Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Park- och naturförvaltningen

2022-12-20

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.

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

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

- Förvaltningen bör teckna ett personuppgiftsbiträdesavtal (överenskommelse) med Göteborg Leasing som uppfyller kraven i artikel 28 i GDPR.

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 (2018): Organisatoriska förutsättningar för dataskyddsarbetet.

Verksamheten gavs ursprungligen följande rekommendationer (2018):

Vid den aktuella kontrollen hade verksamheten beskrivit en genomtänkt organisation med utpekade roller. Verksamheten hade en plan för hur dataskyddsarbetet skulle förankras i alla delar av verksamheten. Dataskyddsombudet hade inget att anmärka på verksamhetens planer om arbetet med dataskyddsfrågorna utan bara att de skulle fullföljas. Verksamheten rekommenderades att se över sin integritetspolicy

Och vid 2021 års uppföljning följande kompletterande rekommendation (2021)

Uppföljningen visar att dåvarande planer om dataskyddsarbetet inte riktigt fallit ut som man önskat. Det finns flera rutiner på plats men det finns brister i arbetet med dataskyddsfrågor som en naturlig och integrerad del i det dagliga arbetet inom verksamheten. Därtill behöver rapporteringsvägar definieras så att samtliga dataskyddsfrågor når dataskyddskontakterna i verksamheten. Uppföljning kommer därför att ske igen under 2022.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Förvaltningen upphör att existera som en följd av omorganisation NOS, eftersom en ny organisation kommer finnas på plats kommer ingen vidare uppföljning att ske.

Kontroll 1 (2021): Personuppgiftsbehandlingsregistret.

Verksamheten gavs följande rekommendationer:

• Organisationen behöver se över behandlingarna som idag finns registrerade och komplettera de behandlingar som saknar kontaktuppgift till biträdet/biträden samt lägga till behandlingar som helt saknas.

• Organisationen behöver ta fram en rutin/plan för hur organisationen ska hålla registret uppdaterat och organisationen bör även se över ansvarsfördelningen för detta.

Verksamheten angav att de inte har vidtagit åtgärder för några av de lämnade rekommendationerna. Anledningen till att inte åtgärder har vidtagits enligt rekommendationerna beror på dels personalbrist/personalomsättning, dels tidsbrist

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Park- och naturförvaltningen 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:

• Ta fram anvisningar/rutiner (eller komplettera nuvarande anvisning) gällande behandlingarna kopplade till vinterväghållningen

• Dokumentera rättslig grund i anvisningen avseende ändamålet misstanke om misskötsamhet

• Genomför konsekvensbedömning avseende ISA och personlig körjournal.

• Dokumentera riskerna som finns och eventuella åtgärder/riktlinjer för uppgifterna som samlas in från fordonen i smarta parker.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Park- och naturförvaltningen 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 Park- och naturförvaltningens 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.

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens

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

dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i stora drag med förvaltningens bedömning och anser att verksamheten tagit flera positiva steg under det gångna året med bättre definierade roller och ansvar inom dataskyddsorganisationen och en kontinuerlig och bra dialog med dataskyddsombudet.

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. Dataskyddsombudets uppfattning är att förvaltningen behöver fortsätta arbeta med frågan genom kunskapshöjande åtgärder hos medarbetarna. Dataskyddsombudet kan inte erinra sig att ha kontaktats av förvaltningen rörande någon personuppgiftsincident under året. Med tanke på park- och naturförvaltningens storlek och det betydande antal personuppgifter som hanteras framstår det dock som osannolikt att någon incident inte skulle inträffat under året.

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 året fördjupade kontroll, för kommentarer och rekommendationer hänvisas därför till avsnittet om fördjupad kontroll samt bilaga 2 ”fördjupad kontroll”.

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:

Verksamheten skattar sig själva högt för kontrollpunkten. Verksamheten har angett att de har under eller upp till 75 % av sina behandlingar i ett register. Dataskyddsombudet rekommenderar verksamheten att uppdatera registret med samtliga behandlingar. Verksamheten har de rutiner som behövs och dataskydds-ombudets uppfattning är att förvaltningen kommit en bra bit på väg, men att verksamheten nu behöver ta sista steget i detta arbete genom att skapa ett komplett register.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Kontrollpunkten är något som verksamheten förbättrat under året och dataskyddsombudets uppfattning är att det är ett av dom områden som förvaltningen rört sig framåt i som en del i det allmänna förbättringsarbetet rörande dataskyddsfrågorna. Verksamheten saknar dock fortfarande en fastställd informationssäkerhetspolicy för behandling av personuppgifter och rekommenderas därför att säkerställa att en sådan tas fram inom ramen för den nya förvaltning som uppstår efter årsskiftet.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Verksamheten anser sig ge medarbetare möjlighet att regelbundet delta på externa utbildningar och att förvaltningen regelbundet genomför informationsinsatser för att utbilda och informera medarbetare inom dataskydd. Svaren indikerar också att park- och naturförvaltningen anser att den allmänna kunskapsnivån ger goda förutsättningar i dataskyddsarbetet och att det finns rutiner för att följa upp och bibehålla kunskapsnivån hos medarbetare. Dataskyddsombudets rekommendation är att verksamheten fortsätter med regelbundna informationsinsatser för att bibehålla/höja nivån hos medarbetarna.

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:

Verksamheten har här skattat sig själva med det högsta värdet. Dataskyddsombudet har ingen anledning att göra någon annan bedömning än verksamheten i denna del.

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 genomgående skattat sig själva högt i sina svar för denna kontrollpunkt. Samtidigt uppger förvaltningen att det saknas dokumenterade rutiner och anvisningar för hantering av personuppgifter i e-post. Det är också dataskyddsombudets uppfattning att det generellt är här som de stora bristerna tenderar att förekomma, inte bara hos park- och naturförvaltningen, utan i organisationer generellt.

Det är positivt och nödvändigt att uppdaterade rutiner för dokumenthantering och gallring finns på plats, samtidigt är de största integritetsriskerna ofta knutna just till hanteringen av personuppgifter i e-post. Uppgifter riskerar att lagras under längre

tid än vad som är lämpligt och det är ofta svårt att få en överblick. Rekommendationen är därför att ta fram tydliga rutiner för hanteringen av personuppgifter i e-post och framför allt att säkerställa att efterlevnaden av dessa kan garanteras genom organisatoriska eller tekniska åtgärder.

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:

Dataskyddsombudets kommentar och rekommendation är i allt väsentligt de samma som för 2021 avseende denna kontrollpunkt. Det saknas fortfarande flertalet rutiner för att arbetet med konsekvensbedömningar. Dataskyddsombudet har uppmanat verksamheten att genomföra konsekvensbedömningar för bland annat behandlingar innefattande positioneringsteknik (GPS). En konsekvens-bedömning behöver fortfarande genomföras avseende behandling innefattandes positioneringsteknik såsom ISA och personlig körjournal. Dataskyddsombudet delar därför inte förvaltningens bedömning att konsekvensbedömningar har tagits fram för samtliga av de behandlingar som park- och naturförvaltningen utför och där det kan finnas höga risker för de registrerades fri- och rättigheter.

Dataskyddsombudets rekommendation är att en konsekvensbedömning avseende personlig körjournal tas fram snarast då det är en kvarstående rekommendation ifrån förra årets rapport. Därtill bör en översyn göras över verksamhetens samtliga behandlingar och bedömning av behovet av konsekvensbedömning för dessa. Detta då det rimligen finns fler behandlingar som uppfyller kravet på att verksamheten ska ha genomfört en konsekvensbedömning.

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:

Verksamhetens svar indikerar att det kvarstår brister avseende kontrollpunkten som behöver åtgärdas. Verksamheten har angett att det saknas tillräckliga rutiner för att genomföra risk/behovsanalys med syfte att säkerställa att nya IT-lösningar uppfyller de grundläggande kraven i GDPR. Verksamheten arbetar inte heller systematiskt och kontinuerligt med att bedöma risker för personuppgiftsbehandlingar i såväl nya som befintliga system och tjänster. Verksamheten anger vidare att de inte via kravställningen säkerställer att nya system/tjänster har dataskydd som standard och/eller inbyggt dataskydd. Förvaltningen rekommenderas därför att ta fram rutiner för att kunna genomföra en risk-/behovsanalys med syfte att säkerställa att nya IT-lösningar uppfyller kraven i GDPR. Verksamheten behöver även ta fram rutiner för att i upphandlingar via kravställningen säkerställa att nya system/tjänster är anpassade till principerna om inbyggt dataskydd och dataskydd som standard. Därtill bör förvaltningen arbeta systematiskt och kontinuerligt med att bedöma risker för personuppgifts-behandlingar i upphandlingar av nya, samt utveckling av, befintliga system och tjänster.

Dess risker är kvarstående från föregående år, likaså är dataskyddsombudets rekommendationer kvarstående och detta är ett arbete som behöver prioriteras i den nya organisation som införs 2023.

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:

Park- och naturförvaltningens svar indikerar att det inte förelomme några stora risker under kontrollpunkten. Förvaltningens svar visar dock att det fortfarande finns åtgärder som behöver vidtas, till exempel har verksamheten på tre av enkätfrågorna angett svaret ”0/vet ej” något som i sig är ett tecken på att en verksamhet inte fullt ut har överblick.

Med ledning av svaren rekommenderas verksamheten därför att ta utreda/ta fram rutiner avseende användandet av olika kommunikationskanaler och att dessa följer GDPR, ta fram målgruppsanpassad information för de digitala verktyg som används, samt ta fram rutiner för att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster såsom gratisappar eller 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:

Dataskyddsombudet gör ingen annan bedömning än verksamheten för den aktuella kontrollpunkten. Men förvaltningen rekommenderas att öka kunskaperna hos medarbetare om de registrerades rättigheter och i vilka fall rättigheterna kan begränsas.

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 9: Konsekvensbedömning/samråd
  Genomför översyn över verksamhetens samtliga behandlingar och bedöm behovet av konsekvensbedömningar för dessa.

- Kontrollpunkt 10: IT- projekt och upphandling
  Ta fram rutiner för att kunna genomföra en risk-/behovsanalys med syfte att säkerställa att nya IT-lösningar uppfyller kraven i GDPR.

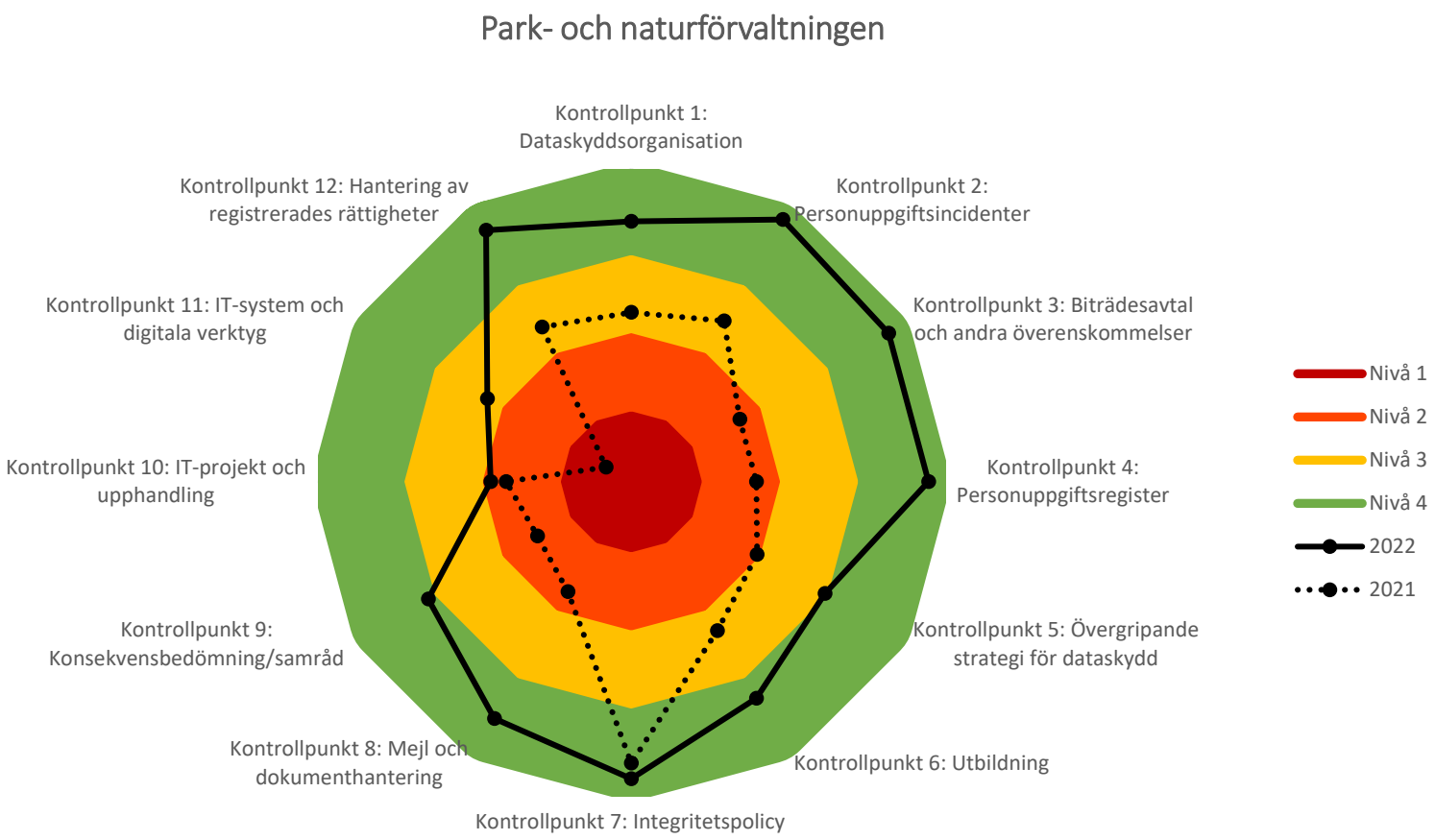
- Kontrollpunkt 10: IT- projekt och upphandling
  Ta fram rutiner för att i upphandlingar via kravställningen säkerställa att nya system/tjänster är anpassade till principerna om inbyggt dataskydd och dataskydd som standard

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: Park- och naturförvaltningen

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 och personuppgiftsbiträde 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 (PUA) 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

Park- och naturförvaltningen har tecknat biträdesavtal med 15 personuppgiftsbiträden. Dataskyddsombudet noterar utöver detta att det förefaller saknas ett antal leverantörer som borde vara 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, uppmanas förvaltningen att så snart som möjligt utreda huruvida biträdesavtal ska tecknas och att därefter tillse att avtal upprättas med samtliga personuppgiftsbiträden.

Biträdesavtal och instruktioner

Av de 15 avtal som förvaltningen har tecknat så uppger verksamheten att instruktioner saknas i fyra fall. I de fall avtal finns, men där instruktion saknas, så bör förvaltningen snarast upprätta instruktioner för biträdet. Det framgår av artikel 28 i GDPR att en personuppgiftsansvarig ska ge tydliga instruktioner till ett underbiträde angående vilka personuppgifter som får hanteras och på vilket sätt detta ska ske. Förvaltningen uppger att en skriftlig rutin har upprättats för att avgöra huruvida en behandling kräver att ett biträdesavtal tecknas och också hur detta ska ske rent praktiskt. Rutinen gäller från och med 31 mars 2022.

Kontroll och uppföljning

I rutinen som refereras till enligt ovan beskrivs också hur förvaltningen ska arbeta för att följa upp de garantier som personuppgiftsbiträden lämnat avseende tekniska och organisatoriska åtgärder. Förvaltningen har inte tidigare prioriterat detta och det har saknats rutiner och struktur för ett sådant arbete. Park – och naturförvaltningen har i och med den framtagna rutinen tagit ett första och viktigt steg mot att ta sig an frågan. Rutinen tar också upp avtalsuppföljning, något som verksamheten inte heller tidigare arbetat aktivt med

Förvaltningen har i sitt svar angett att verksamheten inte tidigare har sett ett behov av rutiner då arbetet med personuppgiftsbiträdesavtal legat på en väldigt liten krets av medarbetare. Även om dataskyddsombudet kan ha viss förståelse för det synsättet så skapar det en organisation som är personberoende och därmed sårbar. 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 är dock att kunna visa att man följer förordningen och hur detta görs.

Detta gäller inte minst i händelse av inspektion från tillsynsmyndigheten. Upprättandet av tydliga skriftliga instruktioner för arbetet med biträdesavtal innebär också att verksamheten rör sig bort ifrån de risker som kan kopplas till ett stort personberoende. Dataskyddsombudet uppfattning är att förvaltningen har kompetens för att arbeta med dataskyddsfrågorna, men i likhet med många andra verksamheter så bör verksamheten minska beroendet av enskilda medarbetare då det innebär en sårbarhet. Ett viktigt led i detta är att förvaltningen fastställer skriftliga rutiner 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 i förvaltningens delegationsordning och dataskyddsombudet har inga synpunkter på det. Varje medarbetare får anses vara införstådd med att man som anställd bara har rätt att agera i enlighet med den delegationsordning som är fastställd.

Vad gäller övriga överenskommelser på området, till exempel sådana som avser delat eller gemensamt personuppgiftsansvar så uppger förvaltningen att verksamheten har överenskommelser med Göta Lejon gällande försäkringsärenden och Front Advokatbyrå för juridiska frågor.

Förvaltningen uppger att frågan om delat personuppgiftsansvar är ytterst sällsynt och har bara uppstått vid ett par enstaka tillfällen. Förvaltningen har därför inte tidigare övervägt behovet av att upprätta en rutin. I den nyupprättade rutinen har verksamheten dock adresserat även den här frågan. Detta anser dataskyddsombudet vara positivt även om förvaltningen tydligare kunde ha beskrivit i rutinen när ett avtal om delat personuppgiftsansvar behövs.

Som dataskyddsombudet redan nämnt så bör skriftliga rutiner finnas även vid sällsynta situationer, då det är en väg att komma bort ifrån personberoendet i dataskyddsorganisationen och är ett sätt att påvisa att verksamheten har ett fungerande dataskyddsarbete och följer GDPR. Skriftliga rutiner fyller två funktioner; som ett stöd för att tillse att verksamheten följer dataskyddsförordningen och som ett sätt att visa att organisationen uppfyller ansvarsskyldigheten enligt artikel 5. Det räcker alltså inte att följa förordningen, verksamheten ska också kunna visa att den gör det och hur.

Granskning av avtal

Som en del i den fördjupade kontrollen har dataskyddsombudet tittat på tre slumpmässigt utvalda biträdesavtal som förvaltningen upprättat med sina personuppgiftsbiträden.

Avtalet med Göteborgs Stad leasing, finner dataskyddsombudet vara mycket knapphändigt och det saknar många av de delar som normalt återfinns i ett biträdesavtal, Avtalet är också tecknat före det att dataskyddsförordningen trädde i kraft. Avtalet saknar helt reglering av tredjelandsöverföringar och ansvarsfrågan. Det saknas också en instruktion till avtalet.

Avsaknaden av instruktion är det som är mest kritiskt och förvaltningen bör snarast utfärda en sådan. Dataskyddsombudets rekommendation är att verksamheten tecknar ett helt nytt avtal, gärna utifrån SKR:s mall för biträdesavtal och däri inkluderar en nyutfärdad instruktion till biträdet. Vad gäller personuppgiftsbiträdesavtalen med Mercell och Safeteam så följer dessa avtal SKR:s standardmall, dataskyddsombudet har inga synpunkter på avtalen eller dess instruktioner.

Sammanfattande rekommendationer

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

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

- Förvaltningen bör teckna ett personuppgiftsbiträdesavtal (överenskommelse) med Göteborg Leasing som uppfyller kraven i artikel 28 i GDPR.

Bilagor

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

Bilaga 1

Fördjupad kontroll: Park- och naturförvaltningen

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.