Stockholms stad

Bilaga 9

GDPR årsrapport

År 2025

Miljö- och hälsoskyddsnämnden

GDPR årsrapport
Januari 2026

Dnr: 2025-23761
Utgivningsdatum: 2026-01-08
Kontaktperson: Sofia Rohdin, Dataskyddsombud

Sammanfattning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Ett dataskyddsombud har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar dataskyddsombudet årets granskning av Miljö- och hälsoskyddsnämndens dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Miljö- och hälsoskyddsnämnden uppvisar god mognad i dataskyddsarbetet med välfungerande registerförteckning, etablerade styrdokument, regelbunden utbildning och ändamålsenliga incidentrutiner. En ytterligare styrka är Miljö- och hälsoskyddsnämndens interna GDPR-grupp som har stor kunskap om dataskyddsarbete och är ett bra stöd för verksamheten. Samtidigt kvarstår betydande brister som påverkar registrerades rättigheter och nämndens möjlighet att visa efterlevnad. Sammantaget bedöms den sammanlagda risken som medelhög. Styrkorna väger upp flera områden, men några centrala risker kräver åtgärder.

De största riskerna enligt dataskyddsombudets bedömning rör principen om öppenhet, i form av registrerades rätt till tillgång (art 15) och registrerades rätt till information (art 13–14). Stickprov har visat att registerutdrag saknar faktiska personuppgifter och komplett information. DSO:s granskning visar även att det finns en betydande risk kopplad till otydlig fördelning av det kommuninterna personuppgiftsansvaret. Nämndens begränsade faktiska rådighet över vissa personuppgiftsbehandlingar som de anses ha personuppgiftsansvaret för och otydligheten påverkar förmågan att uppfylla flera grundläggande krav i GDPR så som ansvarsskyldigheten (art 5.2, art 24 GDPR), registrerades rättigheter (art 12-22) och säkerhet. Dataskyddsombudet vill i sammanhanget påpeka att arbete för att minska den här risken förutsätter samarbete, åtminstone med t ex Stadsledningskontoret, och risken inte kan mitigeras av Miljö- och hälsoskyddsnämnden på egen hand.

Miljö- och hälsoskyddsnämnden uppfyller GDPR i väsentliga delar, men behöver vidta åtgärder för att stärka transparens och öppenhet mot registrerade och verka för att tydliggöra det kommuninterna personuppgiftsansvaret.

Störst risker enligt dataskyddsombudets bedömning:

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Ändamålsenliga mallar och rutiner för hantering av registrerades rättigheter samt om svar till de registrerade uppfyller lagkrav		DSO rekommenderar att uppdatera rutiner samt ta fram ändamålsenlig mall för svar.
Kommuninternt personuppgiftsansvar – otydlig fördelning begränsar förmåga att följa GDPR		DSO rekommenderar flera åtgärder, bland annat att driva klarläggande med SLK och att verka för upprättande av stadeninterna instruktioner. Se granskningen i sin helhet i bilaga 3.
Information till registrerade (anställda, användare av e-tjänster)		DSO rekommenderar att uppdatera information om personuppgiftsbehandling till anställda och användare av två av Miljö- och hälsoskyddsnämndens e-tjänster i enlighet med artiklar 12–14 samt relevant praxis och vägledning.

Innehållsförteckning

Inledning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Dataskyddsreglerna (*kallas GDPR fortsättningsvis*) sätter tydliga ramar för hur personuppgifter får behandlas för att minimera risken för skada och säkerställa att hanteringen sker ansvarsfullt och rättvist. GDPR har sin grund i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse ett dataskyddsombud. Dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Ombudets roll är att kontrollera att GDPR följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till nämnder och styrelser.

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och styrelse. Genom rapporten kan nämnd och styrelse ta emot de råd och rekommendationer som dataskyddsombudet lämnar. Årsrapporten syftar till att nämnd/styrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Årsrapporten är ett medel för nämnds/styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Granskning av dataskyddsarbetet 2025

Kontroll av obligatoriska områden

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete utifrån sex obligatoriska områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten (IMY) utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del.

Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.

Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena. Vidare redovisas dataskyddsombudets centrala iakttagelser, inklusive områden där verksamheten uppvisar goda resultat och bör upprätthålla sitt arbete, samt identifierade brister som kan utgöra dataskyddsrisker. Avsnittet innehåller även dataskyddsombudets rekommenderade åtgärder för att hantera dessa risker och stärka dataskyddsarbetet.

En fullständig redovisning av dataskyddsombudets underlag och resultat från granskningen av de sex obligatoriska områdena finns att läsa i bilaga 1. Bilagan innehåller även en beskrivning av syftet och bakgrunden för varje område.

Register över personuppgiftsbehandlingar

Sammanfattning

DSO har inte noterat några brister kopplade till registerförteckningen. Registerförteckningen har utökats med sju behandlingar sedan 2024 års kontroll. Rutinerna och samordning av uppdatering sker på samma sätt som tidigare år. Allting tyder på att verksamheten har goda rutiner för att hålla förteckningen uppdaterad och korrekt, genom medvetandegörande hos de som äger informationsmängder och/eller processer, samordning av uppdatering årligen och vid behov och överlag en god struktur.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		139 behandlingar registrerade (år 2024: 132). DSO rekommenderar att den personuppgiftsansvarige fortsätter hålla registerförteckningen uppdaterad och korrekt.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Verksamheten har ändamålsenliga rutiner. DSO rekommenderar att fortsätta hålla i dessa rutiner och medvetenheten om registerförteckningen.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		En gång om året genomförs en stor genomlysning, och utöver det uppdateras registerförteckningen vid förändrade eller nya behandlingar. DSO konstaterar att dessa rutiner är välfungerande och rekommenderar att hålla i dessa.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		DSO har granskat registerförteckningen och konstaterar att den innehåller vad som krävs enligt artikel 30 GDPR, och mer information därutöver.

Säkerhet i samband med behandlingen

Sammanfattning

DSO har inte identifierat några höga risker på området. I intervjuer med verksamheten (GDPR-gruppen och ett antal objektledare) har det framkommit att verksamheten anser att rutiner och styrande dokument kopplade till personuppgiftsbehandling, där genomförande av informationsklassningar är en rutin, är välfungerande. Under året har registraturen kartlagt informationsklassningar och refererat relevanta klassningar i registerförteckningen för att säkerställa att alla personuppgiftsbehandlingar har informationsklassats enligt stadens riktlinjer för informationssäkerhet. I informationsklassningarna ingår även att beakta känsligheten av de personuppgifter som behandlas.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		Dataskyddsombudet har gjort tre stickprov där två av tre visar att verksamheten har beaktat graden av känslighet för personuppgifterna vid informationsklassningsarbetet. Den tredje klassningen har genomförts i KLASSA enligt Miljöförvaltningen. DSO har tagit emot ett aggregerat resultat av aktuell klassning. I en informationsklassning saknas information om eventuella skyddade personuppgifter behandlas. DSO rekommenderar att fortsätta arbeta med informationsklassningar regelbundet i enlighet med styrande dokument, samt att uppdatera klassningen för ärendehanteringssystemet Ecos då den är något föråldrad (2023) och Ecos är verksamhetskritiskt med omfattande personuppgiftsbehandling.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		DSO har inte identifierat några brister i styrande dokument och verksamheten har i ett flertal intervjuer uppgett att dokumenten ger tillräckligt stöd.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		DSO bedömer att verksamheten har en relativt hög mognad på dataskyddsområdet. Genom utbildning och regelbundna påminnelser om säkerhet och dataskydd verkar verksamheten ha gjort dokument och rutiner implementerade och kända på ett bra sätt. Särskilt Miljöförvaltningens GDPR-grupp är en viktig del av detta. Finns visst

		behov av implementering av rollerna inom systemförvaltningen. DSO rekommenderar att fortsätta med att utbilda årligen, att enhetschefer påminner i möten med sina medarbetare och att informera genom t ex nyhetsbrev och intranätet. DSO rekommenderar även att kommunicera till de med roller inom systemförvaltningen vad deras arbetsuppgifter och ansvarsområden är.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Miljöförvaltningen har goda rutiner och mallar för tröskelanalyser och konsekvensbedömningar, men inga nya tröskelanalyser har genomförts och tidigare rekommendationer om behandling av anställdas personuppgifter har ännu inte följts. Det senare beror på att verksamheten avvaktar färdigställandet av en utredning om personuppgiftsansvar av SLK. Det finns sannolikt behov av en konsekvensbedömning för behandling av anställdas känsliga personuppgifter (exklusive flextidsredovisningssystemet) och en översyn av befintliga bedömningar, som inte har uppdaterats sedan de gjordes. Införandet av AI-assistenten kan innebära ny personuppgiftsbehandling och kräver därför en tröskelanalys.

DSO rekommenderar att genomföra tröskelanalyser och revidera befintliga konsekvensbedömningar i den mån det behövs efter en översyn.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Miljöförvaltningen uppger att verksamhetens arbete i stort ser likadant ut varje år. När det inkommer nya uppdrag eller arbete förändras finns rutiner för att fånga upp det. DSO rekommenderar att fortsätta med utbildning, kommunikation och upprätthålla rutiner kring dataskydd. DSO rekommenderar att göra en översyn av befintliga konsekvensbedömningar och uppdatera dem om det behövs.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		I dagsläget finns inga dokumenterade tröskelanalyser. Stadsledningskontoret erbjuder en mall för tröskelanalys. Miljöförvaltningen uppger att de hade använt den när de identifierar ett sådant behov. DSO ser inga brister i förevarande kategori (se dock nedan)
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Verksamheten använder Stadsledningskontorets mall för konsekvensbedömning avseende dataskydd. Verksamheten har också en egen rutin för konsekvensbedömningar.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Se nedan.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		DSO rekommenderade verksamheten i GDPR årsrapport 2024 att genomföra en tröskelanalys för den del av behandling av anställdas personuppgifter som omfattar känsliga personuppgifter. Verksamheten har avvaktat utredning/vägledning från SLK och har ännu inte genomfört åtgärden. DSO rekommenderar att verksamheten genomför en tröskelanalys och, i det fall det krävs, en konsekvensbedömning avseende dataskydd.

Den registrerades rättigheter

Sammanfattning

Miljöförvaltningen har rutiner och mallar för att hantera begäranden från registrerade, men stickprov visar brister i registerutdrag enligt artikel 15, där faktiska personuppgifter och fullständig information saknas. Under året inkom tre begäranden om tillgång, en begäran om radering och ett klagomål, alla besvarade inom en månad. Förmågan bedöms som huvudsakligen god, men rutiner har inte följts, vilket är allvarligt då rätten till tillgång är central i GDPR. DSO rekommenderar bland annat att säkerställa användning av rutiner och ta fram exempelmallar för kompletta registerutdrag.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Stickprov visar att en registrerad inte har fått tillgång till de personuppgifter som behandlas vid begäran om registerutdrag. DSO:s granskning visar att rutin och mall för hantering av begäranden är bristfälliga. DSO rekommenderar att ta fram rutiner och mallar som skapar förutsättningar för registerutdrag för de kategorier av registrerade som behandlas, i synnerhet anställda.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Antal begäranden: 4
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		I intervjuer med Miljöförvaltningen framgår att begäranden från registrerade har besvarats inom en månad, vilket uppfyller kraven i enlighet med GDPR.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		DSO har tagit del av ett stickprov som avsåg begäran om tillgång (registerutdrag). Stickprovet visar att registerutdraget saknar en kopia på behandling i enlighet med kravet i artikel 15 GDPR. Öppenhet och transparens är en av GDPR:s grundläggande principer, vilket innebär att risken är betydande. DSO rekommenderar verksamheten att ta fram rutiner och mallar som skapar förutsättningar för registerutdrag för de kategorier av

		registrerade som behandlas, i synnerhet anställda.

Personuppgiftsincidenter

Sammanfattning

Den personuppgiftsansvarige har goda rutiner och genomför flera insatser för att höja kunskapen om personuppgiftsincidenter, bland annat årliga utbildningar, intranätinformation och påminnelser. Rutiner för hantering av incidenter är ändamålsenliga och följs, och lämpliga riskanalyser görs vid utredning av incidenter. Under året har 12 incidenter dokumenterats och en har anmälts till IMY, kopplad till cyberangreppet mot Miljödata i Karlskrona AB, vilken belyser riskerna med den otydliga fördelningen och regleringen av det kommuninterna personuppgiftsansvaret. DSO bedömer att hanteringen är god och rekommenderar fortsatt kunskapsspridning, användning av verkliga incidenter i kommunikation samt att verka för förtydligande av personuppgiftsansvaret tillsammans med Stadsledningskontoret.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		Medarbetarna får utbildning, information och påminnelser om personuppgiftsincidenter regelbundet (utbildning, e-utbildning, information på intranätet och påminnelser i respektive enhet). DSO rekommenderar att fortsätta med detta.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		DSO bedömer att verksamheten har goda rutiner och förutsättningar för att upptäcka och hantera personuppgiftsincidenter. DSO rekommenderar att fortsätta utbilda och medvetandegöra anställda om personuppgiftsincidenter.
Hur många personuppgiftsincidenter har dokumenterats under året?		Antal: 12
Hur många personuppgiftsincidenter har anmälts till IMY under året?		Antal: 1 personuppgiftsincident har anmälts till IMY. Incidenten avsåg testmiljön i systemet för arbetsmiljöincidenter, Stella, som hanterades av Stadsledningskontoret.

Överföring till tredje land

Sammanfattning

Miljöförvaltningen har i registerförteckningen dokumenterat tredjelandsöverföringar kopplat till användning av sociala medier (Facebook, Linkedin, Instagram, Flickr). Överföringarna omfattas huvudsakligen av EU:s adekvansbeslut för USA och Storbritannien. Lagring av information, inklusive personuppgifter, för Miljöförvaltningens kärnverksamhet är inom Sverige, eller åtminstone EU/EES, vilket ger ett högt skydd för personuppgifter. DSO bedömer att överföringar sker i mycket begränsad omfattning, men rekommenderar att dokumentera saknade uppgifter i registerförteckningen (två behandlingar) samt ställa frågan till Stadsledningskontoret om kartläggning av överföringar till länder utan adekvansbeslut vid användning av sociala medier.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Förekomsten eller avsaknaden av tredjelandsöverföring dokumenteras i registerförteckningen. Två behandlingar saknas information om eventuell tredjelandsöverföring. Det bör åtgärdas. Utöver det rekommenderas den personuppgiftsansvarige att fortsätta dokumentera eventuell tredjelandsöverföring så som redan sker.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Tredjelandsöverföring sker i mycket begränsad omfattning. Två behandlingar innebär tredjelandsöverföring (sociala medier). Här saknas dokumentation om överföringsverktyg. Den personuppgiftsansvarige bör komplettera dokumentationen med information om detta.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Granskningen visar att TIA inte har genomförts för användningen av sociala medier. Huvudsakligen sker dock överföring till länder som omfattas av adekvansbeslut. SLK har ett inriktningsbeslut och information på intranätet. DSO rekommenderar Miljöförvaltningen att fråga SLK om det finns en kartläggning av överföring till andra tredjeländer. Om inte utgör detta en risk.

		DSO rekommenderar att bevaka adekvansbeslutens giltighet (Storbritannien, USA).

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 3: Översyn av det kommuninterna personuppgiftsansvaret

Bilaga 4: Granskning av personuppgiftsbiträdesavtal

Bilaga 5: Omvärldsbevakning

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Denna bilaga innehåller en beskrivning av syftet med respektive obligatoriskt område samt en mer detaljerad redovisning av dataskyddsombudets granskning och slutsatser. Här framgår vilka iakttagelser som gjorts och vilken information som samlats in under granskningsarbetet av de sex obligatoriska rapporteringsområdena. För varje område redovisas de underlag som har använts, de iakttagelser som har gjorts samt hur dessa har utgjort grunden för dataskyddsombudets riskbedömning och rekommenderade åtgärder.

1. Register över personuppgiftsbehandlingar

Syftet med området

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgiftsbehandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att rapportera om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Antal behandlingar som är registrerade?

139 behandlingar har registrerats i registerförteckningen den 3:e november 2025.

Har verksamheten ändamålsenliga rutiner som möjliggör att nya/förändrade behandlingar registreras?

Verksamheten har dokumenterade rutiner för arbetet med att hålla registerförteckningen uppdaterad och korrekt. I intervjuer i samband med granskningen har det framgått att uppdatering genomförs vid behov och att en översyn görs årligen, vilket överensstämmer med vad som framgår av den dokumenterade rutinen. Att förteckningen är uppdaterad nyligen och att DSO inte har noterat något som uppenbart saknas talar också för att rutinerna är välfungerande.

DSO bedömer att rutinerna är lämpliga för att hålla registerförteckningen uppdaterad.

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?

Den senaste versionen av registerförteckningen som har tillhandahållits DSO är daterad till den 3:e november 2025. Under årets intervjuer med arkivarien som ansvarar för samordningen av registerförteckningen har det framgått att uppdatering av registerförteckningen är välfungerande. DSO har inte noterat något som saknas i registerförteckningen och bedömer mot bakgrund av ovanstående att nödvändiga uppdateringar har gjorts.

Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?

Registerförteckningen innehåller samtliga obligatoriska kategorier av uppgifter som krävs enligt artikel 30 GDPR. Utöver detta innehåller förteckningen också information om relevanta informationsklassningar, var personuppgifterna finns (system), handlingstyper och allmän beskrivning av säkerhetsåtgärder.

Kontrollen visar att registerförteckningen är fullständig.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Föregående år konstaterade DSO att det inte fanns några risker att rapportera på området, vilket är också är 2025 års slutsats. Ett par behandlingar har tillkommit i förteckningen, vilket DSO tolkar som ett tecken på att förteckningen uppdateras i enlighet med rutiner.

Föregående år rekommenderades verksamheten att dokumentera genomförda informationsklassningar i registerförteckningen, vilket har gjorts under året. Resultatet av insatsen är att det finns en överblick över vilka informationsklassningar som har genomförts, och hur dessa kan hittas vid behov.

Dataskyddsombudets bedömning samt rekommendationer

DSO bedömer att den personuppgiftsansvarige har mycket ändamålsenliga rutiner som följs genom året. Samordningen av uppdateringen är välfungerande och kvaliteten på registerförteckningen är, utifrån DSO:s bedömning, god.

Registerförteckningen är omfattande, och föregående år rekommenderades verksamheten att formatera om registret till tabellformat för bättre överblick och sökbarhet. Rekommendationen kvarstår.

DSO rekommenderar att verksamheten fortsätter arbeta med registerförteckningen systematiskt på så sätt som redan görs, och upprätthåller den medvetenhet som finns i verksamheten om anmälan om ny personuppgiftsbehandling. Det är till exempel bra att avdelningschefer och enhetschefer påminns, och DSO rekommenderar att dessa påminnelser och information ska fortsätta.

2. Säkerhet i samband med behandlingen

Bakgrund och syfte

Personuppgiftsansvarig ska tillse att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna eller att uppgifterna förloras.

Personuppgiftsansvarig behöver bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. Genom riskanalyser identifierar informationsägaren risker och väljer åtgärder för att minska riskerna. Risker i samband med personuppgiftsbehandling är en typ av risk som informationsägaren behöver omhänderta i riskanalyser.

Att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner medför att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd. Den personuppgiftsansvariga måste kunna *visa* hur GDPR efterlevs och att det finns styrdokument och rutiner är en viktig del i detta.

Syftet med detta rapporteringsområde är därmed att rapportera huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser. Vidare bedömer DSO huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

Kontroller och iakttagelser gjord av dataskyddsombudet

Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?

DSO har gjort tre stickprov vilket omfattade informationsklassningar av Ecos (ärendehanteringssystem), Agresso (ekonomi- och inköpssystem) samt LISA (HR-system).

Informationsklassningsprotokollen för Agresso och LISA Självservice beaktar personuppgifter. DSO bedömer att KRT[1] i individperspektivet har en lämplig klassificering med hänsyn till vilka personuppgifter som behandlas och i vilken kontext. Protokollet för

[1] Konfidentialitet, Riktighet, Tillgänglighet.

Agresso saknar dock information om huruvida skyddade personuppgifter behandlas. Bägge protokoll är från 2025 vilket DSO ser som ett tecken på att de är uppdaterade.

Ecos är Miljöförvaltningens ärendehanteringssystem och utgör ett centralt system som stödjer Miljöförvaltningens kärnverksamhet. Miljöförvaltningen meddelar att informationsklassningen för Ecos har gjorts i KLASSA. DSO har tagit emot ett aggregerat resultat över klassningen där det framgår att det sammantaget är klassat 2, 2, 2 för KRT[2]. Det är sannolikt en rimlig klassning. DSO har dock inte haft möjlighet att kontrollera klassningen i sin helhet. Informationssäkerhetssamordnare uppger dock att de lägger mycket tid på klassning av Ecos och dataskydd och konfidentialitet för personuppgifterna där. DSO har ingen anledning att tvivla på detta.

Datumstämpeln för resultatet av klassningen av Ecos är 2023, vilket innebär att klassningen är genomförd för drygt två och ett halvt år sedan. Det framgår av resultatet att flera rekommenderade åtgärder så som behörighetshantering, åtkomstbegränsning och spårbarhet inte är uppfyllda vilket utgör en risk om verksamheten inte har åtgärdat detta. I intervjuer framgår dock till exempel att behörighetshantering sker löpande när medarbetare börjar och slutar.

Mot bakgrund av hur centralt systemet är, att det kan hantera känsliga personuppgifter och innebär en relativt omfattande behandling (åtminstone avseende mängden ärenden) är det viktigt att säkerhetsåtgärder för systemet genomförs om de ännu inte gjort det. Utöver det är klassningen aningen föråldrad och DSO rekommenderar att verksamheten uppdaterar den, eftersom klassningar bör ses över regelbundet.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?

Stockholms stads informationssäkerhetsarbete är nära förankrat med, och stödjer, dataskyddsarbetet och införandet av lämpliga tekniska och organisatoriska skyddsåtgärder i enlighet med artikel 32 GDPR. Informationssäkerhetsarbetet vid Miljöförvaltningen styrs bland annat genom Riktlinje för informationssäkerhet i Stockholms stad[3] och Tillämpningsanvisning till stadens riktlinje för informationssäkerhet[4]. Stadens centrala tillämpningsanvisning kompletteras av Lokal anvisning för informationssäkerhet (beslutad 2023-12-15)[5].

En organisatorisk skyddsåtgärd är att det finns väl utformade personuppgiftsbiträdesavtal, inklusive instruktioner, i de fall Miljöförvaltningen använder externa aktörer som personuppgiftsbiträden. Lokal anvisning för informationssäkerhet saknar information om vem

---

[2] Konfidentialitet, Riktighet, Tillgänglighet,

[3] Riktlinje för informationssäkerhet i Stockholms stad, https://intranat.stockholm.se/globalassets/stod-i-arbetet/rattsfragor-och-juridiskt-stod/informationssakerhet-i-staden/informationssakerhet/stadsledningskontoret/riktlinje-for-informationssakerhet.pdf, hämtad 2025-12-15.

[4] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, https://intranat.stockholm.se/globalassets/stod-i-arbetet/rattsfragor-och-juridiskt-stod/informationssakerhet-i-staden/informationssakerhet/stadsledningskontoret/tillampningsanvisning-informationssakerhet-v-1-3.pdf, hämtad 2025-12-15.

[5] Lokal anvisning för informationssäkerhet, Miljöförvaltningen, lokal-anvisning-for-informationssakerhet-miljoforvaltningen-2024-03-04.pdf, hämtad 2025-12-15.

som är ansvarig för att tillse att personuppgiftsbiträdesavtal tecknas i det fall det krävs[6]. Ansvarsfördelningen framgår dock av den centrala tillämpningsanvisningen[7] och den lokala anvisningen innehåller en generell hänvisning till tillämpningsanvisningen.[8]

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?

DSO bedömer att de styrande dokumenten och rutinerna väsentligen är implementerade och kända. Verksamheten har i intervjuer under granskningsperioden berättat att de har kommit långt med utbildning, checklistor och informationsmaterial. Relevanta rutiner och mallar har gjorts tillgängliga på intranätet. Utöver det är GDPR-gruppen tillgängliga för frågor, vilka de tar emot löpande.

DSO har i årets granskning identifierat att det kan finnas ett behov av att ytterligare kommunicera om ansvaret och arbetsuppgifterna för objektledare och objektägare. DSO rekommenderar mot bakgrund av detta att informationssäkerhetsarbetet – som också syftar till att stärka dataskyddsarbetet avseende t ex tekniska och organisatoriska skyddsåtgärder – stärks genom att utbilda och kommunicera tydligt om rollerna inom IT-förvaltning/systemförvaltning för dem det är aktuellt för. Detta för att ytterligare stärka dataskyddsarbetet.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

I förra årets årsrapport rekommenderade DSO verksamheten att utreda om samtliga personuppgiftsbehandlingar har informationsklassats. Den åtgärden har vidtagits under året. DSO bedömde överlag att styrande dokument var överskådliga, lättillgängliga, omfattande och utformade för att kunna användas av alla anställda. DSO bedömer fortsatt att rutinerna och styrdokumenten ger ett bra stöd för dataskyddsarbetet och bedömningen av risken är fortsatt ”gul”.

Dataskyddsombudets bedömning samt rekommendationer

DSO bedömer att de organisatoriska skyddsåtgärderna i Miljöförvaltningen, så som informationsmaterial, kommunikation, utbildning och styrdokument, är goda. Som framgår ovan kan arbetet med systemförvaltning och leverantörshantering stärkas, t ex genom att påminna om vilka ansvarsområden som finns för respektive roller.

---

[6] Ibid, s 8 och 13, hämtad 2025-12-15.

[7] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, s 29, hämtad 2025-12-15.

[8] I Lokal anvisning för informationssäkerhet, s 8, framgår: *Att tillse att stadens riktlinjer och tillämpningsanvisningar följs vad gäller informationssäkerhet för it-tjänster.*

Arbetet med kartläggningen av informationsklassningar som har genomförts under året stärker strukturen i dataskyddsarbetet.

DSO är positivt inställd till de resurser som förvaltningen lägger på utbildning och *awareness*. DSO rekommenderar att fortsätta med alla de initiativ som förvaltningen redan genomför (e-utbildning, årlig utbildning, påminnelser i mejl). Utbildning är centralt för att bygga en stark dataskyddskultur och medvetenhet om rutiner och risker.

DSO rekommenderar verksamheten att uppdatera informationsklassningen för Ecos då granskningen har visat att den senaste klassningen är gjord 2023.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en s.k. tröskelanalys.

En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utfös för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas.

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

Kontroller och iakttagelser gjord av dataskyddsombudet

Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?

DSO har i intervjuer blivit informerad om att det är ovanligt att Miljöförvaltningen ändrar befintliga eller genomför nya personuppgiftsbehandlingar. I de fall det händer får GDPR-gruppen reda på det och är stöd till verksamheten.

Det finns en mall för tröskelanalys på intranätet och rutin för genomförande av konsekvensbedömning, där det framgår när en konsekvensbedömning behöver genomföras. DSO bedömer att rutinerna är goda och har inga rekommendationer på området.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Verksamheten uppger att de kommer att genomföra tröskelanalyser i det fall nya eller förändrade personuppgiftsbehandlingar aktualiseras. I dagsläget har ingen tröskelanalys genomförts för nya eller förändrade personuppgiftsbehandlingar. DSO noterade 2024 att verksamheten inte har gjort en tröskelanalys (eller konsekvensbedömning) för behandling av anställdas personuppgifter, bortsett från för flextidsredovisningssystemet. DSO rekommenderade då att genomföra en tröskelanalys. Verksamheten har ännu inte färdigställt någon tröskelanalys. Anledningen är att verksamheten bedömer att det är osäkert hur personuppgiftsansvaret är fördelat och inväntar en utredning som leds av juridiska avdelningen vid Stadsledningskontoret.

I intervjuer har verksamheten informerat DSO om ett pågående införlivande av en AI-assistent (Intric) i Miljöförvaltningen. DSO rekommenderar verksamheten att genomföra en tröskelanalys med anledning av en möjlig ny personuppgiftsbehandling, beroende på hur verktyget används. Användning av AI-verktyg uppfyller åtminstone ett av kriterierna i IMY:s förteckning över när en konsekvensbedömning krävs.[9] Om en behandling uppfyller två kriterier är den personuppgiftsansvarige skyldig att genomföra en konsekvensbedömning.

Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?

Miljöförvaltningen använder Stadsledningskontorets mall. DSO bedömer att den håller god kvalitet och uppfyller kraven för en konsekvensbedömning enligt artikel 35. Utöver det har Miljöförvaltningen även en rutin för konsekvensbedömning.[10] I denna framgår bland annat när en konsekvensbedömning behöver genomföras och vem som har ansvar för att genomföra en. DSO bedömer att mallar och rutiner håller god kvalitet.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

DSO konstaterade i årsrapporten 2024 att det sannolikt saknas en konsekvensbedömning avseende dataskydd för behandling av anställdas personuppgifter (särskilt de känsliga personuppgifterna enligt artikel 9). DSO rekommenderade 2024 att genomföra en tröskelanalys för att bedöma om det krävs, eller om det finns något tillämpligt undantag.

DSO rekommenderar att genomföra tröskelanalysen avseende behandling av anställdas personuppgifter och vidta nödvändiga åtgärder med anledning av resultatet.

---

[9] Integritetssskyddsmyndigheten, Förteckning enligt artikel 35.4 i Dataskyddsförordningen, diarienummer 2018-13200, 2019-01-16.

[10] Rutin för konsekvensbedömning enligt artikel 35 dataskyddsförordningen, https://intranat.stockholm.se/globalassets/stod-i-arbetet/rattsfragor-och-juridiskt-stod/informationssakerhet-i-staden/gdpr/gdpr-och-personuppgifter/miljoforvaltningen/rutin-for-konsekvensbedomning-enligt-artikel-35-dataskyddsforordningen-221129.pdf, ver 1.0, 2021-10-11, hämtad 2025-12-15.

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?

Ja, DSO bedömer att den personuppgiftsansvarige har identifierat alla personuppgiftsbehandlingar som kräver en konsekvensbedömning. Det är dock sannolikt att den personuppgiftsansvarige är skyldig att genomföra en konsekvensbedömning om behandling av anställdas personuppgifter (se ovan).

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Föregående år rapporterade DSO samma bedömning och resultat som ovan. DSO rekommenderade i GDPR Årsrapport 2024 även att se över befintliga konsekvensbedömningar, då de ska ses som levande dokument. GDPR-gruppen vid Miljöförvaltningen har informerat DSO om att de ska göra detta årligen från och med 2026, vilket DSO ser positivt på.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet konstaterar att Miljöförvaltningens personuppgiftsbehandling framför allt inte omfattar sådan behandling som aktualiserar skyldigheten att genomföra en konsekvensbedömning. Miljöförvaltningen har i all väsentlighet god kontroll på området men konsekvensbedömningar omhändertar till sin natur – bedömning som medför sannolikt höga risker för registrerade – höga risker. Därmed finns det ändå en risk både avseende den konsekvensbedömning som eventuellt saknas och de befintliga konsekvensbedömningarna som inte har genomgått en översyn sedan de genomfördes.

- DSO rekommenderar även att verksamheten genomför en tröskelanalys för den del av behandling av anställdas personuppgifter som omfattar känsliga personuppgifter, i enlighet med rekommendationen i GDPR Årsrapport 2024.
- DSO rekommenderar att verksamheten gör en översyn av befintliga konsekvensbedömningar i syfte att kontrollera om någon av dem behöver revideras, i enlighet med rekommendationen i GDPR Årsrapport 2024.
- DSO rekommenderar att verksamheten genomför en tröskelanalys av eventuell personuppgiftsbehandling kopplat till införlivandet av AI-assistenten.

4. Den registrerades rättigheter

Bakgrund och syfte

Den registrerade har ett antal rättigheter enligt GDPR. Den registrerade kan bland annat begära tillgång (registerutdrag), rättelse eller radering. Den som är personuppgiftsansvarig har att tillmötesgå en begäran enligt de krav som finns.

Syftet med detta rapporteringsområde är att kontrollera huruvida det finns ändamålsenliga mallar samt rutiner för besvarande av rättighetsbegäran, huruvida inkomna begäranden har

hanterats inom den tidsram som finns att förhålla sig till samt huruvida svaren till de registrerade, baserat på ett antal stickprov, uppfyller lagkraven.

Kontroller och iakttagelser gjord av dataskyddsombudet

Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?

Miljöförvaltningen har som stöd i sitt arbete flera rutiner och stöddokument:

- Rutin för tillvaratagande av de registrerades rättigheter enligt artiklarna 16-22 dataskyddsförordningen (ver 1.2, rev 2025-05-14)
- Rutin vid begäran om registerutdrag (rev. 2022-11-23)
- Mall för information vid registerutdrag

Rutinen för tillvaratagande av de registrerades rättigheter ger ett bra stöd för hantering av registrerades rättigheter enligt de artiklar som omfattas. Rätten till tillgång omfattas inte av rutinen. Rutinen vid begäran om registerutdrag är en praktisk genomgång om hur man går till väga för att hantera en begäran om registerutdrag med t ex slagningar i olika system. Begärandena ska hanteras av Arkiv och registratur, och ska skickas till funktionen om en annan anställd tar emot dem.

Mallen för information vid registerutdrag ger förutsättningar för att ge den registrerade tillgång till information om behandlingen (ändamål, kategorier, mottagare, varaktighet etc). Det finns dock inget utrymme i mallen för att tillhandahålla de faktiska personuppgifterna (kopia på behandlingen). DSO förutsätter att dessa normalt skickas i en bilaga vid sidan av den ifyllda mallen med beskrivningen.

Mot bakgrund av ovanstående har den personuppgiftsansvarige förutsättningar att tillgodose registrerades rättigheter. Möjligtvis kan förutsättningarna förbättras genom att skapa ifyllda mallar för de vanliga typerna av registrerade som stöd vid registerutdrag. Till exempel en mall för medborgare, en för Miljöförvaltningens vanligaste ”kunder” och en för anställda.

Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?

Miljöförvaltningen har tagit emot tre registerutdrag, en begäran om radering och ett klagomål om felaktig behandling. Klagomålet ledde till en uppdatering av en rutin.

Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?

Begärandena har besvarats inom en månad.

Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?

DSO har gjort ett stickprov på svaren till de registrerade, ett registerutdrag. Begäran om registerutdrag gjordes av en anställd. I det aktuella fallet sammanställde

Stadsledningskontoret en del av registerutdraget, och Miljöförvaltningen en annan del.[11] DSO har tagit del av den del som Miljöförvaltningen sammanställde. Nedanstående avser således enbart det.

Den registrerade har använt sin rätt till tillgång enligt artikel 15. En begäran om registerutdrag, eller rätten till tillgång, består av tre komponenter:

- bekräftelse om huruvida personuppgifter har behandlats
- tillgång till **dessa personuppgifter**
- tillgång till information om behandlingen, t ex ändamål kategorier av personuppgifter och mottagare, behandlingens varaktighet, de registrerades rättigheter och om relevant lämpliga skyddsåtgärder vid överföringar till tredjeland

Europeiska dataskyddsstyrelsen (EDPB) skriver i sin vägledning om rätten till tillgång[12] att detta kan omfatta en obegränsad mängd uppgifter. Tillgång till personuppgifter syftar på tillgången till de faktiska personuppgifterna, inte bara en allmän beskrivning av uppgifterna eller enbart en hänvisning till de kategorier av personuppgifter som behandlas av den personuppgiftsansvarige. Syftet är att den registrerade ska få information om den faktiska behandlingen, för att kunna kontrollera till exempel riktigheten och lagligheten. Den personuppgiftsansvarige behöver således tillhandahålla en kopia av de personuppgifter som behandlingen avser (artikel 15.3). Det är dock inte nödvändigt med en kopia på själva handlingen (det är inte samma sak som utlämnande av allmän handling), utan en kopia av de personuppgifter som behandlas.

Den tredje delen av rätten till tillgång är information om behandlingen enligt artikel 15.1 a-h och i relevanta fall 15.2 (tredjelandsöverföring). Den här informationen kan t ex hämtas från registerförteckningen.

Det är inte tillräckligt att skicka information om de kategorier av personuppgifter som behandlas så som "namn", "adress".[13]

Miljöförvaltningens registerutdrag till den registrerade har innehållit kategorier av personuppgifter. Registerutdraget saknar tillgång till information om behandling och tillgång till de faktiska personuppgifterna. Registerutdraget är därmed ofullkomligt och har stora brister i förhållande till GDPR:s krav, vägledning på området från Europeiska dataskyddsstyrelsen och DSO:s rekommendation.[14]

---

[11] På grund av att anställdas personuppgifter behandlades i en miljö som Miljö- och hälsoskyddsnämnden inte hade åtkomst till (Stella).

[12] Riktlinjer 01/2022 om registrerades rättigheter – rätt till tillgång, ver 2.1, Europeiska dataskyddsstyrelsen.

[13] Ovanstående har även kommunicerats till den personuppgiftsansvarige i svar på mejl om rätten till tillgång 2025-09-18.

[14] Mejl till den personuppgiftsansvarige, 2025-09-18.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

I föregående årsrapport bedömde DSO att verksamhetens förmåga och förutsättningar att hantera begäranden från registrerade var god. DSO rekommenderade att komplettera en rutin med information om radering från backups (vid begäran av radering). Under förevarande granskning har stickprov visat att registerutdrag inte hanteras i enlighet med GDPR. DSO bedömer fortsatt att styrdokument och stödmaterial är tillräckliga.

Dataskyddsombudets bedömning samt rekommendationer

DSO bedömer att verksamhetens förmåga att hantera begärandena huvudsakligen är god. Ett stickprov har dock visat att rutiner och mallar inte har följts, vilket resulterade i att en registrerad inte fick sina rättigheter tillgodosedda enligt GDPR artikel 15 (rätten till tillgång). Registrerades rätt till tillgång är central i GDPR eftersom det är ett sätt för den registrerade att kontrollera att personuppgifter som behandlas är korrekta samt att det sker på ett lagligt sätt och som den registrerade kan förvänta sig. Om den personuppgiftsansvarige brister i rätten tillgång innebär det därmed att de registrerade förlorar möjligheten att kontrollera behandlingars laglighet, korrekthet och riktighet (bland annat). Därför ser DSO allvarligt på att stickprovet har visat att rätten till tillgång inte har tillgodosetts korrekt.

DSO rekommenderar den personuppgiftsansvarige att vidta åtgärder för att tillse att rutiner och mallar används för att tillgodose begäranden om rätten till tillgång. Exempelvis kan den personuppgiftsansvarige ta fram exempel på hur registerutdrag kan se ut för de vanligaste kategorier av registrerade som verksamheten hanterar.

5. Personuppgiftsincidenter

Bakgrund och syfte

Med begreppet personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Om en inträffad personuppgiftsincident medför en risk för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från upptäckt. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste de informeras utan onödigt dröjsmål.

Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras.

Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

Kontroller och iakttagelser gjord av dataskyddsombudet

Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?

I intervjuer har framgått att den personuppgiftsansvarige genomför flera åtgärder för att säkerställa att medarbetare har kunskap om personuppgiftsincidenter och hur de ska rapporteras:

- Årlig utbildning om GDPR där personuppgiftsincidenter ingår,
- Instruktioner och information på intranätet.
- Påminnelser till avdelningschefer om att informera sina medarbetare.
- Kommunikation i enhetsmöten.
- Stadens centrala e-utbildningar.

DSO bedömer att den personuppgiftsansvarige gör goda insatser för att tillhandahålla medarbetare med kunskap och förutsättningar för att upptäcka och rapportera personuppgiftsincidenter.

Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?

DSO konstaterar att det finns information på intranätet inklusive ”Rutin och vägledning vid händelse av en personuppgiftsincident.[15] DSO bedömer att dessa rutiner är ändamålsenliga och skapar goda förutsättningar för korrekt hantering av personuppgiftsincidenter. DSO har även under året blivit informerad om personuppgiftsincidenter löpande. Dokumentationen visar att den personuppgiftsansvarige gör lämpliga riskanalyser och tar hänsyn till de registrerade vid bedömning av risken.

Hur många personuppgiftsincidenter har dokumenterats under året?

Under 2025 har den personuppgiftsansvarige dokumenterat 12 personuppgiftsincidenter. Föregående år var antalet 6.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

En personuppgiftsincident har anmälts till IMY. Incidenten avsåg cyberangreppet mot systemleverantören Miljödata i Karlskrona Aktiebolag (Miljödata) som tillhandahåller ett system för hantering av arbetsmiljöincidenter – Stella. Systemet Stella är inte i produktion hos Stockholms stad, utan för Stockholms stads del gällde det en testmiljö där anställdas personuppgifter behandlades för att verifiera integrationen mellan stadens IT-miljö och Stella. Stadsledningskontoret har haft i uppdrag att upphandla och tillhandahålla ett sådant system och vid införandet har Stadsledningskontoret för verifieringsändamål skapat en integration som inneburit att samtliga anställdas personuppgifter har överförts till Stella.

[15] Rutin och vägledning vid händelse av en personuppgiftsincident, rev. 2020-12-18.

Det råder sedan tidigare osäkerhet kring det kommuninterna personuppgiftsansvarets fördelning. I dagsläget förhåller det sig så att kommunstyrelsen (Stadsledningskontoret) tecknar personuppgiftsbiträdesavtal å nämndernas vägnar. På grund av det hanterades personuppgiftsincidenten i enlighet med det förhållningssättet, trots att Miljö- och hälsoskyddsnämnden varken har haft uppdraget att upphandla ett system för arbetsmiljöincidenter, eller har haft rådighet över eller insyn i arbetet med uppdraget.

Mot bakgrund av detta gjorde Miljö- och hälsoskyddsnämnden en anmälan till IMY om incidenten, informerade anställda och dokumenterade incidenten internt.

DSO ställer sig frågande till att det är Miljö- och hälsoskyddsnämden som är den personuppgiftsansvarige för behandlingen som har skett för verifiering av ett system som Stadsledningskontoret har haft i uppdrag att införa, och som ännu inte är i drift hos nämnderna.

Cyberattacken mot Miljödata omfattade flera organisationer och ledde till att personuppgifter om över en miljon svenskar, inklusive anställda vid Stockholms stad, offentliggjordes på darknet.[16] Säkerhetsåtgärderna i Stockholms stads testmiljö har varit utformade för att motsvara produktionsmiljöns nivå. Med anledning av incidenten genomför IMY tillsyn av Miljödata för att granska om det har funnits åtgärder för att för att bedöma om lämpliga säkerhetsåtgärder har vidtagits med hänsyn till de risker som är förknippade med den behandling av personuppgifter som utförs inom deras tjänster.[17] Personuppgiftsincidenter kan inträffa trots väl implementerade skyddsåtgärder. DSO uttalar sig inte om säkerhetsåtgärdernas effektivitet då insyn saknas.

Det konstateras dock att bristande tydlighet kring det interna ansvaret för personuppgifter har lett till att Miljö- och hälsoskyddsnämnden inte varit informerad om hanteringen av de personuppgifter de ansvarar för. Detta har resulterat i att berörda registrerade, exempelvis anställda, inte har fått information om hur deras personuppgifter behandlas, särskilt när behandlingen sker i testmiljö. Denna brist är inte begränsad till Stella. DSO utvecklar det här i granskningen i bilaga 3.

Utredning om personuppgiftsansvarets fördelning pågår hos den juridiska avdelningen vid Stadsledningskontoret.[18]

DSO anser att Miljö- och hälsoskyddsnämnden har hanterat incidenten bra med de förutsättningar som har funnits.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

I 2024 års rapport bedömde DSO att verksamhetens hantering av incidenter är välfungerande, med dokumenterade rutiner, kunskapshöjande insatser och i övrigt goda förutsättningar. DSO

---

[16] SVT Nyheter, Cyberattack mot Miljödata | SVT Nyheter, hämtad 2025-12-15.

[17] Integritetsskyddsmyndigheten, Tillsyn: Miljödata i Karlskrona AB, hämtad 2025-12-15.

[18] Enligt mejl till DSO från representant vid Stadsledningskontorets juridiska avdelning, 2025-12-09.

noterade att antalet rapporterade personuppgiftsincidenter är lågt vilket kan innebära ett mörkertal. DSO rekommenderade därför den personuppgiftsansvarige att lägga särskild fokus på utbildning och att sprida kunskap.

I år är antalet dokumenterade personuppgiftsincidenter det dubbla, jämfört med 2024. Ett ökat antal kan antingen tillskrivas god dataskyddskultur och medvetenhet, eller mer slarv, sämre säkerhet och/eller högre hot. DSO bedömer att Miljöförvaltningens kunskapshöjande och medvetandegörande insatser är goda och vill med viss försiktighet utgå från att antalet har dubblerats med anledning av det förra.

DSO bedömer fortsättningsvis att de genomförda insatserna för att höja kunskapen och medvetenheten är bra. Verksamheten kan dock göra ännu mer (se ovan under första rubriken, stycke 4).

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten hanterar personuppgiftsincidenter på ett sätt som tyder på hög dataskyddsmognad. DSO rekommenderar att den personuppgiftsansvarige fortsätter sprida kunskap, medvetenhet och information om personuppgiftsincenter och vill uppmuntra om att påminna flera gånger om året.

Ett sätt att öka medvetenheten och förmågan hos medarbetare ytterligare är att använda personuppgiftsincidenter som anmäls i kommunikationsmaterial. När personuppgiftsincidenten är utredd och hanterad kan verksamheten berätta för medarbetare om incidenten, varför det var en incident och hur den bedömdes. På så sätt konkretiseras personuppgiftsincidenter i Miljöförvaltningens sammanhang.

Vad gäller personuppgiftsincidenten hos Miljödata belyser den risker som uppstår för registrerade när personuppgiftsansvaret är oklart eller otillräckligt utrett och fastställt. En nämnd bör endast ha ett personuppgiftsansvar inom kommunen för den behandling av personuppgifter som de faktiskt kan påverka och som faller inom dess faktiska kontroll, det vill säga vad de bestämmer ändamål och medel för enligt artikel 4.7 GDPR. Förvaltningen bör gemensamt med främst stadsledningskontoret kräva förtydligande av personuppgiftsansvaret, särskilt i de fall där nämnden saknar beslutsrätt för hela eller delar av personuppgiftsbehandlingen.

DSO rekommenderar följaktligen den personuppgiftsansvarige att:

- Verka för förtydligande av det kommuninterna personuppgiftsansvarets fördelning,
- Fortsätta med kunskapshöjande insatser och medvetandegörande för anställda om personuppgiftsincidenter, till exempel genom att använda verkliga exempel i kommunikation.

6. Överföring till tredje land

Bakgrund och syfte

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att

överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.[19]

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelandsöverföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Den personuppgiftsansvarige dokumenterar tredjelandsöverföringar i registerförteckningen. Registerförteckningen håller god kvalitet. Miljöförvaltningen uppger i intervjuer att de undviker att använda tjänster som innebär tredjelandsöverföring. Mot bakgrund av det är det mycket få behandlingar som innebär tredjelandsöverföring.

Två behandlingar avser behandling som sker vid användning av sociala medier för marknadsföring och kommunikation. Miljöförvaltningen använder enligt registerförteckningen Flickr, Instagram, Facebook och Linkedin. Instagram och Facebook ägs av det amerikanska företaget Meta. Linkedin ägs av det amerikanska företaget Linkedin Corporation (som ägs av Microsoft). Användning av Linkedin innebär tredjelandsöverföring till USA och Storbritannien (ej EU/EES). Både Meta och Linkedin Corporation är certifierade enligt Data Privacy Framework[20] vilket innebär att de omfattas av EU:s adekvansbeslut för USA.[21] Användningen av Meta kan innebära överföring till fler länder. DSO gör den bedömningen mot bakgrund av Metas egen lista över underbiträden där t ex Filippinerna och Singapore framgår.[22]

Två behandlingar i registerförteckningen saknar information om tredjelandsöverföring sker.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Miljöförvaltningen tillämpar adekvansbeslut som överföringsverktyg för användningen av sociala medier, som huvudsakligen innebär överföring till Storbritannien och USA. DSO påminner om att adekvansbeslutet enbart kan vara överföringsverktyg till länder som omfattas

[19] Europeiska dataskyddsstyrelsens (EDPB) Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överenstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.

[20] Data Privacy Framework, uppgift hämtad 2025-12-15.

[21] EU-kommissionen, Data protection adequacy for non-EU countries, hämtad 2025-12-15.

[22] Meta for Work list of sub-processors and subcontractors, hämtad 2025-12-15.

av adekvansbeslutet. Andra överföringar kan vara aktuella vid användning av Facebook och Instagram.

Staden informerar på intranätet sidan *GDPR och sociala medier* att adekvansbeslutet för USA möjliggör stadens närvaro i sociala medier.[23] Staden har också ett inriktningsbeslut avseende tredjelandsöverföringar till USA.[24] Utöver detta har verksamheten i intervjuer under granskningsperioden informerat att de använder sociala medier mycket restriktivt och med sunt förnuft.

Har nödvändig bedömning, ”Transfer Impact Assessment” (TIA), gjorts avseende tredjelandsöverföringarna?

DSO noterar ett visst behov av att kartlägga, eller utesluta, tredjelandsöverföringar till länder utan adekvansbeslut vid användning av Metas sociala medier.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Området ingick inte i DSO:s formella granskning föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att den personuppgiftsansvariges behandling av personuppgifter i mycket begränsad omfattning innebär tredjelandsöverföring. Kärnverksamheten för Miljöförvaltningen sker med lagring i Sverige, eller åtminstone inom EU/EES. DSO uppmuntrar Miljöförvaltningen att fortsätta prioritera behandling av personuppgifter inom EU/EES eftersom detta säkerställer full tillämpning av GDPR, tillsyn av europeiska dataskyddsmyndigheter och ett högt, rättssäkert skydd för de registrerades personuppgifter.

I den mån personuppgifter överförs till tredjeland är det huvudsakligen till länder som omfattas av adekvansbeslut (Storbritannien, USA) vid användning av sociala medier. Det kan vara nödvändigt att utreda eventuella ytterligare tredjelandsöverföringar. Staden har dock centralt informerat om sociala medier, adekvansbeslut för USA[25] och vad det innebär för användning av sociala medier. Såvitt DSO vet har ingen TIA genomförts av Stadsledningskontoret å hela stadens vägnar. DSO rekommenderar ändå den personuppgiftsansvarige att ställa frågan till Stadsledningskontoret om de har kartlagt överföringar till länder utan adekvansbeslut vid användning av sociala medier. DSO rekommenderar även den personuppgiftsansvarige att dokumentera tredjelandsöverföring eller avsaknaden av sådan där dokumentation saknas.[26]

---

[23] GDPR och sociala medier, hämtad 2025-12-15.

[24] Reviderat inriktningsbeslut avseende tredjelandsöverföringar till USA, KS 2023/241, 2023-09-14.

[25] Data Privacy Framework-certifierade organisationer i USA.

[26] Rad 108 och 178 i Miljöförvaltningens registerförteckning ver 2025-11-03.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året.

Granskning 1 – Översyn av det kommuninterna personuppgiftsansvaret

Miljö- och hälsoskyddsnämnden och DSO har sedan tidigare uppmärksammat otydligheter kring fördelningen av personuppgiftsansvaret inom Stockholms stad (så kallat kommuninternt eller stadeninternt personuppgiftsansvar). Granskningen finns i sin helhet i bilaga 3 och visar att Miljö- och hälsoskyddsnämnden saknar rådighet över vissa behandlingar, vilket leder till svårigheter i att uppfylla de skyldigheter den personuppgiftsansvarige har enligt GDPR. Detta skapar risker för bristande efterlevnad av GDPR, exempelvis avseende ansvarsskyldigheten och uppfyllandet av registrerades rättigheter, i synnerhet rätten till information. Avtal finns med externa leverantörer, men stadeninterna instruktioner mellan kommunstyrelsen och Miljö- och hälsoskyddsnämnden saknas, vilket förstärker osäkerheten.

Fråga/kontroll	Risk	Kommentar
Kommuninternt personuppgiftsansvar – otydlig fördelning begränsar förmåga att följa GDPR		Sammantaget bedömer DSO att risken som resultaten av otydligheten av det kommuninterna personuppgiftsansvaret innebär är medelhög. Incidenten som berörde Stella (Miljödata) belyste vilka risker som uppstår vid oklar ansvarsfördelning. Rekommendationerna inkluderar bland annat att verka för att reglera personuppgiftsansvaret mellan kommunstyrelsen och Miljö- och hälsoskyddsnämnden, färdigställa instruktion som reglerar förhållandet mellan Servicenämnden och Miljö- och hälsoskyddsnämnden samt att ta del av objektplaner och delta i normerande klassningar.

Granskning 2 – Personuppgiftsbiträdesavtal

Granskningen av personuppgiftsbiträdesavtal finns i sin helhet i bilaga 4. Resultatet av granskningen är att personuppgiftsbiträdesavtalen uppfyller kraven i artikel 28 GDPR. Granskningen visar även att den personuppgiftsansvarige inte har genomfört uppföljning av sina personuppgiftsbiträden. DSO bedömer sammantaget att risken på området är förhållandevis låg vad gäller personuppgiftsbiträdesavtalen. Arbete med uppföljning är dock viktigt för att säkerställa att personuppgiftsbiträden och leverantörer lever upp till krav på dataskydd och informationssäkerhet, utifrån GDPR och snart även Cybersäkerhetslagen som träder i kraft 15:e januari 2026.

Fråga/kontroll	Risk	Rekommendationer
Personuppgiftsbiträdesavtal		DSO har granskat personuppgiftsbiträdesavtal. Avtalen uppfyller kraven i artikel 28 GDPR.

		Det finns möjliga förbättringsområden som DSO beskriver i sin helhet i granskningen.
Leverantörsuppföljning		Objektägare har inte genomfört leverantörsuppföljning på de personuppgiftsbiträden de har ansvar för. DSO rekommenderar den personuppgiftsansvarige att ta fram rutin och mall för leverantörsuppföljning.

Granskning 3 – Implementering av åtgärder från GDPR Årsrapport 2024

DSO gav i GDPR Årsrapport för 2024 ett flertal rekommendationer för att minska risken för de registrerades fri- och rättigheter vid behandling av deras personuppgifter.

Sprida information om tillåten och otillåten användning av AI till medarbetare

Miljöförvaltningen har informerat om säker användning i ett nyhetsbrev och den årliga GDPR-utbildningen som hålls av förvaltningen.[27] Utöver det finns information om AI på intranätet där det bland annat framgår att det inte är tillåtet att ladda upp personuppgifter i AI-plattformar utan att skyddsåtgärder vidtagits. DSO bedömer att åtgärderna är tillräckliga för närvarande och att den rekommenderade åtgärden är vidtagen.

Utreda att samtliga personuppgiftsbehandlingar omfattas av en informationsklassning

Miljöförvaltningens Arkiv och registratur-funktion har kartlagt informationsklassningarna och identifierat till vilken personuppgiftsbehandling de hör. Det här har sedan dokumenterats i registerförteckningen. Åtgärden har inte inkluderat bedömning av om informationsklassningarna beaktar personuppgifter på ett lämpligt sätt. Miljöförvaltningens mall för informationsklassning och verktyget KLASSA omfattar bedömning av personuppgifter. DSO bedömer att kartläggningen skapar ännu mer struktur i dataskyddsarbetet och konstaterar att de vidtagna åtgärderna är tillräckliga.

Översyn av befintliga konsekvensbedömningar

DSO rekommenderade att se över befintliga konsekvensbedömningar för att det inte har genomförts någon sådan granskning eller uppdatering av genomförda konsekvensbedömningar. Miljöförvaltningen har inte vidtagit några åtgärder under 2025. Däremot planerar Miljöförvaltningens GDPR-grupp att införa en rutin att årligen gå igenom konsekvensbedömningar. DSO rekommenderar att rutinen implementeras.

Tröskelanalys av behandling av anställdas personuppgifter

DSO rekommenderade att genomföra en tröskelanalys av behandling av anställdas personuppgifter för att bedöma om det finns en skyldighet att genomföra en konsekvensbedömning. Mot bakgrund av att det råder osäkerhet kring det kommuninterna

[27] Nyhetsbrev från verksamhetsstöd 2025:3, skickat 22 september 2025.

personuppgiftsansvarets fördelning har verksamheten mött svårigheter i att definiera vilka delar Miljö- och hälsoskyddsnämnden är den personuppgiftsansvarige för. Därför har tröskelanalysen inte färdigställts ännu. Verksamheten uppger att man avvaktar en utredning från Stadsledningskontoret.

DSO rekommenderar att färdigställa tröskelanalysen, och genomföra en konsekvensbedömning om den skyldigheten finns.

Radering från backups

DSO rekommenderade verksamheten att säkerställa att eventuella begäranden om radering från registrerade kan hanteras, specifikt radering från backups.

Miljöförvaltningen har under året uppdaterat sin rutin för tillvaratagande av registrerades rättigheter[28] som bland annat innehåller en rutin för hantering av begäran om radering. Rutinen innehåller nu information om att radering även ska ske från eventuella backups.

Risken har i och med Miljöförvaltningens åtgärder mitigerats och inga vidare åtgärder rekommenderas.

Information om personuppgiftsbehandling till anställda

DSO granskade under 2024 information till anställda om behandlingen av deras personuppgifter och identifierade brister. DSO rekommenderade med anledning av detta att informationen uppdateras med mer specifik information.

Under 2024 har GDPR-gruppen på Miljöförvaltningen arbetat med att ta fram en ny text. Texten är dock inte färdig. En av anledningarna till att texten inte har färdigställts är oklarheter kring det kommuninterna personuppgiftsansvaret. Miljöförvaltningen inväntar stadens utredning om det kommuninterna personuppgiftsansvaret. Stadsledningskontoret leder utredningen.

DSO ser risker att anställda inte får sina rättigheter enligt artiklar 13-14 tillgodosedda. Även bristen i stickprovet avseende registerutdrag talar för detta. Det är av stor vikt att Miljöförvaltningen prioriterar att uppdatera informationen. I den mån det råder oklarheter kring ansvaret bör Miljöförvaltningen vända sig till, till exempel, Stadsledningskontoret och Serviceförvaltningen för att få klarhet i hur de behandlar personuppgifter om anställda, och om de i så fall i någon mån gör det som självständigt personuppgiftsansvariga.

Något som förmildrar risken är att Stadsledningskontorets dataskyddsfunktion har publicerat en text om behandling av personuppgifter om anställda på intranätet.[29]

Tydlig information till anställda om användning av e-post

I årsrapporten från 2023 rekommenderade DSO att ge anställda tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och allmänna handlingar, vilket kan ske genom exempelvis regelbundna utbildningar. DSO påminde om detta i GDPR Årsrapport 2024. Miljöförvaltningen har i intervjuer under granskningsperioden informerat att

[28] Rutin för tillvaratagande av de registrerades rättigheter enligt artiklarna 16-22 dataskyddsförordningen, 2025-05-14, v 1.2.

[29] Så hanterar Stockholms stad dina personuppgifter som anställd, senast uppdaterad 2025-09-19.

de inte har utbildat eller informerat om hur anställda ska hantera e-post med anledning av rekommendationen. Det kommer dock framgå av e-utbildningen som verksamheten arbetar med att ta fram.[30] E-utbildningen skulle kunna kompletteras med en skriftlig rutin för att möjliggöra att anställda kan gå tillbaka till informationen på ett enkelt sätt.

DSO rekommenderar att vidta åtgärder i enlighet med rekommendationen 2023.

Information om personuppgiftsbehandling i e-tjänsterna

DSO identifierade en brist i informationen till registrerade i GDPR Årsrapport 2024 avseende e-tjänsterna Anmälan om matförgiftning och Anmälan om brister i livsmedelshantering. Bägge saknade information om personuppgiftsbehandling. DSO rekommenderade verksamheten att komplettera de nämnda e-tjänsterna med kort information om personuppgiftsbehandling och hänvisning med länk till den fullständiga informationen.

Verksamheten har kompletterat e-tjänsterna med en länk till Stockholms stads övergripande information om personuppgiftsbehandling.[31] Texten är mycket allmänt hållen för att omfatta all personuppgiftsbehandling staden gör och innehåller inte information om till exempel användningen av Miljöförvaltningens e-tjänster.

Rätten till information som framgår av 12–14 GDPR materialiserar den grundläggande principen i GDPR om öppenhet och transparens. Artikel 12 stadgar att information ska vara koncis, klar och tydlig, begriplig och lätt tillgänglig. I Artikel 29-gruppens riktlinjer om öppenhet[32] (som har antagits av Europeiska dataskyddsstyrelsen, EDPB) rekommenderas den personuppgiftsansvarige om hur den personuppgiftsansvarige i praktiken kan uppfylla skyldigheterna om öppenhet och transparens enligt GDPR. I digitala miljöer rekommenderas den personuppgiftsansvarige att tillhandahålla information i lager för att inte överväldiga den registrerade, men ändå tillhandahålla informationen som krävs. Första lagret – det vill säga där den personuppgiftsansvarige ”möter” den registrerade – bör innehålla ändamålen för personuppgiftsbehandlingen, vem den personuppgiftsansvarige är och information om den registrerades rättigheter.

DSO rekommenderar att verksamheten både byter ut länken i respektive e-tjänst till Miljöförvaltningens information om personuppgiftsbehandling,[33] och tillhandahåller en kort information om den personuppgiftsansvarige, ändamålen för personuppgiftsbehandlingen och om den registrerades rättigheter i enlighet med artikel 29-gruppens, och sedermera EDPB:s, riktlinjer, för att uppfylla artikel 12-14 GDPR.

Eftersom öppenhet och transparens är en grundläggande princip i GDPR är det centralt att informationsskyldigheten uppfylls. Den befintliga informationen uppfyller inte artiklar 12-14 på grund av att den registrerade inte får specifik information om behandlingen i e-tjänsten, eller den personuppgiftsansvariges identitet. Det här utgör en brist.

---

[30] Se nedan under avsnittet Utbildning av anställda.

[31] Den här texten: Personuppgifter och dataskydd - Stockholms stad.

[32] Article 29 Working Party, WP260 rev.01, Guidelines on transparency under Regulation 2016/679.

[33] Den här texten: Behandling av personuppgifter på miljöförvaltningen - Stockholms stad.

Utbildning av anställda

DSO rekommenderade verksamheten att fortsätta utbilda anställda om dataskydd och GDPR. Under året har Miljöförvaltningen hållit sin årliga GDPR-utbildningen för samtliga anställda vid förvaltningen. Utöver det går de anställda också de digitala utbildningarna som erbjuds alla stadens medarbetare.

Vid intervjuer under granskningsperioden har miljöförvaltningen informerat om att de håller på att ta fram en ny e-utbildning om diarieföring, arkivering, utlämnande, offentlighet och sekretess samt hantering av e-post. E-utbildningen planeras lanseras under Q1 2026.

DSO ser positivt på att Miljöförvaltningen lägger mycket resurser på utbildning och medvetandegörande genom olika kanaler som hela förvaltningen, enhetsmöten, nyhetsbrev och digitala utbildningar och rekommenderar verksamheten att fortsätta med detta för att upprätthålla en god dataskyddskultur.

Fråga/kontroll	Risk	Rekommendationer
Rutin för granskning av befintliga konsekvensbedömningar		Verksamheten har meddelat att rutinen kommer att införas under nästa år, och DSO ser ingen orsak att tvivla på detta. DSO rekommenderar att rutinen dokumenteras och implementeras.
Tröskelanalys avseende behandling av anställdas personuppgifter		DSO rekommenderar att tröskelanalysen avseende behandling av anställdas personuppgifter färdigställs i enlighet med ovan. Om tröskelanalysen visar en skyldighet att genomföra en konsekvensbedömning rekommenderas den personuppgiftsansvarige att genomföra detta.
Information till registrerade (anställda, användare av e-tjänst)		DSO har noterat att informationen inte har uppdaterats, dels på grund av väntan på en utredning (anställda). DSO rekommenderar att uppdatera informationen till anställda, samt informationen till användare av e-tjänster i enlighet med ovanstående.
Tydlig information till anställda om e-post		DSO har tidigare rekommenderat att ge anställda tydlig information om hantering av e-post i enlighet med bl.a. GDPR. Verksamheten uppger att detta ska genomföras våren 2026 genom e-utbildning. DSO rekommenderar att på lämpligt sätt ge anställda tydlig information om hur de ska hantera sin e-post i förhållande till GDPR och

		allmänna handlingar, i enlighet med tidigare rekommendation.

Dataskyddsombudets rekommendationer

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan.

Dataskyddsombudets rekommendationer

1. *Säkerställa att relevanta personer har kunskap om hur objekten styrs och hur PM3-modellen ser ut (t ex genom utbildning om PM3-modellen och/eller inläsning).*
2. *Säkerställa att relevanta personer (t ex objektägare, objektledare) läser objektplaner, särskilt för de större objekten (som hanterar bl.a. LISA, Agresso).*
3. *Färdigställa den stadeninterna instruktionen som reglerar den personuppgiftsbehandling som Servicenämnden gör för Miljö- och hälsoskyddsnämndens räkning.*
4. *Verka tillsammans med SLK (och andra relevanta nämnder) för att Kommunstyrelsen förtydligar personuppgiftsansvarets fördelning, särskilt vad gäller behandling av anställdas personuppgifter.*
5. *Verka för att reglera personuppgiftsansvaret mellan Kommunstyrelsen och Miljö- och hälsoskyddsnämnden.*
6. *I de fall möjlighet ges, och det anses relevant för Miljöförvaltningens verksamhet, prioritera att delta i normerande klassningar för att på så sätt vara delaktiga i beslut.*
7. *DSO rekommenderar den personuppgiftsansvarige att ta fram rutin och mall för leverantörsuppföljning.*
8. *DSO rekommenderar att dokumentera och implementera rutinen för granskning av befintliga konsekvensbedömningar.*
9. *DSO rekommenderar att färdigställa tröskelanalysen avseende behandling av anställdas personuppgifter (som inte täcks av konsekvensbedömningen om flextidsredovisningssystemet), och att genomföra en konsekvensbedömning om den skyldigheten finns.*
10. *DSO rekommenderar att uppdatera informationen till anställda om behandling av deras personuppgifter i enlighet med artiklar 12–14 GDPR, relevant praxis och vägledning.*
11. *DSO rekommenderar att ge anställda tydlig information om hur de ska hantera sin e-post i förhållande till GDPR och allmänna handlingar.*
12. *DSO rekommenderar att uppdatera hur registrerade ges information i två e-tjänster i enlighet med ovan.*[34]

[34] Se avsnittet om Information om personuppgiftsbehandling i e-tjänsterna.

Bilaga 3 Översyn av det kommuninterna personuppgiftsansvaret

Inledning

Bakgrund

Miljö- och hälsoskyddsnämnden samt dataskyddsombudet (”DSO”) har under flera år uppmärksammat utmaningar gällande tydligheten kring fördelningen av det kommuninterna personuppgiftsansvaret och konsekvenserna av det. Detta har sin huvudsakliga grund i att varje nämnd inom staden är personuppgiftsansvarig för de personuppgifter som behandlas inom den egna verksamheten.[35]

DSO rekommenderade redan i årsrapporten 2021 att arbetet med att lösa dessa kommuninterna personuppgiftsansvarsfrågor bör fortsätta.[36] Denna rekommendation har därefter kvarstått i samtliga efterföljande årsrapporter. Mot denna bakgrund beslutade DSO att genomföra en granskning av hur det kommuninterna personuppgiftsansvaret är fördelat, reglerat och fungerar i praktiken.

Dataskyddsombudets granskning

Syfte och mål

Förevarande granskning syftar till att göra en översyn av och analysera det kommuninterna personuppgiftsansvarets fördelning och hanteringen av detta. Syftet med granskningen är att identifiera eventuella otydligheter och brister i hanteringen ansvaret. Målet är att ge förslag på förbättringar till verksamheten som säkerställer att Miljö- och hälsoskyddsnämnden uppfyller de krav som ställs på nämnden i egenskap av personuppgiftsansvarig, samt identifiera de krav som verksamheten kan ställa på kommuninterna personuppgiftsbiträden och relevanta objekt i Stockholms stad. Detta inkluderar bland annat att reda ut vilka objekt som behandlar de personuppgifter som Miljö- och hälsoskyddsnämnden hanterar.

Genomförande

Dataskyddsombudet har för att genomföra förevarande granskning gjort följande:

- Intervjuat dataskyddshandläggaren vid Servicenämnden
- Haft mejlkontakt med:
    - Systemutvecklingsenheten, som har objektansvaret för Agresso
    - Enheten för HR-system, som har objektansvaret för LISA och Jobba i Staden (Varbi)
- Intervjuat objektledare inom Miljöförvaltningen, för objekten:
    - Jobba i Staden, Varbi
    - IA, incidentrapporteringssystem
    - LISA, HR-system
    - Agresso, ekonomi- och inköpssystem
    - Kommers, upphandlingssystem

[35] Kommunal författningsssamling för Stockholm, 2023:09, Reglemente med allmänna bestämmelser för Stockholms stads nämnder, Dnr KS 2022/1230, 5 §.

[36] Miljö- och hälsoskyddsnämnden, GDPR årsrapport 2021, dnr 2022-802.

    - EDok, ärende- och dokumenthanteringssystem[37]
    - E-arkiv, stadens gemensamma system för att lagra och bevara digitala handlingar
    - Lime
- Kartlagt och analyserat befintliga avtal som reglerar personuppgiftsbehandlingen inom Stockholms stad och leverantörer av gemensam IT till Stockholms stad.
- Granskat styrdokument och vägledning.

Resultatet av granskningen

Personuppgiftsansvar enligt GDPR

Personuppgiftsansvar

Enligt artikel 4.7 GDPR avses med personuppgiftsansvarig:

> ”*en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter*”.

I enlighet med definitionen ska Miljö- och hälsoskyddsnämnden anses vara den personuppgiftsansvarige för den del där nämnden styr över ändamålen och medlen för behandlingen av personuppgifterna. På samma sätt blir andra nämnder och bolag personuppgiftsansvariga när de behandlar personuppgifter för egna ändamål och bestämmer medlen för hur uppgifterna därmed ska behandlas. Vid bedömning av vem som bestämmer ändamålen och medlen ska man följaktligen ta ställning till vem som bestämmer:

- varför behandlingen ska ske och i vilket syfte; och
- hur behandlingen kommer att ske.

Av personuppgiftansvaret följer flera olika skyldigheter enligt GDPR. Till exempel ansvarar den personuppgiftsansvarige för efterlevnaden av GDPR:s grundläggande principer som beskrivs i artikel 5.1 GDPR och att den personuppgiftsansvarige ska kunna *bevisa* efterlevnaden av principerna som beskrivs i artikel 5.1, enligt artikel 5.2 GDPR.[38] Därtill har den personuppgiftsansvarige flera andra skyldigheter så som att säkerställa uppfyllandet av de registrerades rättigheter enligt artiklarna 13-22 GDPR, föra register över personuppgiftsbehandling enligt artikel 30 och vidta lämpliga säkerhetsåtgärder enligt artikel 32. DSO konstaterar att många av dessa skyldigheter är svåra, om inte omöjliga, för en aktör att uppfylla om den inte i faktiskt mening bestämmer ändamål och medel för personuppgiftsbehandling, eller i övrigt inte har rådighet över behandlingen – varför skyldigheterna måste falla på den personuppgiftsansvarige.

[37] Miljöförvaltningen använder systemet mycket sparsamt, t ex för att svara på remisser.

[38] EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, ver 2.0, antaget den 7:e juli 2021, s 9.

Europeiska dataskyddsstyrelsen (EDPB) resonerar i en riktlinje[39] om byggstenarna i begreppet personuppgiftsansvarig. En av byggstenarna är att den personuppgiftsansvarige ska ha inflytande över behandlingen. Den ska besluta över vissa nyckelelement i behandlingen. De utvecklar att analysen ska utgå från faktiska omständigheter, snarare än vad som bestämts i avtal. Omständigheter som ger upphov till kontroll kan till exempel härröra från bestämmelser i lag[40] eller faktiskt inflytande. EDPB noterar här att en och samma enhet kan vara personuppgiftsansvarig för vissa personuppgiftsbehandlingar, och personuppgiftsbiträde för andra, och att detta ska bedömas med hänsyn till varje specifik del av behandlingen.[41]

Personuppgiftsbiträde

En annan ansvarsroll vid behandling av personuppgifter är personuppgiftsbiträde. Enligt artikel 4.8 GDPR avses med personuppgiftsbiträde:

> ” *en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning*”.

Ett personuppgiftsbiträde kan i sin tur med godkännande av den personuppgiftsansvariga anlita underbiträden för att utföra vissa delar av tjänsten.

Gemensamt personuppgiftsansvar

Vidare kan det finnas situationer där ansvaret delas mellan flera aktörer. Ett sådant s.k. gemensamt personuppgiftsansvar uppstår när två eller flera personuppgiftsansvariga gemensamt beslutar om både ändamålet och medlen för behandlingen, eller när deras beslut om ändamålet och medlen konvergerar.[42] Däremot uppstår inte ett gemensamt personuppgiftsansvar när fler personuppgiftsansvariga separat fattar beslut om ändamål och/eller medel med en behandling, även om företagen behandlar samma personuppgifter. En bedömning av om det finns ett gemensamt ansvar för behandlingen bör utföras utifrån en saklig analys av det faktiska inflytandet över de ändamål och medel för behandlingen som vardera parten har. Analysen utgår i dessa fall från en processbeskrivning av den aktuella personuppgiftsbehandlingen där ansvarsfördelningen för de enskilda stegen i behandlingen utreds. Resultatet av utredningen dokumenteras i ett avtal om ansvarsfördelningen mellan de som är gemensamt personuppgiftsansvariga för behandlingen.[43]

---

[39] EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, ver 2.0, antaget den 7:e juli 2021, s 11 ff.

[40] Jämför t ex vårdgivares personuppgiftsansvar som fastställs i patientdatalagen (2008:355).

[41] EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, ver 2.0, antaget den 7:e juli 2021, s 13.

[42] Artikel 26 i GDPR, mål C-604/22 p. 59.

[43] Artikel 26 GDPR.

Personuppgiftsansvar i Stockholms stad enligt reglemente, styrdokument och vägledning

I det här avsnittet beskrivs vad som finns reglerat om personuppgiftsansvar för Stockholms stad i författningar, interna styrdokument, och vägledning som har tagits fram av Juridiska avdelningen vid stadsledningskontoret (”SLK”).

I Stockholms stad är respektive nämnd och styrelse personuppgiftsansvariga för sin verksamhets personuppgiftsbehandling.[44] Det här framgår bland annat av Reglementet med allmänna bestämmelser för Stockholms stads nämnder 5 §:

> *”Nämnden är personuppgiftsansvarig för de personuppgifter som nämnden behandlar i sin verksamhet. Nämnden kan också vara personuppgiftsbiträde åt en annan nämnd eller gemensamt personuppgiftsansvarig tillsammans med en annan nämnd, varvid de inbördes ansvarsförhållandena ska regleras. Vid ett biträdesförhållande ska den personuppgiftsansvariga nämnden ge instruktioner om behandlingen till den personuppgiftsbiträdande nämnden. Om gemensamt personuppgiftsansvar förekommer ska fördelningen av ansvar regleras mellan nämnderna, bl.a. avseende den registrerades rättigheter och tillhandahållande av information till den registrerade.”*[45]

I tillämpningsanvisningen till stadens riktlinje för informationssäkerhet beskrivs att som ett resultat av detta, att respektive nämnd och styrelse är personuppgiftsansvarig, uppstår det ett internt personuppgiftsbiträdesförhållande enligt gällande dataskyddspraxis när en nämnd/styrelse inom staden behandlar personuppgifter för en annan nämnds/styrelses räkning.

Ett resultat av det här är att Servicenämnden är personuppgiftsbiträde till Miljö- och hälsoskyddsnämnden för behandling av personuppgifter för t ex hantering av ekonomiadministration och löne- och pensionsadministration.[46]

Personuppgiftsansvarets fördelning enligt avtal och stadens interna instruktion

I det här avsnittet beskrivs hur avtalen och eventuella stadeninterna instruktioner reglerar personuppgiftsansvaret när flera nämnder delar på gemensam IT.

Enligt stadens tillämpningsanvisning till stadens riktlinje för informationssäkerhet gäller att för IT-tjänster som ingår i avtal som är centralt upphandlade genom kommunstyrelsen ansvarar SLK för framtagande och förvaltning av personuppgiftsbiträdesavtal med leverantörerna.[47]

---

[44] Framgår bland annat av Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, s 4.

[45] Kommunal författningsssamling för Stockholm, 2023:09, Reglemente med allmänna bestämmelser för Stockholms stads nämnder, Dnr KS 2022/1230, 5 §.

[46] Enligt utkast för stadenintern instruktion mellan Miljö- och hälsoskyddsnämnden och Servicenämnden.

[47] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet.

Personuppgiftsansvarets fördelning och Miljö- och hälsoskyddsnämnden

Miljö- och hälsoskyddsnämnden använder flera tjänster, bland annat IT-tjänster, som är gemensamma för Stockholms stad.

Ett exempel är leverantören Vivicta (tidigare Tietoevry AB) som tillhandahåller IT-drift till Stockholms stad. För Miljö- och hälsoskyddsnämndens del innebär det att IT-driften för systemet Ecos[48] sköts av Vivicta. Vivicta sköter även IT-driften av LISA (HR-system) och Agresso (inköps- och ekonomisystem).

Vivicta tillhandahåller drift av verksamhetssystem, lagring av data, applikationsförvaltning, support och konsulttjänster kopplade till verksamhetssystem, samt olika stödtjänster. Det finns ett stadsövergripande systemtjänsteavtal som gäller för alla förvaltningar och bolag inom staden. Avtalet förvaltas centralt av avdelningen för it och digitalisering på SLK.[49] Till systemtjänsteavtalet finns ett PUB-avtal[50] där det framgår att personuppgiftsansvariga är nämnderna som har förtecknats i bilaga 2 till systemtjänsteavtalet (där Miljö- och hälsoskyddsnämnden ingår).[51] Avtalet är således centralt hanterat, men varje nämnd, styrelse, stiftelse och bolag är part i PUB-avtalet med Vivicta på så sätt att de identifieras som personuppgiftsansvariga. SLK (kommunstyrelsen) betraktas således inte som ett stadeninternt personuppgiftsbiträde till nämnderna för tillhandahållandet av IT-driften från Vivicta.

Utöver detta finns det flera PUB-instruktioner för Systemtjänsteavtalet, som reglerar personuppgiftsbehandlingen.[52] En instruktion finns för personalsystem och omfattar bland annat LISA bas och LISA självservice. Det är Enheten för HR-system, som har objektansvaret för objektet Centrala HR-system, där LISA ingår, och som ansvarar för den instruktionen. Liksom PUB-avtalet är Miljö- och hälsoskyddsnämnden markerad som personuppgiftsansvarig i PUB-instruktionen.

En annan instruktion är den som gäller för bl.a. Agresso, som är framtagen av objektorganisationen för objektet ekonomi och inköpssystem.[53] Agresso ligger i stadens miljö hos Vivicta. Det är SLK:s systemutvecklingsenhet som har objektansvaret för objektet.[54] Även här är PUB-instruktionen framtagen centralt, å alla[55] nämnders, bolags och stiftelsers vägnar.

---

[48] Ecos är Miljöförvaltningens ärendehanteringssystem.

[49] Stockholms stads intranät, Systemtjänsteavtal, hämtad 2025-12-19. Systemtjänsteavtal, dnr: KS 2021/1326.

[50] Personuppgiftsbiträdesavtal, bilaga 16 till Systemtjänsteavtalet, dnr KS 2021/1327.

[51] Bilaga 2 Deltagande Förvaltningar, Bolag och Stiftelser, dnr KS 2021/1326, ver 1.2.

[52] Instruktion till Personuppgiftsbiträdesavtal, upprättad 2022-12-22, dns KS 2021/1326, för personalsystem.

[53] Instruktion till personuppgiftsbiträdesavtal; upprättad 2024-04-09, dnr KS 2021/1326, för Stockholms stads koncerngemensamma ekonomi och inköpssystem.

[54] Enligt mejl från Systemutvecklingsenheten till DSO 2025-12-04. Se även objektplan för Agresso på intranätet: Om Agresso.

[55] Nämnda i Bilaga 2 Deltagande Förvaltningar, Bolag och Stiftelser, dnr KS 2021/1326, ver 1.2.

Utöver ovanstående har Miljöförvaltningen tagit fram PUB-instruktioner till Vivicta som gäller för Ecos och geodataplattformen.[56]

Sammanfattningsvis är det, liksom framgår av tillämpningsanvisningen till stadens riktlinje om informationssäkerhet, SLK som ansvarar för framtagande och förvaltning av personuppgiftsbiträdesavtal när det gäller centralt upphandlade tjänster. SLK (kommunstyrelsen) betraktas dock *inte* som ett stadeninternt personuppgiftsbiträde för detta, utan respektive nämnd, inklusive Miljö- och hälsoskyddsnämnden, är själv utpekad som ”part” i avtalen. Avtal och stadenintern instruktion mellan Miljö- och hälsoskyddsnämnden och SLK som reglerar behandling av personuppgifter saknas.

Avtalen

Avtalen finns att hitta i Kommers:

- Agresso, Unit4: Kommers Stockholms Stad
- Agresso, Vivicta: Kommers Stockholms Stad
- LISA, Vivicta: Kommers Stockholms Stad
- Kommers, Antirio System AB: Kommers Stockholms Stad
- Jobba i Staden, Varbi: Kommers Stockholms Stad
- Lime, Insight Technology Solutions AB: Kommers Stockholms stad

Pågående arbete vid Stadsledningskontoret

I skrivande stund pågår arbete på olika delar av SLK med att utreda personuppgiftsansvarets fördelning. På SLK pågår ett arbete för att utreda personuppgiftsansvaret som kan ge verksamheterna vägledning för behandling och dokumentation av personuppgiftsansvaret.[57]

Enheten för HR-system har meddelat att de arbetar med en överenskommelse för ett gemensamt personuppgiftsansvar, som enheten hoppas blir färdigställd till våren 2026.[58] DSO ser, i dagsläget, inte att en sådan överenskommelse kommer att lösa osäkerheterna kring personuppgiftsansvarets fördelning.

Resultat av intervjuer med objektledare inom Miljöförvaltningen

DSO har under granskningsperioden haft intervjuer med fyra objektledare vid Miljöförvaltningen. Syftet med intervjuerna var att kunna bilda sig en uppfattning om hur objektledaruppdraget fungerar, vilken informationsöverföring som sker från den centrala förvaltningen till den lokala objektledaren (hos Miljö- och hälsoskyddsnämnden) från objekten till objektledarna och om objektledarna upplever några utmaningar med objektledarskapet.

Objektledarna har lokalt ansvar för system som styrs i objekt i staden. En objektledares ansvar framgår dels av tillämpningsanvisningen respektive lokala anvisningen om

---

[56] Bilaga till PUB-avtal (Systemtjänsteavtalet), dnr KS 2021/1326, Instruktion till Personuppgiftsbiträdesavtal; upprättad 2025-01-15 (Diarium, ärende- och dokumenthanteringssystem) samt Instruktion till Personuppgiftsbiträdesavtal; upprättad 2025-01-15 (Geodataplattform).

[57] Enligt mejl till DSO från stadsledningskontorets funktionsbrevlåda för juridiska avdelningen, 2025-12-09.

[58] Enligt mejl till DSO från stadsledningskontorets funktionsbrevlåda för enheten för hr-system, 2025-12-02.

informationssäkerhet. I Miljö- och hälsoskyddsnämndens lokala anvisning för informationssäkerhet beskrivs objektledare som den som säkerställer att information är uppdaterad och korrekt, att dokumentation om systemet finns och är tillgänglig för dem som behöver den och uppdaterar vid behov (t ex objektplan), samt dokumenterar viktiga förändringar eller händelser kring systemet, t ex uppgraderingar, större textförändringar eller incidenter.

Generellt sätt är objektledarna nöjda med systemen och uppger att rollen som objektledare fungerar bra. Vissa nämnde att specialanpassning av system hade kunnat vara en fördel. Angående information från objektet som ansvarar för systemet nämner objektledarna att kommunikationen är god. Kommunikation kan ske både genom nätverk och forum, direktkontakt med systemägare, möten och referensgrupper och informationsutskick. Alla objektledare uppger att de vet vem de ska vända sig till vid frågor, och att objektet är bra på att kommunicera t ex om förändringar. I intervjuer har tre av fyra objektledare uppgett att objekten centralt kommunicerar mycket bra om förändringar och sådant som påverkar Miljöförvaltningen.[59]

I vissa fall finns det lokala rutiner och objektplaner gjorda vid Miljöförvaltningen, i andra fall saknas det och finns enbart centralt. Det här har inte uppmärksammats som problematiskt av de intervjuade objektledarna.

Konsekvenser av otydlig fördelning av personuppgiftsansvar

Den personuppgiftsansvarige har många skyldigheter som följer av GDPR.[60] Dessa skyldigheter spänner över områden som informationsskyldighet till individer, att vidta lämpliga säkerhetsåtgärder och hantera incidenter. När en personuppgiftsincident 2025, som avsåg ett cyberangrepp mot systemleverantören Miljödata i Karlskrona AB, ledde till att anställda vid stadens personuppgifter spreds på ”darknet” satte det frågor om personuppgiftsansvarets fördelning på sin spets.

Det var SLK som hade haft ett uppdrag att upphandla, och sedan tillhandahålla, ett system för rapportering och uppföljning av arbetsmiljöincidenter. SLK beslutade att använda personuppgifter om anställda vid respektive nämnd för att kunna verifierings- och acceptanstesta en integration.[61]

Enligt Miljöförvaltningen[62] har förvaltningen varken informerats, eller tillfrågats om, att använda personuppgifter om anställda vid Miljöförvaltningen i samband med detta test av verifiering och acceptans. Miljö- och hälsoskyddsnämnden, som anses vara den personuppgiftsansvarige, har inte haft någon insyn eller rådighet över hur personuppgifterna hanteras centralt av staden. Under de omständigheterna bedömer DSO att Miljö- och hälsoskyddsnämnden inte i faktisk mening har beretts några förutsättningar att uppfylla den

[59] Objektledare för LIME, ett nyhetsbrevsverktyg, har ingen kontakt med det centrala objektet, men har inte heller något behov av det.

[60] Se ovan under rubriken ”Personuppgiftsansvar enligt GDPR”.

[61] Enligt mejl till DSO från enhetschef vid enheten för hr-system, 2025-09-16.

[62] Enligt möte med Miljöförvaltningens objektledare för LISA, 2025-11-25, samt mejl till DSO från avdelningschefen vid verksamhetsstöd, 2025-08-28.

personuppgiftsansvariges skyldigheter. I ljuset av detta bör inte heller Miljö- och hälsoskyddsnämnden anses vara den personuppgiftsansvarige enligt GDPR.

För att förtydliga konsekvenserna har resultatet blivit att Miljö- och hälsoskyddsnämnden bl.a.:

- Inte har haft möjlighet att informera registrerade innan personuppgiftsbehandlingen (enligt art 13-14 GDPR).
- Inte har kunnat besvara frågor från registrerade med säkerhet, särskilt avseende deras rättigheter enligt artikel 15-22 GDPR.
- Inte har kunnat göra en bedömning av rättslig grund eller uppfyllande av GDPR:s principer (innan behandling)[63]

Dessa brister har i sin tur negativt påverkat de registrerades fri- och rättigheter, särskilt med hänsyn till principen om öppenhet och transparens, och registrerades rätt till information.

Dataskyddsombudets bedömning

Granskningen visar att otydligheter i fördelningen av det kommuninterna personuppgiftsansvaret medför betydande risker ur ett dataskyddsperspektiv, särskilt för de registrerade. När ansvarsförhållanden inte är klart definierade finns en risk att grundläggande skyldigheter enligt GDPR – såsom informationsskyldighet, säkerhetsåtgärder och hantering av registrerades rättigheter – inte uppfylls. Det uppstår även strukturell osäkerhet och tilltagande press hos Miljö- och hälsoskyddsnämnden, som inte vet var deras ansvar börjar eller slutar avseende dataskydd.

Det finns visserligen personuppgiftsbiträdesavtal med externa leverantörer, men det saknas avtalsförhållanden och instruktioner mellan Kommunstyrelsen (SLK) och Miljö- och hälsoskyddsnämnden som reglerar ansvarsfördelningen internt. Denna avsaknad förstärker osäkerheten kring vem som har kontroll över behandlingen och därmed vem som ska uppfylla skyldigheterna enligt GDPR.

Slutsats: Granskningen visar att Miljö- och hälsoskyddsnämnden i vissa situationer saknar faktisk rådighet över personuppgiftsbehandlingen, trots att nämnden såväl enligt lagens bokstav som enligt interna styrdokument är personuppgiftsansvarig. I vissa fall är det tvärtom så att Miljö- och hälsoskyddsnämnden är den utsedda personuppgiftsansvarige enligt stadenintern praxis eller instruktion, men har varken bestämt ändamål eller medel för personuppgiftsbehandlingen enligt artikel 4.7. Sammantaget skapar det här en strukturell brist som gör det svårt, och i vissa fall omöjligt, att uppfylla de krav som följer av GDPR. Slutsatsen är att nuvarande ordning inte ger tillräckliga förutsättningar för att säkerställa efterlevnad och att risken för bristande dataskydd är påtaglig.

[63] Stadsledningskontoret har meddelat att de har en referenskonsekvensbedömning avseende införandet av Stella. I september hade referenskonsekvensbedömningen dock inte färdigställts. DSO har hittills inte fått ta del av referenskonsekvensbedömningen av SLK.

DSO:s rekommendationer

DSO konstaterar inledningsvis att otydligheterna med det kommuninterna personuppgiftsansvarsförhållandet inte är möjligt att lösa av Miljö- och hälsoskyddsnämnden själv, utan kräver samverkan.

Dataskyddsombudet rekommenderar Miljö- och hälsoskyddsnämnden att:

- Säkerställa att relevanta personer har kunskap om hur objekten styrs och hur PM3-modellen ser ut (t ex genom utbildning om PM3-modellen och/eller inläsning).
- Säkerställa att relevanta personer (t ex objektägare, objektledare) läser objektplaner, särskilt för de större objekten (som hanterar bl.a. LISA, Agresso).
- Färdigställa den stadeninterna instruktionen som reglerar den personuppgiftsbehandling som Servicenämnden gör för Miljö- och hälsoskyddsnämndens räkning.
- Verka tillsammans med SLK (och andra relevanta nämnder) för att Kommunstyrelsen förtydligar personuppgiftsansvarets fördelning, särskilt vad gäller behandling av anställdas personuppgifter.
- Verka för att reglera personuppgiftsansvaret mellan Kommunstyrelsen (SLK) och Miljö- och hälsoskyddsnämnden.
- I de fall möjlighet ges, och det anses relevant för Miljöförvaltningens verksamhet, prioritera att delta i normerande klassningar för att på så sätt vara delaktiga i beslut.

Bilaga 4. Granskning av personuppgiftsbiträdesavtal

Bakgrund och kraven i GDPR

DSO har genomfört en granskning av Miljöförvaltningens personuppgiftsbiträdesavtal (PUB-avtal), vilket annonserades i GDPR Årsrapport 2024. Syftet med granskningen var att bedöma om PUB-avtalen uppfyller de krav som ställs i GDPR artikel 28. PUB-avtal är en grundläggande del av att reglera och säkerställa ett korrekt och säkert samarbete med externa leverantörer. Korrekt hantering av PUB-avtal minskar bland annat risken för bristande säkerhet.

Krav om personuppgiftsbiträdesavtal i GDPR

GDPR ställer särskilda krav på vad ett PUB-avtal ska innehålla. Dessa krav framgår av artikel 28 och kortfattat ska ett PUB-avtal innehålla följande krav:

- Att PUB ska enbart behandla uppgifter enligt den Personuppgiftsansvariges dokumenterade instruktioner.
- Att PUB ska säkerställa att personer som behandlar personuppgifter för den personuppgiftsansvariges räkning ska iaktta konfidentialitet eller omfattas av lagstadgad tystnadsplikt
- Att PUB ska skydda personuppgifter med lämpliga tekniska och organisatoriska åtgärder enligt artikel 32.
- Att PUB ska hjälpa den personuppgiftsansvarige att fullgöra sina skyldigheter, dels för att svara på registrerades begäranden om utövande av rättigheter, dels enligt artiklar 32-36 om hantering av konsekvensbedömning, personuppgiftsincidenter och säkerhet.
- Att PUB ska radera eller återlämna personuppgifter vid avslutad relation.
- Att PUB ska ge den personuppgiftsansvarige information som krävs för att visa att de uppfyller alla skyldigheter enligt artikel 28, samt möjliggöra bland annat granskningar och inspektioner som genomförs av den personuppgiftsansvarige.
- Reglering om underbiträden, t ex villkor för vad PUB behöver göra innan anlitande av ett annat personuppgiftsbiträde (inhämta tillstånd, informera, ålägga personuppgiftsbiträdet skyldigheter i avtal).

Andra relevanta krav i GDPR

Den personuppgiftsansvarige har andra skyldigheter som är relevanta i förhållande till anlitande av personuppgiftsbiträden och hanteringen av dem, bortsett från vad ett personuppgiftsbiträdesavtal ska innehålla.

Den personuppgiftsansvarige ska enligt artikel 28.1 enbart anlita personuppgiftsbiträden som kan ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder för att uppfylla kraven i GDPR och skydda registrerades rättigheter. Det här fastslår den personuppgiftsansvariges så kallade omsorgsplikt att vid anlitande av biträde.

Den grundläggande principen om ansvarsskyldighet (art. 5.2 GDPR) fastslår att den personuppgiftsansvarige ska kunna visa att principerna i GDPR följs. Vidare fastställer artikel 24 GDPR den personuppgiftsansvariges skyldighet att både genomföra och kunna visa att personuppgiftsbehandlingen utförs i enlighet med GDPR.

Mot bakgrund av detta är löpande granskning av personuppgiftsbiträden en naturlig följd av artiklarna 24 och 5.2 GDPR, som kräver att den personuppgiftsansvariga kan *säkerställa och*

visa efterlevnad, samt artikel 28, som förutsätter att biträden fortsatt ger tillräckliga garantier. Utan återkommande uppföljning kan dessa skyldigheter inte uppfyllas i praktiken.[64]

Krav i Stockholms stads interna styrdokument

Dataskyddsarbetet i Stockholms stad styrs bland annat genom Tillämpningsanvisning till stadens riktlinje för informationssäkerhet och Lokal anvisning för informationssäkerhet (Miljöförvaltningen) som också inkorporerar kraven i GDPR. Av den lokala anvisningen framgår bland annat att PUB-avtal krävs om den personuppgiftsansvarige anlitar någon annan för att behandla personuppgifter enligt vissa instruktioner, t ex en systemleverantör.[65] Av tillämpningsanvisningen framgår att objektägaren är ansvarig för att upprätta personuppgiftsbiträdesavtal.[66]

När man anlitar ett personuppgiftsbiträde ska man välja ett biträde som ger tillräckliga garantier om att de har förmåga att följa GDPR och vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter (artikel 28). Personuppgiftsansvaret kan aldrig delegeras till ett biträde, utan det är enbart uppgiften i fråga som genomförs av biträdet. Därför behöver den personuppgiftsansvarige följa upp att personuppgiftsbehandlingen genomförs på så sätt man avtalat och instruerat. Av tillämpningsanvisningen framgår det att det är objektägaren som är ansvarig för att tillse att rutiner upprättas för regelbunden uppföljning av hur en leverantör lever upp till de ställda informationssäkerhetskraven.[67]

På stadens intranät finns också mallar och vägledning gällande personuppgiftsbiträdesavtal med instruktion, inkluderat stadenintern instruktion som ska användas när en nämnd behandlar personuppgifter för en annan nämnds räkning.[68]

Utöver ovanstående framgår av stadens tillämpningsanvisning att för **it-tjänster**[69] som ingår i avtal som är centralt upphandlade genom kommunstyrelsen ansvarar stadsledningskontoret för framtagande och förvaltning av personuppgiftsbiträdesavtal med leverantörerna.[70]

Genomförande

DSO beskrev i GDPR Årsrapport 2024 att granskningen kommer att innebära följande:

---

[64] Mer läsning: Personuppgiftsansvariges ansvar för personuppgiftsbiträden beskrivs även i Yttrande 22/2024 av EDPB. IMY tar upp bristfällande kontroll och uppföljning av leverantörer som en del i riskhanteringen vid en konsekvensbedömning (se här).

[65] Lokal anvisning för informationssäkerhet, Miljöförvaltningen, s 13.

[66] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, s 29.

[67] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, s 30.

[68] GDPR och personuppgifter, hämtad 2025-12-15.

[69] Notera att det formuleras specifikt it-tjänster, och därmed eventuellt utesluter andra typer av tjänster.

[70] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet.

- En genomgång av befintliga PUB-avtal för att säkerställa att alla avtal inkluderar de krav som anges i artikel 28 i dataskyddsförordningen, så som tydliga instruktioner om behandling, säkerhetsåtgärder och biträdets skyldigheter.
- En översyn av hur verksamheten följer upp att leverantörer lever upp till avtalsvillkor.

Granskningen har genomförts genom att DSO har gjort en översyn av registerförteckningen och noterade mottagare/personuppgiftsbiträden i den. PUB-avtalen för dessa personuppgiftsbiträden har begärts ut från registraturen. Därefter har DSO granskat PUB-avtalen utifrån kraven i artikel 28. Utöver detta har DSO kontaktat objektägare, tillika avtalsägare, för respektive avtal för att kontrollera om leverantörsgranskning har genomförts under avtalstiden.

Omfattning och avgränsning

Granskningen har omfattat externa leverantörer som framgår som personuppgiftsbiträden i den personuppgiftsansvariges registerförteckning. Dessa inkluderar:

- Sokigo AB
- Avista Time AB
- Entergate AB
- Feelgood Företagshälsovård AB
- Gullers Grupp AB
- Antura AB

Personuppgiftsbiträdesavtal som Stadsledningskontoret ansvarar för i enlighet med Tillämpningsanvisning till stadens riktlinje för informationssäkerhet har inte ingått i granskningen.

Resultat

Sammanställning

I tabellen nedan finns en sammanställning över vilka leverantörer som har omfattats av granskningen och resultatet av granskningen.

Leverantör	Avtal	Resultat artikel 28.3 GDPR	Leverantörsuppföljning
1. Antura AB	Samverkans-överenskommelse inom EKR och datadelningsavtal inom EKR.	PUB-avtal med Antura AB har inte granskats. Datadelningsavtalet håller god kvalitet.	Ej relevant.
2. Avista Time AB	Avtal + PUB-avtal finns.	Uppfyller kraven	Har inte genomförts.
3. Entergate AB	Avtal + PUB-avtal finns.	Uppfyller kraven	Har inte genomförts.

4. Feelgood Företagshälsovård AB	Ramavtal centralt. PUB-avtal krävs ej.	Ej relevant.	Ej relevant.
5. Gullers Grupp AB	Ramavtal centralt. PUB-avtal finns.	Uppfyller kraven.	Har inte genomförts.
6. Sokigo AB	Avtal + PUB-avtal finns.	Uppfyller kraven	Har inte genomförts.

1. Datadelningsavtal avseende Antura AB

Stockholms stad har en samverkansöverenskommelse mellan kommunerna i Stockholms län (”Storsthlm”) avseende den regionala Energi- och klimatrådgivningen i Stockholms län. Målsättningen är att skapa förutsättningar för en effektiv användning av de resurser som tillfaller kommunerna i Stockholms län för EKR-verksamhet via statsbidrag. Syftet är att minska regionens negativa klimatpåverkan.[71] För samverkan finns ett datadelningsavtal som gäller personuppgiftsbehandling som sker inom ramen för rådgivningen.

I datadelningsavtalet framgår bland annat parternas åtaganden, reglering om underbiträden, beskrivning av behandlingen av personuppgifter och respektive parts skyldighet att informera registrerade.[72] DSO bedömer att datadelningsavtalet håller god kvalitet.

För samarbetet används, enligt mejl från Arkiv och registratur vid miljöförvaltningen, Antura Projects som tillhandahålls av Antura AB via Järfälla kommun. Arkiv och registratur informerar att Järfälla kommun har tecknat ett personuppgiftsbiträdesavtal med Antura AB. Det framgår av datadelningsavtalet att den som anlitar ett personuppgiftsbiträde själv ska svara för underbiträdets utförda arbete som om denne själv utfört arbetet enligt datadelningsavtalet.

DSO anser att regleringen av det gemensamma personuppgiftsansvaret är tillräckligt tydligt, och konstaterar att det är Järfälla kommuns ansvar att avtalet med Antura AB följer kraven i GDPR. DSO lämnar inga ytterligare rekommendationer om förevarande leverantör.

2. Personuppgiftsbiträdesavtal med Avista Time AB

Avista Time AB är leverantör av flextidsredovisningssystemet som används på Miljöförvaltningen. Personuppgiftsbehandlingen omfattar identifierande uppgifter, uppgifter relaterade till anställning så som yrkesbeteckning och frånvaro samt inloggningsinformation. Känsliga personuppgifter enligt artikel 9 GDPR omfattas inte.

---

[71] Enligt Samverkansöverenskommelse för regionala Energi- och klimatrådgivningen 1-2 §§, S/25/0052-5, 2025-06-16.

[72] *Notis: Huruvida Miljö- och hälsoskyddsnämnden har uppfyllt sin informationsskyldighet har inte omfattats av DSO:s granskning*.

Personuppgiftsbiträdesavtalet

Granskningen av personuppgiftsbiträdesavtalet (från 2022) mellan Miljö- och hälsoskyddsnämnden och Avista Time AB visar att avtalet huvudsakligen uppfyller artikel 28 GDPR, men att vissa punkter skulle kunna förtydligas för att minska riskerna ytterligare.

- Incidentrapportering
  Incidentrapporteringen regleras väl, men tidsfrist saknas (”utan onödigt dröjsmål”). DSO rekommenderar att vid omförhandling av avtal inkludera en tydlig tidsfrist för att kunna uppfylla sin anmälningsplikt och information till registrerade.

- Säkerhetskraven
  Säkerhetskraven är allmänt hållna och hänvisar till artikel 32, huvudavtalet och att PUB ska införa de skyddsåtgärder som följer av Miljöförvaltningen informationsklassning. Utöver det ska PUB även utföra åtaganden enligt Miljöförvaltningens riktlinjer för it-säkerhet och informationssäkerhet. DSO saknar krav om skyddsåtgärder från informationsklassning och riktlinjer om it- och informationssäkerhet har förmedlats till personuppgiftsbiträdet. DSO rekommenderar att säkerhetsåtgärder som Miljöförvaltningen bedömer lämpliga dokumenteras mer preciserat i instruktionerna som tillhör personuppgiftsbiträdesavtalet för att säkerställa en lämplig skyddsnivå för personuppgifterna. Ett alternativ är att bilägga riktlinjer om it- och informationssäkerhet.

Leverantörsuppföljning

Leverantörsgranskning har inte genomförts för att följa upp och kontrollera att leverantören lever upp till avtalet och GDPR.

3. Personuppgiftsbiträdesavtal med Entergate AB

Entergate AB är leverantör av programvaran Esmaker som är en tjänst för enkäthantering som används av Miljöförvaltningen. Personuppgiftsbehandlingen omfattar enligt PUB-avtalet identifierande uppgifter, kontaktuppgifter och uppgifter som samlas in genom enkäter/anmälningsformulär, vilka enligt avtalet kan avse t ex allmänheten, anställda och företrädare för andra organisationer.

Personuppgiftsbiträdesavtalet

Granskningen av personuppgiftsbiträdesavtalet (från 2018) mellan Miljö- och hälsoskyddsnämnden och Entergate AB har visat att avtalet uppfyller kraven i artikel 28 GDPR.

Lagring och annan behandling av personuppgifter sker i Sverige.
Personuppgiftsbehandlingens natur, omfattning och karaktär är inte känslig mot bakgrund av att det är ett enkätverktyg. I det fall integritetskänsliga uppgifter hanteras är det om själva enkäten handlar om någonting av känsligare grad. DSO har inte fått information om att det används för någonting annat än t ex anmälningar till event.

Mot bakgrund av ovanstående, att behandlingen inte utgör någon hög risk för registrerade och att PUB-avtalet uppfyller kraven i artikel 28, ger DSO inga rekommendationer. DSO vill dock påminna om att se över personuppgiftsbiträdesavtal regelbundet för att tillse att till exempel säkerställa att instruktioner är uppdaterade.

Leverantörsuppföljning

Leverantörsgranskning har inte genomförts för att följa upp och kontrollera att leverantören lever upp till avtalet och GDPR.

4. Feelgood Företagshälsovård AB

Feelgood Företagshälsovård AB (Feelgood) tillhandahåller företagshälsovård till flera nämnder vid Stockholms stad via ett ramavtal som ägs av Stadsledningskontoret.

Personuppgiftsbiträdesavtal finns inte, utan Feelgood agerar som självständigt personuppgiftsansvariga. Anledningen till att personuppgiftsbiträdesavtal inte finns är att Stadsledningskontorets juridiska avdelning har bedömt att Feelgood är personuppgiftsansvarig hela vägen i kontakter med stadens medarbetare och chefer. DSO utgår från att den slutsatsen är ett resultat av att Feelgood tillhandahåller tjänster där de anses vara vårdgivare (vårdgivare är självständigt personuppgiftsansvariga), och/eller att Feelgood bestämmer ändamål och medel själva enligt artikel 4. Mot bakgrund av juridiska avdelningens beslut, och att DSO inte har sett tecken på att bedömningen inte stämmer, har DSO valt att inte gå vidare med granskningen.

5. Personuppgiftsbiträdesavtal med Gullers Grupp AB

Gullers Grupp AB tillhandahåller strategiska kommunikationstjänster till Stockholms stad genom ett ramavtal. Ändamålet med personuppgiftsbehandlingen hos personuppgiftsbiträdet för Miljöförvaltningen är bland annat att informera bostadsrättsföreningar och mindre fastighetsägare av flerbostadshus om gällande lagkrav kring energieffektivisering. Behandlingen omfattar namn, roll, adress, telefonnummer och innebär således inte en behandling av personuppgifter som innebär hög risk för registrerade.

Personuppgiftsbiträdesavtalet

Granskningen av personuppgiftsbiträdesavtalet mellan Miljö- och hälsoskyddsnämnden och Gullers Grupp AB har visat att avtalet uppfyller alla krav i artikel 28 GDPR. Miljöförvaltningen har använt stadens mall för personuppgiftsbiträdesavtal. PUB-avtalet innehåller instruktioner till biträdet så som radering, för vilka ändamål biträdet får behandla personuppgifter, vilka personuppgifter som ska behandlas och relevanta säkerhetsåtgärder. Även stadens riktlinje för informationssäkerhet och tillämpningsanvisning för informationssäkerhet är bilagda avtalet. Det saknas en fast tidsfrist för incidentrapportering (”utan onödigt dröjsmål”), vilket skulle kunna åtgärdas vid nytt avtal.

Leverantörsuppföljning

Leverantörsgranskning har inte genomförts för att följa upp och kontrollera att leverantören lever upp till avtalet och GDPR.

6. Personuppgiftsbiträdesavtal med Sokigo AB

Sokigo AB är leverantör av licenserna för systemet Ecos. Systemet är installerat lokalt i Stockholms stads IT-miljö (som tillhandahålls av Vivicta Sweden AB, tidigare TietoEvry). Ecos är Miljöförvaltningens ärendehanteringssystem och är centralt för förvaltningens kärnverksamhet. Mot bakgrund av hur betydande systemet är för Miljöförvaltningens verksamhet, och hur omfattande personuppgiftsbehandlingen är i systemet är det viktigt att

personuppgiftsbiträdesavtalet är bra. Sokigo AB kan till exempel få del av personuppgifter vid användning av Sokigos personal för support av systemet.

Personuppgiftsbiträdesavtalet

Granskningen av personuppgiftsbiträdesavtalet mellan Miljö- och hälsoskyddsnämnden och Sokigo AB har visat att avtalet uppfyller alla krav i artikel 28. Det är välstrukturerat och detaljerat. Avtalet innehåller till exempel detaljerade säkerhetskrav på personuppgiftsbiträdet och en tydlig reglering av anlitande av underbiträden. Det saknas en fast tidsfrist för incidentrapportering (”utan onödigt dröjsmål”), vilket skulle kunna åtgärdas vid nytt avtal.

Leverantörsuppföljning

Leverantörsgranskning har inte genomförts för att följa upp och kontrollera att leverantören lever upp till avtalet och GDPR.

Slutsats och rekommendationer

Sammanfattningsvis visar granskningen av personuppgiftsbiträdesavtalen att avtalen i allt väsentligt uppfyller kraven enligt artikel 28 GDPR. DSO noterar att vissa av avtalen använder Stockholms stads mall för personuppgiftsbiträdesavtal. Genom att använda dessa mallar som grund kan Miljö- och hälsoskyddsnämnden säkerställa att avtalet är granskat av jurister och innehåller lämpliga klausuler. DSO uppmuntrar att i de fall det är möjligt använda Stockholms stads mall.

I flera avtal saknas en fast tidsfrist för incidentrapportering, vilket kan ses över vid framtida avtal. Det är inget krav med en sådan tidsfrist enligt GDPR, men det kan förbättra förutsättningarna för hantering av incidenter.

En annan brist är att leverantörsgranskning inte har genomförts av Miljöförvaltningens personuppgiftsbiträden, vilket innebär att det saknas en systematisk uppföljning av att leverantörerna verkligen efterlever avtalen och GDPR. För att säkerställa ett fortsatt gott dataskydd bör Miljöförvaltningen införa rutiner för regelbunden leverantörsuppföljning och överväga att inkludera en tydlig tidsfrist för incidentrapportering i framtida avtal.

DSO rekommenderar att skapa förutsättningar för regelbunden, riskbaserad leverantörshantering. Det kan till exempel inkludera att förtydliga den lokala anvisningen för informationssäkerhet med ansvar och rutiner avseende leverantörsgranskning, ställa krav att granskning ska ingå i objektplanen och att ta fram mallar för leverantörsgranskning (självvärdering) eller rutiner för andra metoder av granskning. Hur ofta leverantörsgranskning behöver ske, och hur omfattande en sådan leverantörsgranskning ska vara, är beroende av hur hög risken är för personuppgiftsbehandlingen som personuppgiftsbiträdet gör för den personuppgiftsansvariges räkning.