Stockholms stad

Bilaga 7

GDPR Årsrapport

År 2024

Miljö- och hälsoskyddsnämnden

GDPR årsrapport
Januari 2025

Dnr: 2025-51
Utgivningsdatum: 2025-01-08
Kontaktperson: Sofia Rohdin

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

Som DSO vid Miljö- och hälsoskyddsnämnden i Stockholms stad lämnar jag härmed en årsrapport som täcker sex obligatoriska rapporteringsområden och två ytterligare granskningsområden.

DSO har under året getts god insyn i dataskyddsarbetet genom intervjuer och möten med GDPR-gruppen, kontinuerlig kontakt med informationssäkerhetssamordnaren vid personuppgiftsincidenter, mejlkontakt med verksamhetens enhetschefer samt Stockholms stads intranät. DSO bedömer att Miljöförvaltningen vid Stockholms stad bedriver ett dataskyddsarbete på en god nivå.

DSO helhetsbedömning är att verksamheten i hög utsträckning uppfyller dataskyddsförordningens krav. Det finns dock vissa brister. DSO ger i årsrapporten ett antal rekommendationer, både kopplade till de sex obligatoriska granskningsområdena och ytterligare granskningar som genomförts. DSO rekommenderar följande:

- DSO rekommenderar att verksamheten sprider information om tillåten och otillåten användning av AI till medarbetare för att minska risken för olaglig personuppgiftsbehandling och obehörigt röjande av personuppgifter.
- DSO rekommenderar att verksamheten utreder om samtliga personuppgiftsbehandlingar är informationsklassade, och kontrollerar om genomförda klassningar tar personuppgifter i beaktning på ett lämpligt sätt.
- DSO rekommenderar att verksamheten genomför en översyn av befintliga konsekvensbedömningar i syfte att kontrollera om de är aktuella eller kräver uppdatering.
- DSO rekommenderar att verksamheten genomför en tröskelanalys av den del av behandling av anställdas personuppgifter som omfattar känsliga personuppgifter. Om verksamheten inte identifierar något relevant undantag i dataskyddsförordningen rekommenderar DSO att verksamheten genomför en konsekvensbedömning avseende dataskydd.
- DSO rekommenderar att verksamheten säkerställer att eventuella begäranden om radering från registrerade kan hanteras, specifikt radering från backups.

- DSO rekommenderar att fortsätta utbilda medarbetare om riskerna med personuppgiftsbehandling, om personuppgiftsincidenter och god dataskyddspraxis.
- DSO rekommenderar att verksamheten snarast tillser att registrerade ges information om personuppgiftsbehandling vid användning av verksamhetens e-tjänster.
- DSO rekommenderar att verksamheten uppdaterar informationen till anställda om behandlingen av deras personuppgifter i enlighet med artiklarna 12–14 i dataskyddsförordningen. Verksamheten bör överväga att ge informationen i lager för att tillgängliggöra den ytterligare.
- DSO rekommenderar att verksamheten säkerställer att samtliga rekommenderade åtgärder från tidigare årsrapport åtgärdas.

3 Obligatoriska granskningsområden

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	132
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

I artikel 30 dataskyddsförordningen anges en skyldighet för varje personuppgiftsansvarig och personuppgiftsbiträde att upprätta ett register över samtliga personuppgiftsbehandlingar som utförs under dess ansvar.

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas som säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

Det är viktigt att personuppgiftsansvarige får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och

riskbaserade dataskyddsarbete. Man kan styra insatserna där de gör störst nytta.

Syftet med detta rapporteringsområde är således att rapportera till personuppgiftsansvarige hur väl verksamhetens har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som personuppgiftsansvarige behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

132 behandlingar har registrerats i registerförteckningen.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Den senaste versionen av registerförteckningen som har tillhandahållits DSO är daterad till den 4:e december 2024. Under årets samtliga 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.

DSO bedömer hur fullständig registerförteckningen är

DSO bedömer att registerförteckningen är att anse som fullständig. Det har under tillsynen framgått hur verksamheten jobbar med registerförteckningen. DSO ser det som värdefullt att samordnande av registerförteckningen inom verksamheten är Arkiv och registratur då det finns hög sannolikhet för att den delen av verksamheten har god kännedom om vilken informationshantering som sker i allmänhet inom verksamheten. Detta talar ytterligare för att registerförteckningen med hög sannolikhet är fullständig.

Att registerförteckningen innehåller information om var personuppgifterna behandlas, vilka handlingstyper som generellt

förekommer i respektive behandling och tidsfrister för radering på samtliga behandlingar är tecken på hög dataskyddsmognad. I mångt och mycket går det att relatera registerförteckningen till verksamhetens dokumenthanteringsplan, vilket även det är positivt då det bland annat kan leda till goda synergieffekter i informationshanteringen över lag.

Utöver detta har DSO genomfört stickprovskontroller för att kontrollera att viktiga behandlingar inte saknas i registerförteckningen. Kontrollerna visade att behandlingar inte saknas.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

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

3.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.1.5 DSO ger råd och rekommendationer till PUA

DSO har inte noterat några brister kopplade till registerförteckningen.

DSO konstaterar dock att formatet för registerförteckningen är något oöverskådligt. DSO:s förbättringsförslag är att göra om registerförteckningen till tabellform för att öka överskådligheten och sökbarheten.

DSO rekommenderar att verksamheten fortsätter arbeta löpande med registerförteckningen på så sätt som verksamheten redan gör och upprätthåller den medvetenhet som finns i verksamheten om anmälan om ny personuppgiftsbehandling. Ett effektivt sätt att upprätthålla detta är troligen att regelbundet påminna verksamhetens informationsägare och enhetschefer, vilka är de som är mest sannolika att vara ansvariga för och känna till nya eller förändrade personuppgiftsbehandlingar.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i Dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna *visa* att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?
DSO konstaterar likt föregående år att verksamhetens styrdokument omfattar en stor del av dataskyddsområdet.

DSO har tidigare år granskat följande styrdokument:

- Rutin och vägledning vid händelse av en personuppgiftsincident
- Samtycke/modellavtal vid fotografering: mall för modellavtal och mall för samtycke
- Rutin för att hålla Artikel 30-registret uppdaterat
- Rutin för tillvaratagande av de registrerades rättigheter
- Rutin för konsekvensbedömning enligt artikel 35 dataskyddsförordningen
- Rutin vid begäran om registerutdrag och mall för information vid registerutdrag
- Rutin för elektronisk information
- Handbok för molntjänster
- Ansökan för användning av ny molntjänst
- Riktlinjer för sociala medier

I föregående årsrapport identifierade DSO att det saknades dokumentation som beskriver den interna GDPR-gruppens arbetsuppgifter. Under mars 2024 utarbetade verksamheten dokumentation i enlighet med DSO:s rekommendation: ”GDPR-gruppen på Miljöförvaltningen”.

DSO konstaterar att de styrdokument som finns ger en stark grund för verksamhetens dataskyddsarbete.

Vidare ser DSO att informationsinsatser och instruktioner till användare om användningen av AI-verktyg kan vara påkallat med hänsyn till ökningen av användningen av generativ AI så som ChatGPT och Copilot vilket kan leda till risker för individer. Användning av denna typ av lättillgängliga AI-verktyg (LLM) kan leda till otillåten behandling av personuppgifter, till exempel tredjelandsöverföring och obehörig åtkomst. I dagsläget finns en information på Stockholms stads intranät, men den kan vara svår att hitta (tillbaka till).[1] DSO bedömer att informationen bör kompletteras.

[1] Stadens arbete med AI, Stockholms stads intranät, uppdaterad 2024-09-17, https://intranat.stockholm.se/organisation-och-styrning/utveckling-och-kvalitet/it-

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

I föregående GDPR Årsrapport rekommenderade DSO att dokumentet ”Riktlinjer för sociala medier – Miljöförvaltningen” uppdateras med en hänvisning till vilket verktyg som ska användas för inhämtning av samtycke. DSO rekommenderade i samma årsrapport att dokumentet ”Ansökan användning av ny molntjänst” uppdateras med en justering av en rubrik. Verksamheten har under 2024 genomfört uppdateringar av bägge dokument i enlighet med DSO:s rekommendationer.

Det sedan i år nya dokumentet ”GDPR-gruppen på Miljöförvaltningen” beskriver den gruppens ansvar och uppdrag samt sammansättning. DSO bedömer att PM:n ”GDPR-gruppen på Miljöförvaltningen” på ett tillfredsställande sätt beskriver gruppens arbetsuppgifter i enlighet med DSO:s rekommendation föregående år.

DSO bedömer fortsatt att innehållet i verksamhetens dokument håller god kvalitet. Rutinerna är överskådliga, lättillgängliga, omfattande och är utformade för att kunna användas av samtliga anställda. DSO bedömer att dokumenten är relevanta och uppdaterade.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

och-digitalisering/stadens-arbete-med-ai/?f_id=169#anvandning-av-ai-tjanster-som-chatgpt, hämtad 2024-12-17.

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att fortsätta arbetet med implementera styrdokument för dataskydd där behov finns och att hålla styrdokument uppdaterade.

DSO rekommenderar att verksamheten sprider information om tillåten och otillåten användning av AI till förvaltningens medarbetare. DSO noterar att befintliga styrdokument reglerar användningen men DSO bedömer att konkret information om användning av AI-verktyg är motiverat på grund av de aktuella riskerna.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	DSO har inte fått information om detta.
Är klassade personuppgiftsbehandlingar aktuella?	-

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att en klassning faktisk initieras.

Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar *personuppgifter* är av intresse för DSO:s årsrapportering.

3.3.3 Resultat

I föregående årsrapport rekommenderade DSO att verksamheten ska fortsätta med sitt informationsklassningsarbete och att informationsklassningen av verksamhetens diskar och e-post ska fullföljas. I november färdigställde verksamheten

informationsklassningarna av personuppgiftsbehandlingen på de gemensamma diskarna samt e-post.

I samband med informationsklassningen har verksamheten också genomfört en riskanalys av e-posten där de identifierat risker och identifierat hur riskerna ska åtgärdas. DSO bedömer att verksamheten har identifierat relevanta risker som uppkommer vid personuppgiftsbehandling i epostsystem.

Det har i intervjuer under granskningsperioden framkommit att informationsklassning skett av alla system, vilket innebär att näst intill alla personuppgiftsbehandlingar har informationsklassats. Enligt den lokala tillämpningsanvisningen för informationssäkerhet ska informationsägaren eller objektägaren årligen i samverkan med ISAM dokumentera att man sett över om det behövs en ny klassning. DSO har inte fått information om att så inte skett. DSO uppfattar därmed klassningarna som aktuella. Förutsatt att klassningarna sker i enlighet med tillämpningsanvisningen har lämpliga tekniska och organisatoriska åtgärder vidtagits även för personuppgiftsbehandlingarna.

Det ska dock noteras att DSO i föregående årsrapport rapporterade att DSO inte hade fått uppgift om hur många av personuppgiftsbehandlingarna har informationsklassats. I år rapporterar DSO samma sak. DSO bedömer därför att det finns risk att ett antal personuppgiftsbehandlingar inte har klassats. Om informationsklassning inte sker, eller om informationsklassningen inte tar hänsyn till personuppgifternas art, omfattning, sammanhang och ändamål finns sämre förutsättningar att välja lämpliga tekniska och organisatoriska åtgärder som skyddar personuppgifterna.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten utreder om samtliga personuppgiftsbehandlingar är informationsklassade. Detta inkluderar att kontrollera om de klassningar som har genomförts tar i beaktning eventuell personuppgiftbehandlings art, omfattning, sammanhang och ändamål. I den mån verksamheten upptäcker att eventuella personuppgiftsbehandlingar inte har informationsklassats, eller informationsklassningarna är inaktuella, rekommenderar DSO att dessa informationsklassificeras. En lämplig plats för att dokumentera om och när en informationsklassning av en personuppgiftsbehandling har skett kan till exempel vara registerförteckningen.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej
Är de genomförda bedömningarna aktuella?	Ja

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom uttryckligen angivet i GDPR och ska utföras för alla nya behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). Det är viktigt att personuppgiftsansvarige genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

DSO har blivit informerad att verksamheten har genomfört tre konsekvensbedömningar. En miljöförvaltnings verksamhet är inte typiskt sådan att den hanterar stora mängder känsliga

personuppgifter eller genomför andra typer av personuppgiftsbehandlingar som medför en skyldighet att genomföra konsekvensbedömningar ofta.

DSO noterar att verksamheten inte har genomfört en konsekvensbedömning av behandling av anställdas personuppgifter, till exempel för administrationen av anställningsförhållandet, inkluderat rapportering av närvaro och frånvaro (t ex sjukfrånvaro).[2] Om personuppgiftsbehandling uppfyller minst två av kriterierna i IMY:s förteckning[3] ska en konsekvensbedömning göras om det inte finns ett undantag i artikel 35.3 eller artikel 35.10. Behandling av anställdas personuppgifter omfattar behandling av känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen (t ex hälsouppgifter). Det betyder att personuppgiftsbehandlingen av anställdas personuppgifter uppfyller två kriterium:

- kriterium 4, behandling av känsliga personuppgifter, och
- kriterium 7, behandling av personuppgifter om personer i underläge eller i beroendeställning, till exempel anställda.

Således finns en skyldighet att genomföra en konsekvensbedömning avseende dataskydd åtminstone för den behandling av anställdas personuppgifter som omfattar behandling av känsliga personuppgifter. I Stockholms stad är det respektive nämnd eller styrelsen i det bolag som hanterar personuppgifterna som är den personuppgiftsansvarige. Det åligger den personuppgiftsansvarige att genomföra en konsekvensbedömning avseende dataskydd i de fall personuppgiftsbehandlingen sannolikt leder till en hög risk för registrerade.[4] DSO noterar att personalsystemet tillhandahålls Miljöförvaltningen av Stockholms stad centralt, vilket dock inte förändrar den personuppgiftsansvariges skyldighet att genomföra en konsekvensbedömning.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Konsekvensbedömning har genomförts på tre av verksamhetens behandlingar. DSO bedömer att en konsekvensbedömning saknas.

---

[2] Verksamheten har genomfört en konsekvensbedömning av flextidssystemet Avista.
[3] Förteckning enligt artikel 35.4 i Dataskyddsförordningen, diarienr DI-2018-13200, Integritetsskyddsmyndigheten, 2019-01-16, https://www.imy.se/globalassets/dokument/ovrigt/forteckning---konsekvensbedomningar.pdf, hämtad 2024-12-03.
[4] Artikel 35 i Dataskyddsförordningen.

Är de genomförda konsekvensbedömningarna aktuella?

De befintliga konsekvensbedömningarna genomfördes för 2-4 år sedan. Under intervjuer i samband med granskning har det framkommit att personuppgiftsbehandlingarna och/eller systemen som har konsekvensbedömts inte har förändrats nämnvärt. Därav bedömer DSO att konsekvensbedömningarna åtminstone inte är inaktuella.

Det har framkommit att verksamheten inte har som rutin att gå igenom befintliga konsekvensbedömningar i syfte att uppdatera dem vid behov. Det är viktigt att konsekvensbedömningar ses som levande dokument då den allmänna riskbilden, system och personuppgiftsbehandlingen kan ändras vilket kan kräva ändrade säkerhetsåtgärder. Under tillsynen har GDPR-gruppen konstaterat att de ska implementera en sådan rutin, vilket DSO ser positivt på.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.4.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten gör en översyn av befintliga konsekvensbedömningar i syfte att kontrollera om någon av dem behöver revideras.

DSO rekommenderar även att verksamheten genomför en tröskelanalys för den del av behandling av anställdas personuppgifter som omfattar känsliga personuppgifter. Om verksamheten inte identifierar något undantag rekommenderar DSO att verksamheten genomför en konsekvensbedömning avseende dataskydd i enlighet med artikel 35 och IMY:s förteckning över när en konsekvensbedömning ska göras. DSO är tillgänglig för att ge råd.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1 (begäran om registerutdrag)
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	1

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt garanterar att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den personuppgiftsansvarige tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens organ lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera även att det finns undantagssituationer angivna i artikel 12.3, där svarsfristen kan förlängas till mer än en månad.)

Dataskyddombudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd i hur processer och rutiner för att tillgodose rättigheterna bör utformas.

Om verksamheten inte klarar av att hantera en begäran från registrerade personer i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från IMY:s sida, med sanktioner som följd. Det är därför viktigt att personuppgiftsansvarige regelbundet ges en bild av i vilken mån

verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

DSO uppfattar det som att verksamheten ur ett helhetsperspektiv har god kunskap och goda förutsättningar att hantera begäran från registrerade. Det finns dokumenterade rutiner och ansvariga som handlägger begäran bedöms ha en god förmåga att hantera begäranden.

I intervjuer som genomfördes under granskningsperioden framkom viss osäkerhet hos verksamheten angående hur radering av personuppgifter från Stockholms stads IT-driftsleverantörs backups kan fullföljas om det blir aktuellt. Radering innebär enligt Datalagskommittén att uppgifter ska förstöras så att de inte kan återskapas.[5] Om backups raderas efter en tidsbestämd tid av IT-driftsleverantören skulle detta kunna vara ett sätt att fullfölja radering. Med hänsyn till tidsfristen vid en eventuell begäran om radering är det viktigt att känna till förutsättningarna och tillvägagångssättet för hantering av en begäran om radering innan en sådan inkommer eftersom det annars kan leda till att begäran hanteras inkorrekt eller försenat. Utöver detta bedömer DSO som nämnt att verksamhetens förmåga att hantera en begäran om radering är god.

Föregående år gav DSO förbättringsförslag på strukturen på webbformuläret där registrerade kan göra begäranden för att tillvarata sina rättigheter enligt dataskyddsförordningen. Verksamheten har genomfört dessa förbättringar i enlighet med DSO:s rekommendation.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder

[5] SOU 1997:39, s 403.

X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.5.5 DSO ger råd och rekommendationer till PUA

DSO bedömer verksamhetens förmåga att hantera begäranden från registrerade som god. DSO:s råd för att säkerställa att eventuella framtida begäranden om radering kan hanteras är att säkerställa att radering av personuppgifter även kan ske från eventuella backups. DSO föreslår att relevanta objektägare i verksamheten kontaktar Stadsledningskontoret eller IT-driftsleverantören och frågar om de tekniska förutsättningarna, och därefter dokumenterar hur verksamheten ska gå till väga vid en begäran i Rutin för hantering av begäran. Om radering från backup inte är möjlig bör verksamheten på annat sätt säkerställa att personuppgifterna inte är åtkomliga, till exempel säkerställa att personuppgifter inte återskapas från backups efter en begäran om radering har hanterats. Även detta bör dokumenteras.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom att någon berörd rapporterar in
Hur många personuppgiftsincidenter har dokumenterats?	6
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Ej aktuellt

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskydds-förordningen (artikel 4.12) ”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.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en god personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att flera personuppgiftsincidenter ska rapporteras till IMY, och då inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål.

Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering även till de berörda personerna.

Om en organisation brister i förmåga att rapportera personuppgiftsincidenter i tid kan det leda till sanktioner från IMY:s sida. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för den egna organisationen att förbättra sin personuppgiftshantering genom systematiskt kvalitetsarbete och för tillsynsmyndigheten (IMY) att kontrollera efterlevnaden. Bristande dokumentation är sanktionsgrundande.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

Av de sex personuppgiftsincidenter som har dokumenterats under tillsynsåret har ingen av personuppgiftsincidenterna rapporterats till IMY eller till berörda personer. DSO bedömer att riskbedömningarna av incidenterna, att det har varit osannolikt att incidenterna har medfört en risk för registrerades fri- och rättigheter, har varit korrekta. Majoriteten av de upptäckta personuppgiftsincidenterna är felskickade mejl eller dokument som inträffat på grund av den mänskliga faktorn.

DSO konstaterar att verksamhetens hantering av personuppgiftsincidenter är välfungerande. Verksamheten har dokumenterade rutiner, kunskap och förutsättningar att hantera incidenter.

Både 2023 och 2024 har antalet personuppgiftsincidenter varit lågt (åtta respektive sex) i förhållande till storleken på den personuppgiftsansvariges verksamhet. Det finns en risk att detta beror på mörkertal med anledning av bristande insikt hos tjänstemännen och att det låga antalet incidenter beror på att de inte upptäcks. I föregående årsrapport rekommenderade därför DSO verksamheten att lägga särskilt fokus på att sprida kunskap om vad en personuppgiftsincident är och hur de ska hanteras.

Under 2024 har verksamheten genomfört ett antal insatser för att informera personuppgiftsincidenter. Utöver att verksamheten har lyft personuppgiftsincidenter under den årliga fysiska utbildningen om dataskydd och informerat i ett nyhetsbrev visar DSO:s granskning att majoriteten av enhetscheferna i verksamheten har informerat medarbetare genom mejl, på enhetsmöten och/eller i medarbetarsamtal. Enhetscheferna har även påmint och följt upp om Stockholms stads obligatoriska utbildning om dataskydd i vilken personuppgiftsincidenter är ett avsnitt. DSO uppfattar att informationsinsatserna genom dess bredd av kanaler sannolikt har nått den största majoriteten av verksamhetens medarbetare och bör ge en god förmåga att upptäcka och anmäla personuppgiftsincidenter.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

DSO noterar att det fortsatt är ett lågt antal internt rapporterade personuppgiftsincidenter. Det kan, liksom nämnt i föregående årsrapporter, bero på olika saker. DSO rekommenderar att fortsätta sprida kunskap regelbundet om vad personuppgiftsincidenter är och hur de ska hanteras i nyhetsbrev, fysiska utbildningar och under enhetsmöten.

Med hänsyn till att de flesta dokumenterade personuppgiftsincidenter har orsakats av den mänskliga faktorn, rekommenderar DSO att verksamheten utbildar medarbetare om riskerna med personuppgiftsbehandling. Detta inkluderar särskilt att vara noggrann vid val av mottagare på ett mejl som innehåller personuppgifter och/eller att välja andra sätt att dela personuppgifter bortsett från mejl i de fall det är möjligt.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Granskning 1 – Implementering av åtgärder från förra årets tillsynsrapport*
- *Granskning 2 – Information till registrerade*

4.2 Syfte

En av dataskyddsombudets centrala uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En viktig del av detta arbete är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten behöver fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarige är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under tillsynsåret och vad resultaten av granskningarna är.

4.3 Genomförda granskningar och deras resultat

Granskning 1 – Implementering av åtgärder från förra årets tillsynsrapport

I föregående årsrapport identifierade DSO ett antal åtgärder som PUA inte implementerat från tidigare årsrapporter:

1. informationsklassning av samtliga personuppgiftsbehandlingar.
2. Att problemen kring de kommuninterna personuppgiftsansvaren skulle åtgärdas

Avseende nr. 1: Verksamheten har under året arbetat med att informationsklassa epostsystemet MS Outlook och de gemensamma gruppdiskarna. DSO konstaterar att verksamheten har implementerat tidigare års rekommendationen.

Avseende nr. 2: Under året har frågan om fördelningen av det kommuninterna personuppgiftsansvaret ännu inte lösts fullt ut. I intervjuer under granskningsperioden har det framkommit att denna otydlighet kan försvåra verksamhetens dataskyddsarbete, särskilt eftersom det blir svårt att avgöra vem som ansvarar för vad. För att

stödja verksamheten i att hantera detta avser DSO under 2025 att prioritera detta område. Arbetet kommer dels att inkludera stödinsatser under året, dels en uppföljande granskning vid årets slut.

DSO rekommenderade i föregående årsrapport efter granskning av anställdas användning av e-post på arbetet att:

3. 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.

Avseende nr. 3: DSO noterar att verksamheten under året har genomfört en informationsklassning och riskanalys av epostsystemet och personuppgiftsbehandlingarna däri. Riskanalysen omfattade även att verksamheten identifierade mitigerande åtgärder som minskar de risker som verksamheten valde att inte hantera. Informationsklassningarna slutfördes under november 2024. Verksamheten avser att nu arbeta med att implementera de åtgärder som identifierades, varav en av dessa är tydlig information till anställda.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Granskning 2 – Information till registrerade

Bakgrund

Principen om öppenhet är en av Dataskyddsförordningens grundläggande principer[6] och registrerade har rätt till information om behandling av deras personuppgifter. Rätten till information är omfattande och framgår av artiklar 12-14 i dataskyddsförordningen, den har även utvecklats i tillsynsbeslut, vägledningar och EU-domstolens praxis. Den registrerade har rätt att få information om

[6] Artikel 5.1 i Dataskyddsförordningen.

behandling av deras personuppgifter vid insamling eller inom en rimlig period efter det att personuppgifterna har erhållits.[7]

Resultat
DSO har granskat information om personuppgiftsbehandling till två kategorier av registrerade. Den första granskningen omfattade information som ges till medborgare som använder Miljöförvaltningens e-tjänster. Den andra granskningen omfattade information som ges till anställda vid Miljöförvaltningen.

Information till registrerade som använder Miljöförvaltningens e-tjänster
Information om personuppgiftsbehandling till registrerade som använder Miljöförvaltningens e-tjänster på webben visade brister i informationsgivningen. Kontrollen visade att i e-tjänsterna Anmälan om brister i livsmedelshantering och Anmälan om matförgiftning saknades information om personuppgiftsbehandling enligt dataskyddsförordningens krav. I e-tjänsten ”Anmälan om matförgiftning” kan känsliga personuppgifter samlas in och behandlas då uppgift om matförgiftning avslöjar uppgifter om personens hälsa vilket är känsliga personuppgifter enligt artikel 9. För att säkerställa att personuppgiftsbehandlingen följer dataskyddsförordningens grundläggande princip om öppenhet[8] och artikel 13 måste organisationen tillse att den registrerade får information om personuppgiftsbehandlingen vid insamling i e-tjänsterna. Det kan göras genom kort information i e-tjänsten samt länk till Miljö- och hälsoskyddsnämndens fullständiga information.[9]

DSO noterar att den information som finns på hemsidan om Miljöförvaltningens personuppgiftsbehandling håller god kvalitet. Sannolikheten är dock låg att registrerade hittar till den vid användning av e-tjänsterna, och därmed vid insamlingstillfället av deras personuppgifter.

Information till anställda om behandlingen av deras personuppgifter
DSO har granskat den information som beskriver personuppgiftsbehandling om anställda.[10] Anställda får information

[7] Förtydligande och mer detaljer när personuppgifter inte erhålls från den registrerade själv framgår av artikel 14.3 a)-c) i dataskyddsförordningen.
[8] Artikel 5.1 i dataskyddsförordningen.
[9] Behandling av personuppgifter på Miljöförvaltningen, Stockholms stad, Behandling av personuppgifter på miljöförvaltningen - Stockholms stad, uppdaterad 2024-06-19, hämtad 2024-12-17.
[10] En mer omfattande dokumentation av granskningen, inklusive DSO:s råd, har skickats till verksamheten den 30:e december 2024.

om behandling av deras personuppgifter i ett välkomstpaket när de anställs. Informationen är kortfattad och översiktlig, men ofullständig. Det saknas information om lagringstid och exempelvis är informationen om ändamålen för personuppgiftsbehandlingen inte tillräckligt detaljerad. Med tanke på att personuppgiftsbehandling av anställdas personuppgifter vanligtvis är omfattande och sker av flera olika ändamål krävs ofta en lång information om personuppgiftsbehandlingen för att den ska kunna anses vara fullständig. Verksamheten behöver uppdatera informationen för att den ska uppfylla informationskraven i dataskyddsförordningen.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten säkerställer att samtliga rekommenderade åtgärder från tidigare årsrapport implementeras, inkluderat att ge tydlig information till anställda om hantering av sin e-post i enlighet med dataskyddsförordningen och lagstiftning om allmänna handlingar.

DSO rekommenderar verksamheten att snarast komplettera de ovan nämnda e-tjänsterna med kort information om personuppgiftsbehandling och hänvisning med länk till den fullständiga informationen på hemsidan.[11]

DSO rekommenderar slutligen verksamheten att revidera informationen till anställda om behandlingen av deras personuppgifter. Informationen ska omfatta vad som föreskrivs i artiklar 13-14 och bör ges i enlighet med artikel 12. Verksamheten bör överväga att ge informationen i lager för att tillgängliggöra den

[11] Behandling av personuppgifter på Miljöförvaltningen, Stockholms stad, Behandling av personuppgifter på miljöförvaltningen - Stockholms stad, uppdaterad 2024-06-19, hämtad 2024-12-17.

omfattande information som fullständig dataskyddsinformation ofta innebär.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:
DSO har inte identifierat eller blivit uppmärksammad på några risker i verksamheten som inte redan är nämnda ovan i rapporten.

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. DSO behöver som underlag för sin planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, gällande verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

5.4 DSO ger råd och rekommendationer till PUA

DSO har i dagsläget inte uppmärksammat några risker utöver de i årsrapporten nämnda. DSO rekommenderar att genomföra de åtgärder som beskrivits i förevarande årsrapport och att fortsätta verksamhetens pågående dataskyddsarbetet för att på så sätt stärka registrerades rättigheter ytterligare.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granskning 1 – Översyn av det kommuninterna personuppgiftsansvarets fördelning*
- *Granskning 2 – Personuppgiftsbiträdesavtal*
- *Granskning 3 – Implementering av åtgärder från GDPR Årsrapport 2024*

6.2 Syfte

Syftet med de tre granskningarna är att stärka Miljöförvaltningens dataskyddsarbete genom att skapa tydlighet och säkerställa efterlevnad av dataskyddsförordningen i centrala områden.

Granskningarna syftar till att:

- Säkerställa att personuppgiftsansvaret och ansvarsfördelningen är korrekt reglerad och praktiskt hanterad, både i relation till externa personuppgiftsbiträden och i kommuninterna samarbeten.
- Utvärdera implementering av åtgärder från GDPR Årsrapport 2024 för att säkerställa att verksamheten arbetar med påtalade risker.

Genom att identifiera eventuella brister och föreslå förbättringar i dessa tre områden förväntas verksamhetens förmåga att skydda registrerades rättigheter och hantera personuppgifter på ett ansvarsfullt och lagligt sätt stärkas.

6.3 Planerade granskningar

Granskning 1 – Översyn av det kommuninterna personuppgiftsansvarets fördelning

Granskningen syftar till att göra en översyn av och analysera det kommuninterna personuppgiftsansvarets fördelning, och hateringen av detta. Kommunens komplexa organisation och PM3-modellen i vilken systemförvaltningen organiseras skapar vissa utmaningar för säkerställandet av att Miljö- och hälsoskyddsnämnden uppfyller de krav som ställs på den i egenskap av den personuppgiftsansvarige.

Syftet med granskningen är att identifiera eventuella otydligheter och brister i hanteringen av det kommuninterna personuppgiftsansvaret. 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 vilka 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 Miljöförvaltningen hanterar.

Den här granskningen är, innan den inleds, något svår att definiera men kommer sannolikt att inkludera:

- En kartläggning av vilka centrala tjänster (exempelvis IT-tjänster) som levereras till Miljöförvaltningen, och hur personuppgiftsansvaret är reglerat i dessa relationer.
- En genomgång av avtal, överenskommelser och rutiner som reglerar rollerna som personuppgiftsansvarig och personuppgiftsbiträde (etc) mellan de involverade förvaltningarna/bolagen.
- Intervjuer med nyckelpersoner från Miljöförvaltningen och andra aktuella aktörer, bland annat Stadsledningskontoret och relevanta objekt.
- En bedömning av nuvarande situation och förbättringsförslag för att stärka Miljöförvaltningens förutsättningar att arbeta effektivt och organiserat med dataskydd.

Värdet för den personuppgiftsansvarige förväntas vara insikt i hur personuppgiftsansvaret är fördelat och hanterat i kommuninterna relationer där personuppgifter behandlas. Resultatet förväntas bidra till förbättrad tydlighet och kontroll i personuppgiftsansvaret, minskad risk för att dataskyddsförordningens krav inte uppfylls på grund av otydligheter i ansvarsfördelningen och förbättringsförslag.

Förutsättningar för granskningen är:

- Tillgång till relevanta avtal, instruktioner och styrdokument mellan Miljöförvaltningen och Stadsledningskontoret och eventuella andra förvaltningar/bolag.
- Dialog med representanter från Miljöförvaltningen, Stadsledningskontoret och relevanta objekt för att förstå hur ansvarsfördelningen och dataskyddsarbetet fungerar i praktiken.

Granskning 2 – Personuppgiftsbiträdesavtal

Syftet med granskningen är att säkerställa att Miljöförvaltningens personuppgiftsbiträdesavtal (PUB-avtal) uppfyller de krav som ställs i dataskyddsförordningen enligt 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.

Granskningen innebär:

- 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 omfattar alla verksamhetsområden som använder externa leverantörer för behandling av personuppgifter.

Målet är att ge den personuppgiftsansvarige en tydlig översikt över befintliga PUB-avtal och dess kvalitet, samt eventuell avsaknad av PUB-avtal. Då DSO även planerar att göra en översyn av det kommuninterna personuppgiftsansvarets fördelning och hanteringen av detta bedömer DSO att granskning av PUB-avtal, eller eventuell avsaknad av dessa, är ett bra komplement till detta.

Förutsättningar för granskningen är:

- Tillgång till samtliga befintliga PUB-avtal.
- En översikt över verksamhetens personuppgiftsbiträden/leverantörer,
- Medverkan från ansvariga för olika områden för att beskriva respektive personuppgiftsbehandling som PUB-avtalet reglerar.

Granskning 3 – Implementering av åtgärder från GDPR årsrapport 2024

Syftet med granskningen är att följa upp hur väl verksamheten har implementerat de åtgärder som identifieras och rekommenderas i förevarande årsrapport.[12] Uppföljning är en central del av dataskyddsarbetet och bidrar till att säkerställa att påtalade brister har åtgärdats samt att föreslagna rekommendationer har genomförts.

[12] Dnr 2025-51.

DSO:s granskning kommer att innefatta:

- Genomgång av de rekommendationer och åtgärder som föreslås i förevarande årsrapport.
- Utvärdering av åtgärder som har implementerats.
- Identifiering av åtgärder som ännu inte har genomförts.
- Vid behov intervjuer med relevanta ansvariga för att få en förståelse för arbetet och eventuella utmaningar.

Granskningen berör alla verksamhetsområden som påverkas av de åtgärder som beskrivs i förevarande årsrapport. Den här granskningen avser hjälpa den personuppgiftsansvarige att få en tydlig bild över framsteg under året, samtidigt som kvarstående brister och förbättringsområden identifieras.

Förutsättning för granskningen:

- Dialog med ansvariga för implementeringen av rekommendationerna.
- Underlag som visar genomförda åtgärder, till exempel uppdaterade rutiner eller utbildningsinsatser.