Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Lokalförvaltningen

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 därför lämnat ett antal rekommendationer till verksamheten att vidta åtgärder.

- Förvaltningen bör utreda frågan om personuppgiftsansvar för samtliga personuppgiftsbehandlingar, utföra en inventering för att klargöra vilka biträden verksamheten anlitar och därefter teckna personuppgiftsbiträdesavtal 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 och implementera ett strukturerat arbetssätt för hanteringen av dessa frågor. Detta för att kunna visa att ansvarsskyldigheten i artikel 5 i GDPR uppfylls.

- Lokalförvaltningen bör ta fram skriftliga och heltäckande rutiner för att kontrollera och följa upp att de biträden som anlitas efterlever de krav och garantier som lämnats, samt ta fram arbetssätt för regelbunden avtalsuppföljning.

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:

- 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.

- 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. Följande åtgärder har vidtagits: rutiner/information till anställda har tagits fram medan följande rekommendationer återstår: kartlägg behandlingar med positioneringsteknik och genomför konsekvensbedömningar. Lokalförvaltningen 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.	

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

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

Dataskyddsombudets kommentarer:

Förvaltningen har över lag skattat kontrollpunkten utefter en avsaknad av höga risker. Dataskyddsombudet gör en annan bedömning än lokalförvaltningen och är av uppfattningen att verksamheten i stort saknar en intern dataskyddsorganisation. Det finns visserligen vissa utpekade roller, men varken kunskap, resurser eller förutsättningar för att bedriva ett systematiskt dataskyddsarbete. Det som är positivt är att förvaltningen i sin dialog med dataskyddsombudet verkar ha en klar insikt om sina brister och att verksamheten beslutat att anställa en helt dedikerad resurs med adekvat kompetens för att arbeta med frågorna.

Detta är ett bra första steg men inte tillräckligt. En person gör ingen organisation. Förvaltningen behöver därför snarast ta fram en definierad och samordnad dataskyddsorganisation och utreda vilka resurser och vilken kompetens verksamheten behöver inom organisationen för att säkerställa dataskyddsperspektivet. På grund av hur eftersatt arbetet är och svårigheterna med att rekrytera in rätt kompetens, så är dataskyddsombudets rekommendation att förvaltningen bör överväga att ta hjälp av extern konsult för att sparka igång dataskyddsarbetet när lokalförvaltningen upphör och blir stadsfastighetsförvaltningen. Risken är annars att värdefull tid går förlorad i väntan på en mer permanent rekrytering. Det är av stor vikt att arbetet med att leva upp till kraven i GDPR kommer i gång så snart det bara går.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Dataskyddsombudets uppfattning är att detta är en av de delar där förvaltningen har ett fungerande dataskyddsarbete och ett utvecklat arbetssätt och rutiner. Verksamheten har angett att det finns dokumenterade rutiner som ger goda förutsättningar för att upptäcka och utreda incidenter och dataskyddsombudet har inte haft anledning att göra någon annan bedömning. Samtidigt behöver kunskap om vad som utgör personuppgiftsincidenter kontinuerligt spridas i organisationen och rekommendationen är därför att arbeta med kontinuerliga informationsinsatser.

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:

Förvaltningens skattning visar att det föreligger höga risker inom kontrollpunkten. Dataskyddsombudet delar bedömningen och anser att risken i vissa delar är mycket

hög mot bakgrund av att det är ett krav enligt förordningen att ha ett aktuellt och uppdaterat register över personuppgiftsbehandlingar. Verksamheten rekommenderas därför att prioritera detta arbete. Lokalförvaltningen behöver säkerställa att samtliga personuppgiftsbehandlingar dokumenteras i personuppgiftsregistret och att all nödvändig information då läggs in i det samma.

Framgent bör den interna dataskyddsorganisationen även fundera över på vilket sätt personuppgiftsregistret kan användas som del i det löpande dataskyddsarbetet.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Lokalförvaltningens svar indikerar att det inom denna kontrollpunkt finns omfattande risker som kräver omgående åtgärder. Avsaknaden av överblick och tydlig styrning i hur dataskyddsarbetet bedrivs innebär en risk eftersom verksamheten då bland annat riskerar att lägga resurser på fel frågor. Riskerna kvarstår i allt väsentligt ifrån 2021 års rapport och därmed är dataskyddsombudets kommentarer och rekommendation i princip identisk med denna.

Ett systematiskt dataskyddsarbete bör bedrivas utifrån övergripande strategier för verksamheten avseende både dataskydd och informationssäkerhet. Det är därför av stor vikt att förvaltningen säkerställer att styrande dokument som reglerar personuppgifter hålls uppdaterade. Det behöver också finnas en informationssäkerhetspolicy som anger hur personuppgifter kan behandlas i exempelvis IT-system, datorer och mobila enheter.

Av vikt är även att säkerställa att verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet. Verksamheten behöver också regelbundet genomföra kontroller för att se hur dataskyddsförordningen efterlevs.

Utifrån detta rekommenderas lokalförvaltningen att i dokumenterade handlings- och/eller verksamhetsplan, rutiner och policys tydliggöra sin strategi för det övergripande dataskyddsarbetet. Förvaltningen behöver också säkerställa att dataskyddsarbetet samordnas med informationssäkerhetsarbetet och att verksamhetens informationstillgångar värderas.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Förvaltningen har identifierat stora brister i den allmänna kunskapsnivån hos medarbetarna. Dataskyddsombudet rekommenderar därför att förvaltningen ger medarbetarna möjlighet att delta i både interna och externa utbildningsinsatser för att höja den allmänna kunskapsnivån om dataskydd.

Vidare rekommenderas lokalförvaltningen säkerställa att medarbetarna erbjuds rätt utbildningsinsatser, för att möjliggöra detta behöver verksamheten kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.

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 förvaltningens skattning av kontrollpunkten. Jämfört med andra delar av dataskyddsarbetet föreligger här inga höga risker, men då lokalförvaltningen angett att policyn inte är nåbar från samtliga digitala kanaler rekommenderas förvaltningen att 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:

Även för denna kontrollpunkt kvarstår i princip de risker som identifierades vid förra årets rapport. Lokalförvaltningens svar indikerar att verksamheten inom denna kontrollpunkt har omfattande risker som kräver omgående åtgärder.

Dataskyddsombudet har ingen anledning att göra en annan bedömning än den som förvaltningen gjort avseende denna punkt. Principerna om uppgifts- och lagringsminimering är grundläggande i dataskyddsförordningen. Det ställs också höga krav på att hantera uppgifter med tillräcklig säkerhet. Utifrån svaren finns det inom förvaltningen ett behov av att se över organisationens informations-klassificering av personuppgiftsbehandlingar och kontrollera så att detta görs i enlighet med Göteborgs Stads riktlinjer för informationssäkerhet. Verksamheten måste även se till så att medarbetarna vet hur information ska hanteras beroende på informationsklassningen.

Mot bakgrund av att den stora förekomsten av personuppgifter i e-post så är det viktigt att förvaltningen tar fram rutiner som säkerställer att hanteringen av personuppgifter i e-post sköts på ett korrekt och lagenligt sätt. Förvaltningen rekommenderas också att säkerställa att det finns förutsättningar för gallring av personuppgifter som inte längre är nödvändiga att behandla.

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:

Lokalförvaltningens svar indikerar att förvaltningen har omfattande risker inom denna kontrollpunkt, som kräver omgående åtgärder. Till dataskyddsombudets vetskap har förvaltningen inte genomfört några konsekvensbedömningar under året och dataskyddsombudet har utifrån detta ingen anledning att göra en annan bedömning än den som förvaltningen gjort avseende denna punkt.

Att förvaltningen inte arbetar med konsekvensbedömningar är ett naturligt resultat av att verksamheten saknar ett fungerande dataskyddsarbete. Dataskyddsombudets rekommendation är därför att verksamheten tar ett helhetsgrepp på frågan och kartlägger samtliga personuppgiftsbehandlingar med höga risker, tar fram heltäckande rutiner och arbetssätt för samtliga aspekter av konsekvensbedömningsarbetet och genomför bedömningar där så krävs.

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:

Även för denna kontrollpunkt kvarstår i princip de risker som identifierades vid förra årets rapport. Lokalförvaltningens svar indikerar att förvaltningen inom detta område har mycket omfattande risker som kräver omgående insatser som behöver följas upp av ledning och/eller övriga verksamheten.

Skattningen visar att förvaltningen har behov av att säkerställa att dataskyddsperspektivet finns med i arbetet med nya IT- och digitaliseringslösningar, samt vid utvecklingen av redan befintliga system och tjänster. Vid upphandling av nya system/tjänster så behöver det tas med i kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard. Verksamheten bör även ha som rutin att dataskyddsombudet involveras från start i dessa processer.

Dataskyddsombudet rekommenderar att arbetet inom området prioriteras och att den interna dataskyddsorganisationen ges förutsättningar för att, tillsammans med dataskyddsombudet, kunna identifiera vilka åtgärder som behöver vidtas för att hantera riskerna.

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:

Dataskyddsombudet delar inte förvaltningens egen skattning av kontrollpunkten och är av uppfattningen att det inom lokalförvaltningen används flertalet olika digitala verktyg och IT-system som inte har kontrollerats utifrån ett dataskyddsperspektiv innan de införts. Som en konsekvens av detta använder lokalförvaltningen idag tjänster som av olika skäl inte har en tillräcklig säkerhet

vad gäller dataskydd. Förvaltningen rekommenderas därför att kartlägga samtliga de IT-system och digitala verktyg som används inom verksamheten och att kontrollera dessa verktygs följsamhet gentemot GDPR. Det finns även behov av att se över hanteringen av medarbetares behörigheter till dessa digitala verktyg och IT-system i samband med förändrade behov, samt framtagande av rutiner för att kunna kontrollera så att IT-system och digitala verktyg används på rätt sätt.

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, men har inte heller några indikationer som tyder på att skattningen skulle vara missvisande eller felaktig. Med tanke på vad som i övrigt har framkommit under den fasta kontrollen så är ändå dataskyddsombudets rekommendation att förvaltningen gör en översyn även av denna kontrollpunkt, inte minst med tanke på den låga självskattningen av utbildningsnivån inom dataskydd hos medarbetarna.

2.5 Särskilda iakttagelser under året

2.5.1 Avsaknad av ett fungerande dataskyddsarbete

Förvaltningens egna skattningar av de 12 kontrollpunkterna visar med tydlighet att lokalförvaltningen saknar ett fungerande dataskyddarbete. Dataskyddsombudet ser det som positivt att förvaltningen själva identifierat och erkänner problemen som finns i verksamheten, både i form av svaren på dataskyddsombudets kontrollfrågor och i direkt dialog med dataskyddsombudet. Framför allt avseende svaren på frågorna i den fasta kontrollen är det ett fall framåt jämfört med föregående års glädjekalkyler och vittnar om ”sjukdomsinsikt”.

Samtidigt är det en ohållbar situation att förvaltningen fyra år efter GDPR:s införande fortfarande sakna ett adekvat förhållningssätt till integritets- och dataskyddsfrågorna. Riskerna för de registrerades fri- och rättigheter är i många fall påtagliga, liksom den juridiska risken för lokalförvaltningen i form av sanktionsavgifter ifrån tillsynsmyndigheten. Det är därför av största vikt att förvaltningen en gång för alla tar tag i frågan och ser till att verksamheten har resurser och kompetens till sitt förfogande för att möjliggöra efterlevnad av lagstiftningen.

2.6 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

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

- Kontrollpunkt 1: Dataskyddsorganisation
  Förvaltningen behöver därför snarast ta fram en definierad och samordnad dataskyddsorganisation och utreda vilka resurser och vilken kompetens som behövs inom verksamheten för att säkerställa dataskyddsperspektivet.

- Kontrollpunkt 2: Biträdesavtal och andra överenskommelser
  Förvaltningen bör utreda frågan om personuppgiftsansvar för samtliga personuppgiftsbehandlingar, utföra en inventering för att klargöra vilka biträden man anlitar och därefter teckna personuppgiftsbiträdesavtal för de behandlingar som verksamheten anser bör regleras i enlighet med vad som anges i artikel 28 i GDPR.

- Kontrollpunkt 3: Personuppgiftsregister
  Verksamheten behöver säkerställa att samtliga personuppgiftsbehandlingar dokumenteras i personuppgiftsregistret och att all nödvändig information då läggs in i det samma.

- Kontrollpunkt 10: IT-projekt och upphandling

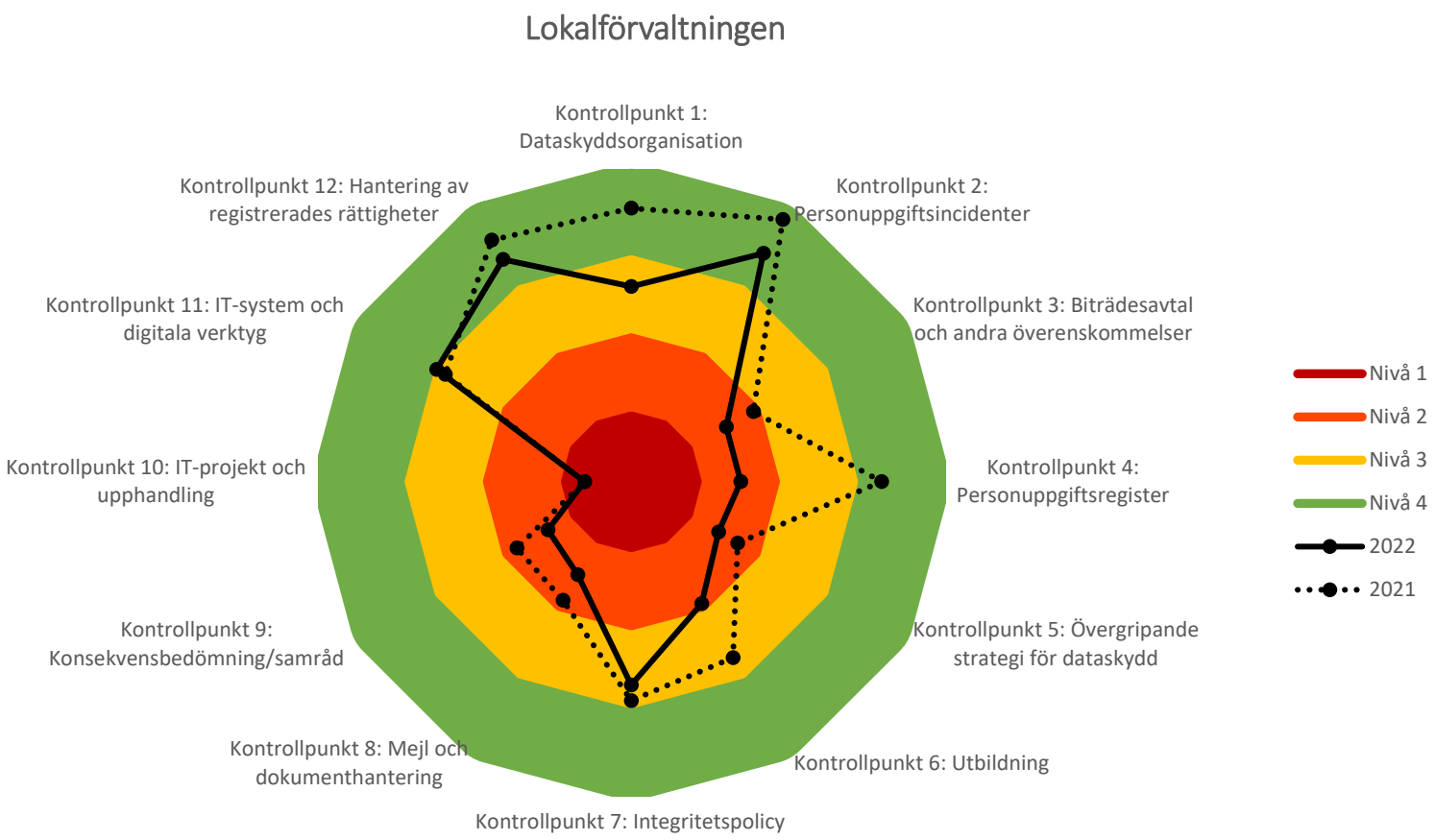
Vid upphandling av nya system/tjänster så behöver det tas med i kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard.

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: Lokalförvaltningen

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

Lokalförvaltningen har tecknat personuppgiftsbiträdesavtal (PUB-avtal) med nio personuppgiftsbiträden, Dataskyddsombudet noterar utöver detta att det förefaller saknas ett antal leverantörer. Avsaknaden av dessa kan dock bero på otydligheter i Stadens styrmodell angående vem som egentligen ska teckna biträdesavtal, då de rör kommungemensamma interna tjänster. Detta går också i linje med förvaltningens eget svar, där verksamheten uppger sig sakna överblick avseende hur många och vilka biträden lokalförvaltningen faktiskt anlitar.

För de fall där biträdesavtal saknas, eller biträdesrelationen är oklar, rekommenderas lokalförvaltningen att snarast utreda huruvida biträdesavtal ska tecknas och att därefter tillse att avtal upprättas med samtliga personuppgiftsbiträden. Ett första steg till att inleda en sådan process är att inventera vilka biträden verksamheten faktiskt använder sig av och sedan ange detta i sitt personuppgiftsbehandlingsregister.

En grundläggande förutsättning för att kunna följa dataskyddsförordningen och visa att man systematiskt arbetar med dataskydd är att verksamheten har koll på sina behandlingar. I detta ingår att ha kännedom om vilka personuppgiftsbiträden som anlitas och tillse att detta regleras i en sådan rättsakt som beskrivs i artikel 28 GDPR. Dataskyddsombudets rekommendation är därför att förvaltningen snarast inventerar i vilka av sina personuppgiftsbehandlingar som man använder sig av ett biträde och därefter tillse att personuppgiftsbiträdesavtal tecknas i de fall det krävs.

Biträdesavtal och instruktioner

Förvaltningen uppger sig ha en skriftlig rutin för att avgöra huruvida en behandling kräver att ett biträdesavtal tecknas och också hur detta ska ske rent praktiskt. Rutinen finns tillgänglig på intranätet och är även en del av lokalförvaltningens utbildningsmaterial kring dataskydd. Av förvaltningens svar till dataskyddsombudet framgår att instruktioner ska finnas till samtliga personuppgiftsbiträdesavtal i form av en särskild bilaga.

Samtidigt uppger sig förvaltningen inte ha någon struktur för att tillse att biträdesavtal tecknas i behörig ordning. En uppgift som förefaller något motstridig. Dataskyddsombudet rekommenderar därför att lokalförvaltningen utreder och tydliggör strukturen för när och hur biträdesavtal ska tecknas och att detta formaliseras i fastställda rutiner som kommuniceras ut i organisationen.

Kontroll och uppföljning

Vad gäller rutiner för att arbeta med att säkerställa och följa upp att personuppgiftsbiträden uppfyller de garantier som dessa har lämnat avseende tekniska och organisatoriska åtgärder, samt rutiner för regelbunden avtalsuppföljning, så uppger verksamheten att det saknas rutiner och struktur för ett sådant arbete.

För övriga överenskommelser, till exempel avseende gemensamt/delat personuppgiftsansvar, säger sig lokalförvaltningen sakna en etablerad struktur för detta arbete, det finns inga rutiner för att fastställa när sådana överenskommelser ska ingås och verksamheten säger sig inte heller ha vetskap om sådana överenskommelser finns på plats idag. Avsaknaden av etablerade rutiner och arbetssätt är en allvarlig brist som kräver omedelbara åtgärder. Eftersom dataskyddsombudet tidigare blivit kontaktad i frågan om delat ansvar, vid åtminstone ett tillfälle, framstår det som anmärkningsvärt att förvaltningen själva inte tycks känna till om det har ingåtts någon sådan överenskommelse med part.

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 verksamheten följer förordningen och även hur detta görs. Detta gäller inte minst i händelse av en inspektion från tillsynsmyndigheten. Med ledning av förvaltningens svar och dataskyddsombudets egna iakttagelser så är den samlade bedömningen att avsaknaden av rutiner, systematisk dokumentation och översikt över de egna personuppgiftsbehandlingarna indikerar att lokalförvaltningen helt enkelt inte har ett systematiskt arbete med frågorna. Detta är en allvarlig brist som behöver åtgärdas snarast.

Förutom att inventera och dokumentera samtliga sina biträdesrelationer och teckna avtal där så krävs, så bör förvaltningen också ta fram skriftliga och heltäckande rutiner för att kontrollera och följa upp att de biträden som anlitas efterlever de krav och garantier som lämnats, ta fram en rutin för regelbunden avtalsuppföljning och säkerställa att rutiner finns på plats för att identifiera när avtal om gemensamt eller delat personuppgiftsansvar ska tecknas. Förvaltningen behöver också fastställa vem som bär ansvaret för och i vilken ordning som biträdesavtal och andra överenskommelser ska tecknas.

Granskning av avtal

Som en andra del i den fördjupade kontrollen har Dataskyddsombudet också granskat tre slumpmässigt utvalda personuppgiftsbiträdesavtal som förvaltningen tecknat med leverantörer. Avtalen som rör Easyapp och Mercel Commerce utgår bägge ifrån SKR:s mall för PUB-avtal. Dataskyddsombudet har inga synpunkter på avtalen i sig, men för Easyapp förefaller det saknas två sidor i den kopia som förvaltningen tillsänt dataskyddsombudet, för detta avtal saknas också instruktion. Det åligger den personuppgiftsansvarige att tillse att det personuppgiftsbiträde verksamheten anlitar får skriftliga instruktioner för hur personuppgifterna ska behandlas. Dataskyddsombudet saknar också tydligare beskrivning av exakt vad det är som biträdet egentligen ska utföra för uppgifter å lokalförvaltningens vägnar.

Detta är också otydligt i avtalet med Precio. I avtalet med Precio saknar dataskyddsombudet också reglering av möjligheten att invända mot eller godkänna nya underbiträden. I avtalet står endast att den personuppgiftsansvarige ska underrättas.

Underbiträdena ska visserligen vara bundna av samma överenskommelse och instruktioner som personuppgiftsbiträdet. Dataskyddsombudet skulle dock vilja se att den personuppgiftansvariges rätt att invända reglerades tydligt i avtalet. Inte heller i denna instruktion framgår det tydligt vad personuppgiftsbiträdet egentligen gör å lokalförvaltningens vägnar.

Dataskyddsombudet rekommenderar därför att lokalförvaltningen tar fram en instruktion för avtalet med Easyapp, lokaliserar de försvunna sidorna av biträdesavtalet och tydliggör vad det egentligen är som biträdet gör. Vad gäller avtalet med Precio rekommenderar dataskyddsombudet även här att det förtydligas vad det är som biträdet utför för uppgift samt att rätten att invända eller godkänna nya underbiträden regleras i avtalet.

Sammanfattande rekommendationer

- Förvaltningen bör utreda frågan om personuppgiftsansvar för samtliga personuppgiftsbehandlingar, utföra en inventering för att klargöra vilka biträden verksamheten anlitar och därefter teckna personuppgiftsbiträdesavtal för de behandlingar som förvaltningen anser bör 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 och implementera ett strukturerat arbetssätt för hanteringen av dessa frågor. Detta för att kunna visa att ansvarsskyldigheten i artikel 5 i GDPR uppfylls.

- Lokalförvaltningen bör ta fram skriftliga och heltäckande rutiner för att kontrollera och följa upp att de biträden som anlitas efterlever de krav och garantier som lämnats, samt ta fram en rutin för regelbunden avtalsuppföljning.

Bilagor

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

Bilaga 1

Fördjupad kontroll: Lokalförvaltningen

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.