saknas avtal i ytterligare 12 fall där man har bedömt att en biträdessituation eventuellt föreligger. Dataskyddsombudet noterar utöver detta att det förefaller saknas ett antal leverantörer i listan över biträden. Avsaknaden av dessa kan dock bero på otydligheter i Stadens styrmodell, angående vem som egentligen ska teckna biträdesavtal då de rör kommungemensamma interna tjänster. För de fall där biträdesavtal saknas, eller biträdesrelationen är oklar, rekommenderas Stadsbyggnadskontoret att så snart som möjligt utreda huruvida biträdesavtal ska tecknas och att därefter tillse att avtal upprättas i samtliga fall där man bedömer att en biträdesrelation föreligger.

Biträdesavtal och instruktioner

I de fall avtal finns, men där instruktion saknas, så bör förvaltningen snarast upprätta instruktioner för biträdet. I enlighet med vad som anges i artikel 28 i GDPR ska en personuppgiftsansvarig ge tydliga instruktioner till ett underbiträde angående vilka personuppgifter som får hanteras och på vilket sätt detta ska ske

Förvaltningen saknar skriftliga instruktioner för bedömningen av om en leverantör eller annan motpart ska anses vara personuppgiftsbiträde, men uppger att det finns ett arbetssätt där bedömningen om en leverantör, eller annan motpart, ska anses vara personuppgiftsbiträde görs av IT-chef, jurist, dataskyddskontakt och handläggare i samband med införskaffandet av och/eller förnyelse av tjänst eller licens. Dataskyddsombudets bedömning utefter de observationer som gjorts under året är att detta inte alltid verkar fungera i praktiken utan att exempelvis licensavtal kan upprättas utan att frågan om biträdesavtal har utretts. Rekommendationen till Stadsbyggnadskontoret är att man tar fram skriftliga rutiner och kommunicerar ut dessa i den egna organisationen. Det behöver inte handla om omfattande rutindokument med luftiga skrivningar, men det behöver vara tydligt i upphandlingsprocessen att frågan om biträdesrelation beaktas och att det är tydligt vem som verksamheten kan och ska kontakta för stöd och vägledning.

Kontroll och uppföljning

Vad gäller rutiner för att säkerställa och följa upp att personuppgiftsbiträden uppfyller de garantier som de har lämnat avseende tekniska och organisatoriska åtgärder så anger förvaltningen även här att skriftliga rutiner saknas men att Stadsbyggnadskontoret

förutsätter att avtalsparterna är seriösa i sina åtaganden. Beroende på tjänstens beskaffenhet förs också löpande diskussioner avseende tekniska och organisatoriska åtgärder i samband med avtalsförnyelse. 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 GDPR och som tillvaratar de registrerades rättigheter. För att kunna göra detta krävs att rutiner/arbetssätt finns på plats avseende hur den personuppgiftsansvarige ska kunna följa upp att personuppgifter som behandlas för dennes räkning hanteras på ett korrekt sätt och med vilka tidsintervall detta ska göras.

Verksamheten bör också ha i åtanke att det inte räcker med att följa GDPR, förvaltningen ska också kunna visa att man följer den. En avsaknad av dokumentation och skriftliga rutiner gör att det i praktiken blir omöjligt att visa på vilket sätt som Stadsbyggnadskontoret faktiskt följer GDPR. Dataskyddsombudets rekommendation är därför att Stadsbyggnadskontoret tar fram sådana rutiner och att man aktivt arbetar med uppföljning gentemot sina leverantörer.

Inte heller för avtalsuppföljning finns några skriftliga rutiner. Förvaltningen uppger förvisso att kontroll görs gentemot avtalsdatabasen där samtliga avtal inklusive personuppgiftsbiträdesavtalen finns samlade. Ändras förutsättningarna för en tjänst eller om något avgörande inträffar i omvärlden kontrolleras relaterade avtal inklusive personuppgiftsbiträdesavtalet. De flesta biträdesavtalen är dock så pass nya att ingen uppföljning varit aktuell ännu. Dataskyddsombudets bedömning är även här att detta bör dokumenteras i en skriftlig rutin. Återigen behöver det inte vara några omfattande dokument. I princip räcker det med att fastställa uppföljning med, låt säga ettårigt intervall och vem som ansvarar för att det görs. Som ett exempel. Vad gäller övriga överenskommelser på området, till exempel sådana som avser delat eller gemensamt personuppgiftsansvar så uppger förvaltningen att verksamheten inte har några sådana överenskommelser och att eftersom frågan inte varit aktuell har man inte heller några rutiner för ändamålet.

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 i att kunna visa att den personuppgiftsansvarige följer förordningen och kan visa hur detta görs i enlighet med ansvarsskyldigheten i artikel 5 i GDPR. Detta gäller inte minst i händelse av inspektion från tillsynsmyndigheten IMY. Avsaknaden av skriftliga rutiner är också många gånger ett tecken på att en dataskyddsorganisation är personbunden. Dataskyddsombudets uppfattning är att Stadsbyggnadskontoret har god kompetens för att arbeta med dataskyddsfrågorna, men att förvaltningen så långt det är möjligt bör minska personberoendet då det innebär en sårbarhet. Ett viktigt led i detta är att verksamheten fastställer rutiner och arbetssätt, knutna till funktion, för hur arbetet med dataskyddsfrågor ska bedrivas, till exempel då det handlar om uppföljning och kontroll av biträdesavtal. Förvaltningen bör även ha rutiner för situationer som ännu inte uppstått, till exempel tecknandet av andra överenskommelser inom dataskyddsområdet. Poängen med rutiner är att dom ska vara ett stöd för den händelse att något sker, inte att verksamheten tar fram dessa efter att något har skett.

I övrigt så regleras tecknandet av avtal enligt en centraliserad process och det framgår i förvaltningens delegationsordning vem som har rätt att teckna avtal. Dataskyddsombudet har inga synpunkter på det utan ser det som ett rimligt förfarande. Varje medarbetare får anses vara införstådd med att man som anställd bara har rätt att agera i enlighet med den delegationsordning som är fastställd.

Granskning av avtal

Dataskyddsombudet har som en del i en fördjupade kontrollen också granskat tre av de personuppgiftsbiträdesavtal som förvaltningen upprättat med biträden. Dataskyddsombudets bedömning är att avtalen, som i stort följer SKR:s mall för personuppgiftsbiträdesavtal, uppfyller de krav som ska ställas på ett biträdesavtal, med undantag för det avtal som tecknats mellan SBK och lantmäterimyndigheten avseende systemet Trossen. Här saknas instruktion till avtalet, vilket förvaltningen också angett i sitt svar på del 1 av den fördjupade kontrollen. Det framgår enligt ovan att en personuppgiftsansvarig ska ge tydliga instruktioner till biträdet om hur personuppgifter får hanteras i enlighet med vad som anges i artikel 28 i GDPR. Dataskyddsombudets rekommendation är därför att förvaltningen snarast tar fram en instruktion att bilägga till avtalet med lantmäterimyndigheten.

Dataskyddsombudet noterar även att förvaltningen uppdaterat ett av sina avtal med anledning av Storbritanniens utträde ur EU, då ett underbiträde i och med detta kom att befinna sig i tredjeland. Detta signalerar att verksamheten har koll på sina avtal och aktivt jobbar med uppföljning, något som är positivt.

Sammanfattande rekommendationer

- Förvaltningen bör snarast teckna personuppgiftsbiträdesavtal i samtliga fall där verksamheten bedömer att en biträdessituation föreligger.

- Förvaltningen bör ta fram dokumenterade rutiner/arbetssätt 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.

- För de fall som biträdesavtal finns men instruktion saknas bör Stadsbyggnadskontoret snarast utfärda skriftliga instruktioner till biträdet.

Bilagor

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

Bilaga 1

Fördjupad kontroll: Stadsbyggnadskontoret

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.