Stockholms stad

Bilaga 6

Dataskyddsombudets årsrapport 2025

Kommunstyrelsen

Stockholms stad

Dataskyddsombudets årsrapport 2025
Dnr: KS 2025/1420
Kontaktperson: Diana Färje, dataskyddsombud

Sammanfattning

Dataskyddsombudets årsrapport är en sammanfattande, oberoende lägesrapport om kommunstyrelsens arbete med dataskydd under det gångna året. Syftet är att ge en samlad bild av nuläge, identifierade utvecklingsområden och förslag på åtgärder och rekommendationer i syfte att ge goda förutsättningar för fortsatt utveckling av processer och arbetssätt.

I årets rapport lyfts flera olika områden som är relevanta för kommunstyrelsens dataskyddsarbete. Dataskyddsombudet vill särskilt belysa tre utvecklingsområden. Dessa utgörs av 1) utredning, bedömning och dokumentation av personuppgiftsansvar, 2) kommunstyrelsens register över personuppgiftsbehandling och 3) översyn av befintlig stöddokumentation gällande dataskydd.

Frågan om utredning och bedömning av personuppgiftsansvar inom staden, och således hur ansvaret förhåller sig mellan stadens olika nämnder och bolag, är centralt och helt avgörande för dataskyddsarbetet i hela staden. Kommunstyrelsen, genom stadsledningskontoret, har till uppdrag är att styra, utveckla och samordna stadens verksamhet på ett strategiskt plan. Härav medförs ett förhållandevis brett inflytande över, och i många fall även ansvar för, personuppgiftsbehandlingar som sker inom ramen för stadens många olika verksamheter och verksamhetsområden. Det är angeläget att utifrån faktiska omständigheter ta ställning till hur den behandling som sker i stadens centrala it-system ska dokumenteras mellan nämnderna – i överenskommelser om gemensamt personuppgiftsansvar eller i stadeninterna instruktioner om personuppgiftsbehandling.

Bedömning och dokumentation av personuppgiftsansvar påverkar kommunstyrelsens register över personuppgiftsbehandling. Kommunstyrelsen bör under kommande år prioritera att se över nuvarande register, säkerställa att samtliga personuppgiftsbehandlingar som kommunstyrelsen är personuppgiftsansvarig för är korrekt inlagda samt ta fram tydliga rutiner som redogör för ansvar och hantering av registret.

Slutligen vill dataskyddsombudet betona vikten av att kommunstyrelsens vägledande stöddokumentation gällande dataskydd ses över och görs mer lättillgänglig. Särskild vikt bör läggas vid vägledning som rör de grundläggande principerna i dataskyddsförordningen och som behöver följas av samtliga medarbetare vid varje personuppgiftsbehandling. Det bör säkerställas att kommunstyrelsens stöddokumentation kring dataskydd är tydlig och utformad med avsikten att kunna tillämpas av varje medarbetare, oavsett förkunskaper. Det ska vara lätt att göra rätt.

Innehållsförteckning

1 Inledning

1.1 Om dataskydd och personuppgiftsansvar

Stockholms stad behandlar dagligen stora mängder personuppgifter om bland annat kommunmedlemmar och medarbetare. Staden har ett ansvar att se till att personuppgifterna behandlas på ett korrekt, säkert och ansvarsfullt sätt. Att värna om enskildas integritet är en fråga om förtroende och det är i alla avseenden angeläget att detta förtroende förvaltas väl.

Regelverket gällande personuppgiftsbehandling (rättsområdet benämns oftast *dataskydd*) är omfattande och föränderligt. Dataskyddsförordningen[1] (GDPR) syftar till att skydda individers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Dataskyddsregelverket anger de yttersta ramarna för en lagenlig behandling av personuppgifter.

Ny lagstiftning och praxis inom dataskydd föranleder ett ständigt pågående arbete inom staden för att se över och utveckla arbetssätt och ta fram vägledningar och andra stöddokument i syfte att uppnå en god systematik och tydliga processer som underlättar för verksamheterna. Ny teknik, till exempel artificiell intelligens (AI), skapar nya möjligheter för utveckling och förbättring av arbetssätt och processer, men medför även dataskyddsrättsliga utmaningar som behöver adresseras på ett ändamålsenligt sätt.

Personuppgiftsansvarig är den myndighet, det vill säga nämnd eller bolagsstyrelse inom Stockholms stad, som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige – Kommunstyrelsen i Stockholms stad – är ytterst ansvarig för att den personuppgiftsbehandling som sker under kommunstyrelsens personuppgiftsansvar sker på ett lagligt, säkert och korrekt sätt.

1.2 Om dataskyddsombudet

Varje nämnd och bolagsstyrelse i Stockholms stad har ett utnämnt dataskyddsombud. Dataskyddsombudet har till uppgift att övervaka nämndens/bolagets efterlevnad av dataskyddsregelverket samt informera och ge råd till den personuppgiftsansvarige. Dataskyddsombudet har en rådgivande och oberoende funktion i organisationen och deltar inte operativt i hantering av frågor som rör dataskydd. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå.

1.3 Om dataskyddsombudets årsrapport

En årlig rapportering från dataskyddsombudet är ett tillvägagångssätt genom vilket kommunstyrelsen ges insyn i nämndens arbete med dataskydd och därtill relaterade frågor. Genom årsrapporten tillhandahålls kommunstyrelsen information, råd och rekommendationer, vilka syftar till att underlätta fullgörandet av det ansvar som åligger kommunstyrelsen i

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

egenskap av personuppgiftsansvarig. Årsrapporten ger kommunstyrelsen förutsättningar att fatta adekvata beslut om prioriteringar, resurser och kommande initiativ inom området för dataskydd och utgör således en del av nämndens systematiska dataskyddsarbete.

I årsrapporten beskrivs sex olika rapporteringsområden för vilka det ges en kort summering av den uppföljning som gjorts utifrån rekommendationerna i föregående års rapport samt en redogörelse för hur kommunstyrelsen har arbetat med rapporteringsområdena under 2025. Därtill ger dataskyddsombudet rekommendationer kring hur kommunstyrelsen bör arbeta med respektive område under 2026.

Sammanfattningsvis utgör dataskyddsombudets årsrapport ett lättillgängligt och överskådligt underlag som ger en god bild av kommunstyrelsens arbete med integritets- och dataskyddsfrågor.

2 Årliga rapporteringsområden

Stadens dataskyddsombud utformar självständigt sina årsrapporter och styr således över innehållet, men ombeds särskilt att rapportera kring sex förbestämda rapporteringsområden. Dessa rapporteringsområden är:

- Register över personuppgiftsbehandling
- Säkerhet i samband med behandling
- Konsekvensbedömning avseende dataskydd
- De registrerades rättigheter
- Personuppgiftsincidenter
- Överföring till tredjeland

Utöver ovanstående årliga rapporteringsområdena redogör kommunstyrelsens dataskyddsombud i år även för följande områden:

- Personuppgiftsansvar inom Stockholms stad
- Styrdokument och annan vägledning
- Arkivering och gallring
- Samverkan kring dataskydd inom stadsledningskontoret samt inom staden

2.1 Register över personuppgiftsbehandling

2.1.1 Allmänt om registret över personuppgiftsbehandlingar

I enlighet med artikel 30 GDPR ska varje personuppgiftsansvarig föra ett register över personuppgiftsbehandlingar som utförts under dess ansvar, även kallat registerförteckning. Dessutom ska kommunstyrelsen även föra ett register över alla personuppgiftsbehandlingar som kommunstyrelsen utför i egenskap av personuppgiftsbiträde, det vill säga ett register över personuppgiftsbehandlingar som kommunstyrelsen utför för andra nämnders och bolags räkning.

Goda och tydliga rutiner kring registerförteckning är en förutsättning för att kommunstyrelsen ska kunna ha kontroll över de personuppgiftsbehandlingar som utförs under nämndens ansvar. Registret över personuppgiftsbehandlingar skapar förutsättningar för en intern synlighet och förståelse för vilka personuppgifter som behandlas inom nämnden och under vilka förutsättningar. Registret ligger till grund för nämndens systematiska och riskbaserade dataskyddsarbete.

Registerförteckningen är dataskyddsarbetets centrala utgångspunkt och underlättar bland annat för verksamheterna att tillse att det finns en rättslig grund för all personuppgiftsbehandling som utförs under kommunstyrelsens ansvar och att personuppgiftsbehandlingen även i övrigt är förenlig med gällande dataskyddslagstiftning. Om registerförteckningen hanteras och uppdateras korrekt kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, vilket är särskilt viktigt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

Kommunstyrelsens registerförteckning hanteras i verktyget Draftit Privacy Records. I enlighet med stadsledningskontorets lokala anvisning för informationssäkerhet ansvarar stadsledningskontorets dataskyddshandläggare för att samordna och sammanställa registerförteckningen.

Sammanfattningsvis utgör en korrekt, komplett och systematiskt uppdaterad registerförteckning en förutsättning för ett effektivt och ändamålsenligt dataskyddsarbete.

2.1.2 Årlig uppföljning av kommunstyrelsens register över personuppgiftsbehandlingar

Uppföljning	Svar/bedömning
Antal behandlingar som är registrerade?	179 st. varav: 15 st. *godkända* 11 st. *komplettering begärd* 115 st. *under bearbetning* 29 st. *redo för granskning*

	9 st. *under granskning*
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?	Nej, rutinerna bör ses över
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?	Nej
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?	Delvis. Flera av de registreringar som är *under bearbetning* saknar obligatorisk information.

2.1.3 Uppföljning av föregående års rekommendationer gällande kommunstyrelsens register över personuppgiftsbehandlingar

I 2024 års rapport framförde dataskyddsombudet att det föreligger ett stort behov av att genomföra en översyn av kommunstyrelsens registerförteckning. Som ett led i översynen rekommenderas att varje avdelning därför bör ges i uppdrag att inventera sina personuppgiftsbehandlingar och tillse att de är korrekt inlagda i kommunstyrelsens register över personuppgiftsbehandlingar (Draftit). Någon generell översyn av kommunstyrelsens register över personuppgiftsbehandlingar har inte gjorts under året, varför behovet kvarstår.

I samband med att juridiska avdelningen utvecklade en rutin för hanteringen av registerutdrag initierades det även ett arbete för avdelningarna att aktualitetspröva och komplettera uppgifterna i kommunstyrelsens registerförteckning. I oktober 2025 inleddes en förstudie under ledning av säkerhetsavdelningen i vilken man har för avsikt att kartlägga och skapa en samlad nulägesbild av stadsledningskontorets systemlandskap och personuppgiftsbehandling. Ur ett dataskyddsperspektiv, och särskilt för att få bättre förutsättningar att säkerställa kvaliteten på kommunstyrelsens register över personuppgiftsbehandlingar, ser dataskyddsombudet mycket positivt på detta initiativ. Dataskyddsombudet vill i sammanhanget lyfta vikten av att stadsledningskontoret, utöver system och objekt, behöver identifiera och dokumentera pågående *personuppgiftsbehandlingar* som kommunstyrelsen är personuppgiftsansvarig för. Det bör i detta sammanhang betonas att personuppgiftsbehandling och personuppgiftsansvar inte kan likställas med informationssäkerhet och informations- eller objektsägarskap, utan bör betraktas och hanteras ur ett dataskyddsrättsligt perspektiv. Dataskyddsombudet utvecklar dessa resonemang i avsnitt 3.1.2.

Arbetet med att lägga in nya personuppgiftsbehandlingar i kommunstyrelsens register över personuppgiftsbehandlingar samt uppdatera de befintliga har varit begränsat under året. Det är mycket angeläget att kommunstyrelsen har etablerade goda rutiner och arbetssätt för hantering av registret.

I 2024 års rapport rekommenderas vidare att kommunstyrelsen tar fram ett register över personuppgiftsbehandlingar som kommunstyrelsen utför i egenskap av *personuppgiftsbiträde*. Ett sådant register, som bör utformas i enlighet med artikel 30.2 GDPR, är ännu inte komplett.

Behovet av dokumenterade tydliga rutiner för att underlätta avdelningarnas hantering av registerförteckning kvarstår, liksom förslaget att överväga att utse en dataskyddskontakt per avdelning, som kan stötta i avdelningarnas arbete med att hålla registret över personuppgiftsbehandlingar uppdaterat.

2.1.4 Dataskyddsombudets rekommendationer gällande kommunstyrelsens register över personuppgiftsbehandlingar

1. Det finns ett betydande behov av att genomföra en grundlig översyn av kommunstyrelsens register över personuppgiftsbehandlingar. Varje avdelning bör ges i uppdrag att inventera sina personuppgiftsbehandlingar och tillse att de är korrekt inlagda i registret.

2. Dataskyddsombudet rekommenderar att kommunstyrelsen, förslagsvis den funktion som har ett operativt helhetsansvar för kommunstyrelsens register över personuppgiftsbehandlingar, vidtar de åtgärder som krävs för att säkerställa att det finns adekvata och lättillgängliga rutiner för hanteringen av registret. Av rutinen bör det framgå *att* samtliga personuppgiftsbehandlingar som sker under kommunstyrelsens personuppgiftsansvar ska läggas in i registret över personuppgiftsbehandlingar, vem som ansvarar för att så sker och att avdelningarnas befintliga registreringar ska följas upp regelbundet och uppdateras vid förändringar beträffande personuppgiftsbehandling. Det bör även finnas praktisk vägledning kring hur hanteringen av registret ska gå till i praktiken samt vägledning beträffande de frågor som ska besvaras vid ifyllnad av registret.

3. Dataskyddsombudet rekommenderar att kommunstyrelsen ser över nuvarande generella synsätt om att nämndens registerförteckningsarbete huvudsakligen säkerställs genom informationsklassningsprocessen. I informationsklassnings-processen klassas en viss informationsmängd som ska hanteras i ett visst system eller objekt. Processer och stöddokumentation för hantering av kommunstyrelsens register över personuppgiftsbehandling behöver utgå från den *personuppgiftsbehandling* (oaktat vem som är informations- eller objektägare) som kommunstyrelsen är personuppgiftsansvarig för. Följden av ett för smalt synsätt eller ett begränsat perspektiv medför en risk för att kommunstyrelsen inte identifierar och dokumenterar samtliga personuppgiftsbehandlingar.

4. För att underlätta avdelningarnas systematiska arbete med registerförteckning bör kommunstyrelsen överväga att utse en dataskyddskontakt per avdelning som, med stöd av stadsledningskontorets dataskyddshandläggare, informationssäkerhets-samordnare (ISAM) och dataskyddsombud, kan stötta avdelningarna i att hålla registret över personuppgiftsbehandlingar uppdaterat och korrekt.

5. Kommunstyrelsen bör i enlighet med artikel 30.2 GDPR ta fram en förteckning över alla kategorier av personuppgiftsbehandlingar som kommunstyrelsen utför i egenskap av *personuppgiftsbiträde*.

2.2 Säkerhet i samband med personuppgiftsbehandling

2.2.1 Allmänt om säkerhet i samband med personuppgiftsbehandling

I egenskap av personuppgiftsansvarig ska kommunstyrelsen vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med personuppgiftsbehandlingen (artikel 32 GDPR). Vid bedömning av säkerhetsåtgärder ska den personuppgiftsansvarige beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för de registrerades rättigheter och friheter.

Även vid anlitande av personuppgiftsbiträden (till exempel it-leverantörer) har den personuppgiftsansvarige det yttersta ansvaret för att personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada. Det åligger således kommunstyrelsen att säkerställa samt löpande följa upp säkerheten i den personuppgiftsbehandling som sker hos kommunstyrelsens personuppgiftsbiträden.

I enlighet med stadens riktlinjer och tillämpningsanvisningar för informationssäkerhet ska staden informationsklassa sin information. Med ”information” avses i den här kontexten även information som utgör personuppgifter. Syftet med informationsklassning är att identifiera vilket skyddsvärde en viss informationsmängd (som således ofta inbegriper personuppgifter) har och vilka skyddsåtgärder som behöver vidtas för att uppnå en adekvat nivå av säkerhet.

Stadens riktlinjer för informationssäkerhet föreskriver att stadens informationstillgångar ska vara klassade med stöd av verktyget KLASSA, som har tagits fram av Sveriges kommuner och regioner (SKR). Inom ramen för informationsklassningen tas det fram en handlingsplan enligt vilken lämpliga tekniska och organisatoriska åtgärder identifieras. Med tekniska säkerhetsåtgärder avses till exempel kryptering, pseudonymisering och säkerhetskopiering. Med organisatoriska säkerhetsåtgärder avses till exempel interna riktlinjer och rutiner.

De tekniska och organisatoriska säkerhetsåtgärder som identifieras inom ramen för informationsklassningsprocessen ligger bland annat till grund för de krav som staden ställer på nuvarande och kommande leverantörer av *it-system* i vilka det behandlas personuppgifter. Ansvaret för att vidta, upprätthålla och följa upp lämpliga säkerhetsåtgärder åligger både kommunstyrelsen själv och kommunstyrelsens personuppgiftsbiträden, men det yttersta och största ansvaret åligger alltid den personuppgiftsansvarige, det vill säga kommunstyrelsen. Således ställs höga krav på kommunstyrelsens kravställning gentemot leverantörer. De säkerhetsåtgärder som åläggs kommunstyrelsens leverantörer behöver tydligt och utförligt anges i avtal eller personuppgiftsbiträdesavtal mellan parterna. Det åligger kommunstyrelsen att löpande följa upp att anlitade personuppgiftsbiträden följer de säkerhetskrav som ställs.

Den 15 januari 2026 träder cybersäkerhetslag (2025:1506) i kraft. Den nya lagen påverkar bland annat kommunstyrelsens riskhantering och identifiering och kravställning av tekniska och organisatoriska säkerhetsåtgärder.

2.2.2 Årlig uppföljning av säkerhet i samband med personuppgiftsbehandling

Uppföljning	Svar/bedömning
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?	Nuvarande processer och styrande dokument baseras på ett informationssäkerhetsperspektiv, där säkerhetskrav och ansvar utgår från system/objekt eller informationsmängd istället för personuppgiftsbehandling. Rekommenderas en översyn. Se avsnitt 3.1.2.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?	Se ovan.

2.2.3 Uppföljning av föregående års rekommendationer gällande säkerhet i samband med personuppgiftsbehandling

I 2024 års rapport redogörs övergripande om ansvaret för tekniska och organisatoriska säkerhetsåtgärder. I enlighet med Stadsledningskontorets lokala anvisning om informationssäkerhet är det *objektägare*, med operativt stöd av *objektledare*, som ansvarar för att informationsklassning, riskanalys och eventuell konsekvensbedömning avseende dataskydd genomförs *avseende objektet* (it-tjänsten). I den lokala anvisningen redogörs för det omfattande antal moment i detta arbete som objektägare/objektledare ansvarar för, vilket inbegriper bland annat identifiering och implementering av skyddsåtgärder, uppföljning av skyddsåtgärderna samt beslut om behörighetstilldelning.

I 2024 års rapport betonas vikten av att objektägare omsorgsfullt bedömer vilka roller och funktioner som ska delta i arbetet med informationsklassningar och riskanalyser. Det är angeläget, även framöver, att det löpande säkerställs att samtliga relevanta kompetenser involveras. I de delar av processerna som rör dataskydd bör dataskyddsjurist och/eller dataskyddsombud involveras.

Informationsklassning görs inom ramen för kommunstyrelsens informationssäkerhetsarbete och det är stadsledningskontorets informationssäkerhetssamordnare (ISAM) som ansvarar för att samordna och följa upp samt stödja och ge råd vid kartläggning av information och informationsklassning och riskanalyser. I början av 2025 tillträdde en ny informationssäkerhetssamordnare vid stadsledningskontoret. Informationssäkerhetssamordnaren har varit tjänstledig sedan i höstas varför en översyn avseende befintliga processer och rutiner gällande säkerhet i samband med personuppgiftsbehandling har varit något begränsad under året.

2.2.4 Dataskyddsombudets rekommendationer gällande säkerhet i samband med personuppgiftsbehandling

Dataskyddsombudet vill påminna om vikten av att kommunstyrelsen har goda rutiner för kravställning, genomförande och uppföljning av tekniska och organisatoriska säkerhetsåtgärder, både internt och i förhållande till personuppgiftsbiträden (leverantörer). Även om det finns adekvata arbetssätt för att *identifiera* risker och säkerhetsåtgärder är det angeläget att det även är tydligt vem (vilken funktion) som ansvarar för dels *implementering* av säkerhetsåtgärder och dels *uppföljning* av säkerhetsåtgärder.

1. Inom ramen för stadens informationsklassningsprocess identifieras ofta ett stort antal krav och åtgärder, varav flera utgörs av olika slags tekniska och organisatoriska säkerhetsåtgärder. Det är angeläget att samtliga identifierade säkerhetsåtgärder vidtas och följs upp. Vilken roll eller funktion som är ansvarig för respektive risk och riskminimerande åtgärd behöver dokumenteras. Det behöver också säkerställas att den roll eller funktion som åläggs ett ansvar för att implementera eller säkerställa en viss åtgärd tydligt görs medveten om detta.

2. I stadsledningskontorets lokala anvisning för informationssäkerhet framgår att det är objektägares ansvar, med operativt stöd av objektledare, att tillse att kravställda skyddsåtgärder implementeras och att följa upp implementeringen av kravställda skyddsåtgärder. I stadens centrala tillämpningsanvisning anges att ansvaret för att skydda information i staden är decentraliserat och följer linjeansvaret. Det innebär, står det i tillämpningsanvisningen, att chefer med verksamhetsansvar har en del i detta ansvar.

   Vid några tillfällen under året har det kommit till dataskyddsombudets kännedom att det föreligger oklarheter kring ansvarsförhållandena när det kommer till kommunstyrelsens (stadsledningskontorets) lokala genomförande och uppföljning av åtgärder som identifieras inom ramen för så kallade normerande informationsklassningar (informationsklassningar som är avsedda att tillämpas av hela staden). Ofta har det rört sig om identifierade *organisatoriska* säkerhetsåtgärder, till exempel lokala anvisningar eller rutiner, vilka i anslutning till senare uppföljning visar sig inte har tagits fram lokalt vid stadsledningskontoret.

   Möjligen upplevs ansvaret som något tydligare beträffande genomförande och uppföljning av *tekniska* säkerhetsåtgärder, där det ligger nära till hands att anta att de omhändertas av objektledare (eller objektstyrgrupp), jämfört med motsvarande ansvar beträffande organisatoriska säkerhetsåtgärder, som möjligen förväntas omhändertas ”i linjen”. Ur ett dataskyddsperspektiv är det mycket angeläget att de organisatoriska säkerhetsåtgärderna omhändertas lika väl som de tekniska. Dataskyddsombudet rekommenderar att kommunstyrelsen utreder om ansvaret för genomförande och uppföljning av säkerhetsåtgärder, och särskilt hur ansvaret förhåller sig mellan objektägare och chefer med verksamhetsansvar (”i linjen”), är tillräckligt tydligt beskrivet i stadens riktlinjer och stadsledningskontorets lokala anvisningar eller om det finns andra omständigheter som bidrar till otydlighet på området.

3. Vid genomförande av konsekvensbedömningar utförs en riskanalys beträffande personuppgiftsbehandlingen i fråga. Också i denna process identifieras risker och riskminimerande åtgärder och även här behöver ansvaret för genomförande och

uppföljning av åtgärderna, samt kvarstående risk, vara tydligt beskrivet och dokumenterat. (Se även rekommendationerna som lämnas i avsnitt 2.3.4.)

I vissa fall kan det tänkas att riskminimerande åtgärder som rör säkerheten för personuppgiftsbehandling identifieras i både informationsklassningsprocessen och processen för konsekvensbedömning. Här behöver det säkerställas att det inte blir en diskrepans mellan det ansvar som dokumenteras inom för respektive process.

4. Kommunstyrelsen bör säkerställa att det finns tydliga rutiner för vilken roll eller funktion som ansvarar för uppföljning av säkerheten hos stadens *personuppgiftsbiträden* och tydliga processer för hur sådan uppföljning ska gå till i praktiken. Det bör här beaktas att det kan förekomma många olika personuppgiftsbehandlingar hos samma personuppgiftsbiträde och därmed även flera olika personuppgiftsbiträdesavtal. Om ansvaret för uppföljning av både informationssäkerhet och dataskydd ligger hos objektledare, det vill säga utgår från ansvaret för ett visst system eller objekt, är det ur ett dataskyddsperspektiv helt avgörande att objektledaren känner till samtliga personuppgiftsbehandlingar som sker hos respektive personuppgiftsbiträde (leverantör) och samtliga personuppgiftsbiträdesavtal som ligger till grund för behandlingarna.

   Olika personuppgiftsbehandlingar kan omfattas av olika krav som ej endast avser den tekniska säkerheten i ett system. Här kan exemplifieras med vikten av uppföljning beträffande *hur* och under vilka förutsättningar uppgifterna får behandlas av personuppgiftsbiträdet samt krav beträffande personuppgiftsbiträdets gallring eller radering av personuppgifterna.

   Sammanfattningsvis rekommenderas att kommunstyrelsen ser över befintliga rutiner för uppföljning av personuppgiftsbiträden (leverantörer) och säkerställer att uppföljningen omfattar både informationssäkerhetskrav och dataskyddsrättsliga krav.

5. Kommunstyrelsen behöver säkerställa att personuppgifter om registrerade med skyddade personuppgifter behandlas med extra varsamhet och på ett sätt som lever upp till kraven på lämplig säkerhet. Det behöver göras särskilt noggranna avvägningar vid bedömning av lämpliga säkerhetsåtgärder och säkerheten behöver löpande följas upp. Ju mer integritetskänslig en personuppgift är, desto mer angeläget är det att begränsa behandlingen till vad som är absolut nödvändigt för verksamhetens behov. Personuppgiftsbehandlingen ska ske i enlighet med stadens policy om skyddade personuppgifter.

6. Med anledning av den nya cybersäkerhetslagen (se avsnitt 2.2.1 ovan) är det under 2026 särskilt angeläget med en god samverkan mellan de olika kompetenser som arbetar med informationssäkerhet, cybersäkerhet och dataskydd, bland annat vid översyn och utformning av nya rutiner, processer och arbetssätt som berörs av de nya lagkraven.

2.3 Konsekvensbedömning avseende dataskydd

2.3.1 Allmänt om konsekvensbedömningar

För personuppgiftsbehandlingar som, utifrån kriterierna i artikel 35 GDPR, sannolikt leder till en *hög* risk för fysiska personers rättigheter och friheter behöver det göras en konsekvensbedömning.

Syftet med konsekvensbedömningar är att i detalj beskriva en viss personuppgiftsbehandling och därtill identifiera och dokumentera riskerna för fysiska personers rättigheter och friheter. Den personuppgiftsansvarige ska bedöma sannolikheter och konsekvenser för riskerna och identifiera vilka åtgärder som behöver vidtas för att personuppgiftsbehandlingen ska kunna ske med den nivå av säkerhet som krävs enligt gällande dataskyddslagstiftning. Om konsekvensbedömningen visar att personuppgiftsbehandlingen, trots identifierade och vidtagna tekniska och organisatoriska säkerhetsåtgärder, kommer att medföra en *hög* risk för de registrerade behöver den personuppgiftsansvarige antingen begära förhandssamråd från Integritetsskyddsmyndigheten (IMY) eller avstå från att inleda den planerade personuppgiftsbehandlingen.

Det bör uppmärksammas att föremålet för en konsekvensbedömning är en viss *personuppgiftsbehandling*. Riskerna med en personuppgiftsbehandling ska bedömas med beaktande av behandlingens *art*, *omfattning*, *sammanhang* och *ändamål*.

Under våren 2025 tog juridiska avdelningen fram en ny process för konsekvensbedömning. Processen innehåller ett metodstöd, mall för behovet av konsekvensbedömning samt mallar för konsekvensbedömning respektive referenskonsekvensbedömning. Dataskyddsombudet ser mycket positivt på att kommunstyrelsen har prioriterat att se över processen för konsekvensbedömning.

Det är av vikt att det finns goda rutiner kring uppföljningen av genomförda konsekvensbedömningar. Vid behov, till exempel vid förändringar gällande risker eller arbetssätt, behöver genomförda och upprättade konsekvensbedömningar ses över och eventuellt justeras.

2.3.2 Årlig uppföljning av konsekvensbedömningar

Uppföljning	Svar/bedömning
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?	Ja
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?	Ja, i vart fall i anslutning till bedömning av nya personuppgiftsbehandlingar.

Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?	Ja, men det föreligger ett behov av förtydliganden. Se rekommendationer i avsnitt 2.3.4 nedan.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?	Ja, när tröskelanalys visar att konsekvensbedömning krävs så är dataskyddsombudets uppfattning att konsekvensbedömning genomförs.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?	Arbete med att identifiera behovet av samt genomföra kvalitativa konsekvensbedömningar pågår löpande.

2.3.3 Uppföljning av föregående års rekommendationer kring konsekvensbedömning

Föregående års rekommendationer kvarstår. Dataskyddsombudet rekommenderar även i år att arbetet med att identifiera behovet av konsekvensbedömningar samt genomförandet av konsekvensbedömningar fortsätter under 2026.

2.3.4 Dataskyddsombudets rekommendationer gällande konsekvensbedömning

1. Dataskyddsombudet rekommenderar att arbetet med att identifiera behovet av konsekvensbedömningar samt genomförandet av konsekvensbedömningar fortsätter under 2026. Det bör prioriteras att upprätta konsekvensbedömningar för personuppgiftsbehandling som innebär särskilt hög risk, bland annat behandlingar som berör känsliga personuppgifter, skyddade personuppgifter eller användning av ny teknik, till exempel AI.

2. Enligt stadsledningskontorets lokala anvisning för informationssäkerhet är det objektägare, med operativt stöd av objektledare, som ansvarar för att eventuell konsekvensbedömning genomförs avseende *objektet*. Kommunstyrelsen bör utreda om nuvarande anvisning är ändamålsenligt utformad, och då titta särskilt på huruvida anvisningen i praktiken medför att samtliga personuppgiftsbehandlingar som kan medföra hög risk faktiskt identifieras och dokumenteras i en konsekvensbedömning i erforderlig omfattning. Om ansvaret för att identifiera behovet av, samt genomföra, konsekvensbedömning åligger objektledare/objektstyrgrupp är det ur ett dataskyddsperspektiv helt avgörande att objektledaren har kännedom om samtliga personuppgiftsbehandlingar som, helt eller till viss del, planeras att ske i systemet/objektet i fråga.

3. Nuvarande mall för konsekvensbedömning saknar utrymme att dokumentera vem eller vilken funktion som ansvarar för att de identifierade riskminimerande tekniska och organisatoriska säkerhetsåtgärderna faktiskt vidtas. Det rekommenderas att mallen uppdateras i detta avseende.

4. Enligt IMY:s rättsliga tolkningsstöd bör den eventuella kvarstående risken tydligt beskrivas och motiveras och det bör anges vilken funktion inom organisationen som är ansvarig för den kvarstående risken. Det rekommenderas att stadsledningskontorets mall för konsekvensbedömning uppdateras även i detta avseende.

5. Dataskyddsombudet har under året fått in synpunkter som indikerar att flera verksamheter bedömer att IMY:s mall för konsekvensbedömning är tydligare och mer lätthantering än stadens motsvarighet. Kommunstyrelsen bör överväga att se över stadens mall för konsekvensbedömning och möjligen göra den mer förenlig med tillsynsmyndighetens mall.

6. Dataskyddsombudet påminner om att det i tveksamma fall alltid bör göras en konsekvensbedömning. Beslut om att inte genomföra konsekvensbedömning ska motiveras och dokumenteras.

2.4 De registrerades rättigheter

2.4.1 Allmänt om de registrerades rättigheter

De registrerade, det vill säga de vars personuppgifter behandlas, till exempel stadens medborgare och anställda, har enligt dataskyddsförordningen ett flertal rättigheter som på olika sätt ska garantera att den registrerade ges insyn och visst inflytande i hur dennes personuppgifter behandlas. En registrerad har till exempel rätt till tydlig information om hur dennes personuppgifter behandlas, rätt till tillgång till sina personuppgifter (registerutdrag), rätt till rättelse av felaktiga personuppgifter och i vissa fall rätt till begränsning och radering av personuppgifter.

Den personuppgiftsansvarige måste beakta vissa tidsfrister och till exempel besvara en registrerads begäran om tillgång utan onödigt dröjsmål, som huvudregel inom en månad. Om verksamheten brister i att hantera en begäran från en registrerad i enlighet med dataskyddsförordningens krav kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter och även leda till tillsyn med sanktioner som följd.

I enlighet med principen om öppenhet (artikel 5.1 a GDPR) ska personuppgifter behandlas på ett öppet sätt i förhållande till den registrerade. Den registrerade har rätt till klar och tydlig information om kommunstyrelsens behandling av deras personuppgifter samt hur den ska gå till väga för att tillvarata sina rättigheter enligt dataskyddsförordningen.

2.4.2 Årlig uppföljning gällande de registrerades rättigheter

Uppföljning	Svar/bedömning
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?	Stadsledningskontoret har en process (rutin och mall) avseende rätten till tillgång (registerutdrag). Motsvarande rutiner bör tas fram även för övriga rättigheter. Stadsledningskontorets nuvarande process för hantering av rätten till tillgång (registerutdrag) bör ses över i bemärkelsen att det behöver bli tydligt att kommunstyrelsens registerutdrag endast ska redogöra för de personuppgiftsbehandlingar som kommunstyrelsen är personuppgiftsansvarig för och hur verksamheterna ska gå till väga för att på mest ändamålsenliga sätt identifiera dessa.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?	Rätt till tillgång (registerutdrag): 25 st.* Rätt till rättelse: 1 st. Rätt till radering: 1 st. Rätt till begränsning: Rätt till dataportabilitet: Rätt att göra invändningar:
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?	4 st. Beträffande 21 ärenden om rätten till tillgång har de registrerade meddelats att kommunstyrelsen behöver förlänga handläggningstiden med en månad, med hänvisning till stort antal inkomna begäranden.

* Det stora antalet inkomna begäranden om rätten till tillgång (registerutdrag) är en följd av en personuppgiftsincident som inträffade i augusti 2025 då stadens systemleverantör Miljödata utsattes för ett cyberangrepp.

2.4.3 Uppföljning av föregående års rekommendationer kring de registrerades rättigheter

I årsrapporten för 2024 rekommenderas att kommunstyrelsen skyndsamt färdigställer och tillgängliggör information om behandlingen av anställdas och förtroendevaldas personuppgifter. Det rekommenderades vidare att informationen ska vara förenlig med artikel

12–14 GDPR och att den tillhandahålls de registrerade i anslutning till nyanställning samt hålls tillgänglig under anställningens gång.

Under 2025 har juridiska avdelningen tagit fram ett utkast till informationstext, vilken till sitt innehåll, särskilt avsnittet om ändamål med personuppgiftsbehandling, har färdigställts i samråd med utvecklings- och hr-avdelningen, avdelningen för it och digitalisering och kommunikations- och omvärldsavdelningen. Utvecklings- och hr-avdelningen har därefter låtit publicera texten på stadens intranät. Att det har tagits fram och tillgängliggjorts en övergripande informationstext om behandlingen av medarbetares personuppgifter är mycket positivt. Det är angeläget att kommunstyrelsens medarbetare lätt kan hitta information om bland annat deras rättigheter och vart man kan vända sig vid synpunkter eller klagomål beträffande behandlingen av deras personuppgifter.

Vidare föreslogs i årsrapporten för 2024 att kommunstyrelsen generellt bör prioritera att löpande följa upp att god och tydlig information om personuppgiftsbehandling lämnas till de registrerade i adekvat omfattning. Det finns alltjämt ett övergripande behov av uppföljning på detta område.

2.4.4 Dataskyddsombudets rekommendationer gällande de registrerades rättigheter

1. Dataskyddsombudet rekommenderar även inför 2026 att kommunstyrelsen prioriterar att löpande följa upp att det lämnas god och tydlig information till de registrerade vars personuppgifter kommunstyrelsen behandlar. Det bör tydliggöras vilken funktion vid avdelningarna som ansvarar för att tillse att informationskravet uppfylls.

2. Det är angeläget att den text om behandling av anställdas personuppgifter som har tagits fram under 2025 ses över under ledning av den funktion som har ett övergripande operativt ansvar för kommunstyrelsens informationsskyldighet. Nuvarande informationstext är tämligen generellt utformad och riktar sig till anställda och förtroendevalda i stadens alla nämnder och bolag, det vill säga till registrerade vars personuppgifter behandlas av flera olika personuppgiftsansvariga. Den ansvarige bör ta ställning till både utformning och innehåll, särskilt vad gäller redogörelsen av de olika ändamål för vilka personuppgifter behandlas. Det bör noteras att informationsskyldigheten berör all personuppgiftsbehandling, varför det är angeläget att säkerställa att den information som lämnas är så heltäckande som möjligt.

3. Dataskyddsombudet vill betona att utformning och tillgängliggörande av information till de registrerade kan se olika ut och ske i olika format, beroende på behandling. Kommunstyrelsen behöver säkerställa att informationen utformas och tillgängliggörs med beaktande av vilken personuppgiftsbehandling det rör sig om och gruppen av registrerade som informationen riktar sig till. Ju högre risk en personuppgiftsbehandling medför gällande den registrerades fri- och rättigheter, desto högre krav ställs det på informationen. Här bör även beaktas vad den registrerade rimligen kan förvänta sig vad gäller behandlingen av dennes personuppgifter.

2.5 Personuppgiftsincidenter

2.5.1 Allmänt om personuppgiftsincidenter

En personuppgiftsincident är 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 (artikel 4.12 GDPR).

Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till IMY.

Om en personuppgiftsincident sannolikt leder till en hög risk för en registrerad ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

Alla personuppgiftsincidenter, samt bedömning och hantering av dem, ska dokumenteras. Dokumentationsskyldigheten gäller både för personuppgiftsincidenter som anmäls till IMY och personuppgiftsincidenter där det bedöms osannolikt att incidenten medfört en risk för de registrerade (dvs. sådana som inte behöver anmälas till IMY). Det är angeläget att det finns en systematik för uppföljning av personuppgiftsincidenter och att adekvata åtgärder vidtas för att minska riskerna för att liknande incidenter ska ske i framtiden. En ändamålsenlig och säker hantering och uppföljning av personuppgiftsincidenter är en mycket viktig del i en verksamhets systematiska dataskyddsarbete.

Kommunstyrelsen agerar som tidigare nämnts både i rollen som personuppgiftsansvarig och personuppgiftsbiträde och i samband med hantering av personuppgiftsincidenter är det nödvändigt att i ett tidigt skede identifiera vilka av stadens andra nämnder/bolag som påverkas av en identifierad incident. Annan personuppgiftsansvarig nämnd eller bolag som berörs av incidenten måste skyndsamt informeras, oavsett om kommunstyrelsen utgör personuppgiftsansvarig eller personuppgiftsbiträde.

2.5.2 Årlig uppföljning gällande personuppgiftsincidenter 2025

Uppföljning	Svar/bedömning
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?	I dagsläget gäller stadsledningskontorets rutin för hantering av informationssäkerhetsincidenter, enligt vilken incidenter (här avses även personuppgiftsincidenter ”av systemmässig karaktär”) ska kommuniceras till *den avdelningschef eller enhetschef som vid tidpunkten bedöms ha verksamhetsansvar för det objekt eller funktion som incidenten i fråga hör till*. Ur ett dataskyddsperspektiv är det svårt att utifrån dessa skrivningar veta hur och till vem (vilken chef) en anställd ska rapportera upptäckta personuppgiftsincidenter till.

Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?	Stadsledningskontorets nuvarande rutin för hantering av informationssäkerhetsincidenter behöver kompletteras i flera avseenden om den ska fungera adekvat för bedömning och hantering av personuppgiftsincidenter.
Hur många personuppgiftsincidenter har dokumenterats under året?	7
Hur många personuppgiftsincidenter har anmälts till IMY under året?	3

2.5.3 Uppföljning av föregående års rekommendationer gällande personuppgiftsincidenter

I föregående års rekommendationer påminner dataskyddsombudet om vikten av att det är tydligt för samtliga medarbetare vid kommunstyrelsen hur man ska agera när det inträffar en personuppgiftsincident. Dataskyddsombudet rekommenderade också en översyn av styrdokument och processer för hantering av personuppgiftsincidenter. Under våren 2025 initierade kommunstyrelsens dataskyddsombud och stadsledningskontorets informationssäkerhetssamordnare en översyn av stadsledningskontorets rutin för hantering av informationssäkerhetsincidenter. En ny rutin för hantering av personuppgiftsincidenter togs fram och har förankrats med representanter från utvecklings- och hr-avdelningen, juridiska avdelningen, avdelningen för it och digitalisering och säkerhetsavdelningen. Rutinen har tillämpats i praktiken vid hantering av personuppgiftsincidenter, men har ännu inte formellt antagits, eftersom det kommer att ingå i översyn av styrdokumenten.

Dataskyddsombudet föreslog vidare att rutinerna för hur kommunstyrelsen ska agera vid personuppgiftsincidenter som berör andra personuppgiftsansvariga inom staden bör förtydligas, särskilt vad gäller informationsöverföring. Denna rekommendation kvarstår. Det är mycket angeläget att det finns etablerade och effektiva kommunikationsvägar mellan nämnderna, särskilt när det inträffar en personuppgiftsincident.

Dataskyddsombudet rekommenderade slutligen att avdelningarnas rutiner för dokumentation av personuppgiftsincidenter följs upp. Även denna rekommendation kvarstår.

2.5.4 Dataskyddsombudets rekommendationer gällande personuppgiftsincidenter

1. Vid en inträffad personuppgiftsincident är det angeläget att det är tydligt för samtliga medarbetare hur man ska agera och då framför allt *hur* incidenten ska rapporteras internt. Oklarheter härom utgör en mycket stor risk. Det är angeläget att det görs

tydligt för samtliga medarbetare vad en personuppgiftsincident är (gärna med illustrerande exempel) och hur man ska agera när en personuppgiftsincident har inträffat. En tydlig och lätt tillgänglig intern rapporteringsväg för rapportering av personuppgiftsincidenter bör skyndsamt tas fram och kommuniceras ut i samtliga verksamheter.

2. Dataskyddsombudet vill understryka att personuppgiftsincidenter inte behöver ha direkt koppling till ett verksamhetssystem, applikation eller it-infrastruktur. Att nuvarande rutin för hantering av informationssäkerhetsincidenter endast adresserar denna sorts incidenter behöver ses över, förslagsvis genom att kommunstyrelsen fastställer det framtagna förslaget till rutin (se avsnitt 2.5.3 ovan), som beskriver hanteringen av alla slags *personuppgiftsincidenter*. I den föreslagna rutinen redogörs för en hanteringsordning och bedömningsgrunder som är förenliga med dataskyddsförordningen, det vill säga utgår från riskerna för de registrerades fri- och rättigheter.

3. Rutinerna för hur kommunstyrelsen ska agera vid personuppgiftsincidenter som berör flera personuppgiftsansvariga inom staden bör ses över och vid behov förtydligas, särskilt vad gäller informationsöverföring mellan kommunstyrelsen och övriga nämnder och bolag.

4. Kommunstyrelsen bör utreda om det finns förutsättningar för ökad samverkan mellan nämnderna beträffande hantering av personuppgiftsincidenter som berör flera nämnder. Det bör vara positivt för både kvalitet och kostnadseffektivitet att skapa en struktur där personuppgiftsincidenter hanteras i närmare samverkan mellan nämnderna än vad som sker idag.

5. Dataskyddsombudet rekommenderar att avdelningarnas rutiner för dokumentation av personuppgiftsincidenter följs upp. Det är angeläget att det finns goda rutiner för dokumentation av samtliga incidenter, även sådana som inte anmäls till IMY. Dataskyddsombudet har tagit fram en mall för dokumentation av personuppgiftsincidenter som med fördel kan användas.

2.5.5 Personuppgiftsincident med anledning av it-angrepp hos Miljödata

Den 23 augusti inträffade ett omfattande it-angrepp hos stadens leverantör Miljödata. Obehöriga beredde sig tillgång till stora mängder personuppgifter, gällande över 1,5 miljoner privatpersoner i Sverige, och lät sedan publicera dessa på Darknet.

Staden har haft för avsikt att införa Miljödatas systemstöd för rapportering och uppföljning av arbetsmiljöincidenter (Stella). Staden hade vid tiden för incidenten ännu inte driftsatt systemet, varför inga uppgifter om arbetsmiljöincidenter har behandlats hos Miljödata. Inför kommande driftsättning har staden från april 2025 haft en produktionsmiljö hos Miljödata i syfte att bland annat verifiera att organisatoriska strukturer och roller är korrekt konfigurerade systemet och för att kunna identifiera problem eller brister i flödet för incidentrapportering, så att systemet ska fungera på ett korrekt och säkert sätt vid driftsättning.

I direkt anslutning till att kommunstyrelsen informerades om it-angreppet hos Miljödata (25 augusti) inleddes en utredning i vilken det inträffade hanterades i enlighet med stadsledningskontorets nya rutin för hantering av personuppgiftsincidenter. Kommunstyrelsen anmälde personuppgiftsincidenten till IMY den 27 augusti.

Den 14 september fick kommunstyrelsen information om att den externa hotaktören ska ha publicerat röjda personuppgifter gällande stadens medarbetare, samt tidigare medarbetare, på Darknet samt uppgifter som medförde att staden inte längre kunde utesluta att även skyddade personuppgifter hade röjts. Samma söndag hölls flera avstämningsmöten med anledning av det inträffade, där bland annat stadsdirektör, tjänsteman i beredskap, hr-direktör, kommunikationsdirektör, kommunikatör i beredskap, säkerhetsdirektör, stadsjurist, incidentledare, informationssäkerhetssamordnare och dataskyddsombud deltog. Dataskyddsombudet har genomgående involverats i kommunstyrelsens hantering av personuppgiftsincidenten.

Dataskyddsombudets uppfattning är att kommunstyrelsen, utifrån den information som har funnits beträffande omständigheterna, har hanterat incidenten skyndsamt, adekvat och gett ärendet högsta prioritet. Primärt fokus var att säkerställa en omgående kontakt med berörda medarbetare och tidigare medarbetare med skyddade personuppgifter, i syfte att informera om det inträffade, bedöma risker och vidta riskminimerande åtgärder. Det har lagts stor omsorg kring utformning och skyndsamt tillhandahållande av information till de registrerade. Initialt lämnades information via intranätet samt stadens externa hemsida, då dessa kommunikationsvägar kunde nyttjas omgående, men så fort det fanns förutsättningar till utskick via elektronisk brevlåda samt brev så lämnades informationen även direkt till de registrerade.

Dataskyddsombudet bedömer sammanfattningsvis att kommunstyrelsens hantering av personuppgiftsincidenten med anledning av it-angreppet hos Miljödata har varit tillfredsställande.

2.6 Överföring till tredjeland

2.6.1 Allmänt om överföring till tredjeland

Behandling av personuppgifter, till exempel anlitande av personuppgiftsbiträden eller lagring av personuppgifter i en molntjänst, i länder utanför EU/EES kan medföra så kallad tredjelandsöverföring. Genom dataskyddsförordningen säkerställs skyddet av personuppgifter som behandlas inom förordningens tillämpningsområde. Utanför EU/EES saknas ofta motsvarande lagstiftning, vilket medför att säkerheten inte kan garanteras. Dataskyddsförordningen innehåller därför regler om under vilka förutsättningar det är tillåtet att föra över personuppgifter till länder utanför EU/EES.

För kommunstyrelsens del möjliggörs tredjelandsöverföringar huvudsakligen på två olika sätt:

1. Beslut från EU-kommissionen om att ett visst land utanför EU/EES säkerställer så kallad *adekvat skyddsnivå*.

2. Upprättande av standardavtalsklausuler i enlighet med artikel 46 GDPR (förutsätter i regel att det upprättas en så kallad transfer impact assessment, TIA, något förenklat

översatt till *tredjelandsöverföringsbedömning*) och att eventuella kompletterande skyddsåtgärder identifieras och vidtas.

Den 10 juli 2023 fattade EU-kommissionen ett beslut om adekvat skyddsnivå för USA, förutsatt att mottagaren omfattas av EU–US Data Privacy Framework (EU-US DPF). Beslutet innebär att överföring till USA är tillåten, förutsatt att mottagaren omfattas av EU-US DPF. Beträffande mottagare som ej omfattas behöver standardavtalsklausuler upprättas och eventuella kompletterande skyddsåtgärder identifieras och vidtas.

EU-kommissionen kan när som helst besluta om att upphäva beslut om adekvat skyddsnivå. Därför är det mycket angeläget att säkerställa att det, i vart fall för verksamhetskritiska personuppgiftsbehandlingar, finns alternativa lösningar som möjliggör tredjelandsöverföring med stöd av annan grund, alternativt att det finns alternativa lösningar som inte medför tredjelandsöverföring till land där adekvansbeslut saknas.

Vid stadsledningskontoret finns det ett gällande inriktningsbeslut avseende tredjelandsöverföringar till USA som ska beaktas vid bedömningen av personuppgiftsbehandlingar som medför sådan tredjelandsöverföring.

2.6.2 Dataskyddsombudets rekommendationer gällande överföring till tredjeland

1. Dataskyddsombudet rekommenderar att kommunstyrelsen kartlägger och dokumenterar samtliga pågående tredjelandsöverföringar, antingen i en egen förteckning eller inom ramen för kommunstyrelsens register över personuppgiftsbehandlingar.

2. För det fall att det i en kartläggning enligt ovan identifieras tredjelandsöverföringar för vilket det saknas ett tillämpligt beslut om adekvat skyddsnivå eller upprättade standardavtalsklausuler behöver åtgärder vidtas för att säkerställa att tredjelandsöverföringen är förenlig med gällande dataskyddslagstiftning.

3. Stadsledningskontorets inriktningsbeslut gällande tredjelandsöverföringar till USA (KS 2023/241) reviderades senast 2023-09-14. Av inriktningsbeslutet framgår att om nu gällande adekvansbeslut (EU-US Data Privacy Framework) inte ändras inom den kommande treårsperioden bör ett nytt inriktningsbeslut tas fram utifrån då rådande förutsättningar. Här bör således uppmärksammas att ett nytt inriktningsbeslut behöver tas fram under 2026. Dataskyddsombudet rekommenderar att ett nytt inriktningsbeslut utformas med omsorg.

3 Övriga rapporteringsområden

3.1 Allmänt om de övriga rapporteringsområdena

Utöver de sex årliga rapporteringsområdena som samtliga dataskyddsombud inom staden uppmanas att lyfta i årsrapporten önskar kommunstyrelsens dataskyddsombud redogöra kort för ytterligare fyra områden:

- Personuppgiftsansvar inom Stockholms stad
- Styrdokument och annan vägledning
- Arkivering och gallring
- Samverkan inom stadsledningskontoret samt inom staden

3.1.1 Personuppgiftsansvar inom Stockholms stad

Personuppgiftsansvarig är den som bestämmer *för vilket ändamål* personuppgifter ska behandlas och *hur* behandlingen ska gå till. Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Bedömningen kring hur personuppgiftsansvaret förhåller sig mellan stadens nämnder och bolag behöver utgå från de faktiska omständigheter som föreligger för respektive personuppgiftsbehandling. Personuppgiftsansvaret kan också variera mellan olika skeden av personuppgiftsbehandlingen. Personuppgiftsansvaret kan vara självständigt eller gemensamt.

Om två eller flera nämnder och/eller bolag gemensamt bestämmer över en viss behandling är de gemensamt personuppgiftsansvariga och måste sinsemellan bestämma vem som är ansvarig för att fullgöra de olika skyldigheterna i dataskyddsförordningen. Staden har en mall för överenskommelse om gemensamt personuppgiftsansvar.

För det fall att en nämnd eller ett bolag behandlar personuppgifter för en annan nämnds eller bolags räkning behöver det upprättas ett inbördes arrangemang som reglerar parternas respektive ansvar enligt dataskyddsförordningen, särskilt vad gäller de registrerades rättigheter. Staden har för detta ändamål en mall för så kallade stadeninterna instruktioner.

Det finns ett övergripande behov av att utreda och dokumentera hur personuppgiftsansvaret förhåller sig mellan nämnder och bolag, kanske framför allt beträffande de centrala stadsövergripande system i vilka flera eller samtliga nämnder behandlar personuppgifter för ibland samma och ibland olika ändamål.

Bedömningen av personuppgiftsansvar påverkar i sin tur annan hantering som rör behandlingen av personuppgifter, bland annat

- ansvaret för att säkerställa att personuppgiftsbehandling sker i enlighet med dataskyddsregelverket

- dokumentation i register över personuppgiftsbehandlingar

- hantering av de registrerades rättigheter (till exempel omfattning/avgränsning av de registrerades rätt till tillgång och skyldigheten att informera de registrerade)

- utformning av personuppgiftsbiträdesavtal (partsförhållanden)

- ansvar för att utreda och anmäla personuppgiftsincidenter

- ansvar för att i förekommande fall upprätta konsekvensbedömning

Det är således mycket angeläget att det inte föreligger oklarheter kring hur personuppgiftsansvaret förhåller sig mellan stadens nämnder och bolag.

Juridiska avdelningen har tagit fram en promemoria som övergripande beskriver förutsättningarna och bedömningsgrunder för gemensamt personuppgiftsansvar. Avdelningens dataskyddsjurist har vidare presenterat slutsatserna kring frågan om personuppgiftsansvar för stadsledningskontorets avdelningschefer och initierat en dialog kring behovet av att se över nuläget och det eventuella behovet av att upprätta överenskommelser om gemensamt personuppgiftsansvar, som tydliggör ansvaret mellan stadens nämnder och bolag.

Dataskyddsombudets rekommendationer: Dataskyddsombudet bedömer juridiska avdelningens arbete med kring personuppgiftsansvar som mycket angeläget och väl prioriterat. Dataskyddsombudet rekommenderar att kommunstyrelsen skyndsamt tar fram ett kompletterande metodstöd för bedömning och dokumentation av personuppgiftsansvar. Dataskyddsombudet rekommenderar vidare att samtliga avdelningar ges i uppdrag att kartlägga de *personuppgiftsbehandlingar* (det vill säga inte it-system eller objekt) som kommunstyrelsen är personuppgiftsansvarig för och säkerställa att de är korrekt inlagda i kommunstyrelsens register över personuppgiftsbehandlingar. Dataskyddsombudet vill även betona vikten av samverkan mellan stadens nämnder och bolag vid verksamheternas utredning och bedömning av personuppgiftsansvar som berör flera nämnder och/eller bolag inom staden.

3.1.2 Styrdokument och annan vägledning

Regelverket för dataskydd berör varje anställd i staden som behandlar personuppgifter inom ramen för sitt arbete. Varje medarbetare behöver ha grundläggande kunskaper om förutsättningarna för en lagenlig behandling av personuppgifter. Det behöver vara lätt att göra rätt. Detta möjliggörs endast genom tydlig och lättillgänglig vägledning som baseras på dataskyddsregelverket och som utformas med avsikten att den ska kunna tillämpas av varje anställd, oavsett förkunskaper. Kommunstyrelsen bör göra noggranna överväganden när det kommer till utformning och tillgängliggörande av stöddokumentation som rör dataskydd.

En utmaning med nuvarande synsätt, arbetssätt och stöddokumentation inom staden är att dataskydd betraktas som en del av informationssäkerhetsbegreppet. Som exempel kan nämnas att läsaren av stadsledningskontorets lokala anvisning för informationssäkerhet uppmanas att notera att *begreppet informationssäkerhet inkluderar dataskydd i detta dokument.*

Härvid vill dataskyddsombudet betona att informationssäkerhet inte bör likställas med dataskydd. Informationssäkerhet syftar till att skydda *information* och informationssäkerhetsarbetet ska, något förenklat uttryckt, säkerställa att Stockholms stad ska ha tillgång till den information som behövs för att staden ska kunna utföra sina uppdrag. Dataskydd syftar till att skydda *personuppgifter* och därigenom säkerställa skyddet för den enskilde individen vars personuppgifter behandlas.

Frågor som har bäring på dataskyddsförordningens krav att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna (artikel 32 GDPR) behöver ske i nära samverkan mellan olika kompetenser, bland annat informationssäkerhet och dataskydd. Ett par konkreta exempel på områden där nära samverkan är nödvändig är vid utformning av kravställning på leverantörer, hantering av personuppgiftsincidenter och riskanalyser som görs inom ramen för konsekvensbedömning.

Vidare bör det dock beaktas att dataskyddsförordningen är teknikneutral och reglerar förutsättningar för personuppgiftsbehandling i ett bredare perspektiv än tekniska och organisatoriska säkerhetsåtgärder som har direkt koppling till it-system eller -objekt. I ett it-system kan det ske ett stort antal olika personuppgiftsbehandlingar, för olika ändamål och med olika rättslig grund. Personuppgiftsbehandling i it-system sker dessutom i flera olika skeden, exempelvis inför implementering, vid normal drift, vid testning och utveckling av systemet och vid avveckling av systemet. Arbetssätt, processer och ansvar som utgår från system- eller objektsperspektiv, såsom vanligtvis är fallet inom ramen för informationssäkerhetsområdet, har således ofta en något begränsad dataskyddsrättslig relevans, eftersom ett sådant fokus sannolikt medför att inte *samtliga personuppgiftsbehandlingar* adresseras. Dessutom utgörs dataskyddsförordningen av ett regelverk som till stora delar tar sikte på avvägningar och bedömningar som inte omfattas av informationssäkerhetsregelverket, men som ur ett dataskyddsperspektiv är mycket centrala. Här bör framför allt nämnas de grundläggande principerna om ändamålsbegränsning, laglighet (rättslig grund), uppgiftsminimering och lagringsminimering. Dessa krav behöver adresseras och dokumenteras *för varje personuppgiftsbehandling*.

Dataskyddsombudets rekommendationer: Kommunstyrelsen bör se över nuvarande vägledning beträffande dataskydd och överväga om det finns förutsättningar att öka tillgängligheten till grundläggande vägledning kring *dataskydd* och tillgängliggöra informationen på ett sätt som är lätt för varje medarbetare att hitta, förstå och tillämpa. Lämpligen ser man över både befintlig stöddokumentation och den information som lämnas via intranätet.

Även om det inom flera områden finns en nära koppling mellan informationssäkerhet och dataskydd bör kommunstyrelsen överväga att tillhandahålla vissa riktlinjer och rutiner för dataskydd i separat stöddokumentation, i syfte att öka tillgängligheten till sådan dataskyddsrelaterad information som varje medarbetare behöver känna till. Det bedöms till exempel vara en fördel att ha en separat rutin för hantering av *personuppgiftsincidenter*, eftersom bedömningsgrunder och hantering av dessa incidenter inte kan likställas med bedömningsgrunder och hantering av andra slags säkerhetsincidenter.

Kommunstyrelsen bör även undersöka om nuvarande processer, bland annat nämndens informationsklassningsprocess, adresserar samtliga *personuppgiftsbehandlingar* i adekvat omfattning.

Exempel på sakområden inom dataskydd som dataskyddsombudet särskilt bedömer bör synliggöras bättre för samtliga medarbetare:

- De grundläggande förutsättningarna för en lagenlig behandling av personuppgifter som behöver beaktas vid all personuppgiftsbehandling, av samtliga medarbetare som behandlar personuppgifter (huvudsakligen de grundläggande principerna i artikel 5 GDPR)

- Metodstöd för hantering av register över personuppgiftsbehandlingar

- Tydlig information om identifiering och intern rapportering av personuppgiftsincidenter

3.1.3 Arkivering och gallring

Ur ett dataskyddsperspektiv är det mycket angeläget att beakta samtliga grundläggande principer för personuppgiftsbehandling (artikel 5 GDPR). En av dem utgörs av principen om *lagringsminimering*, som innebär att personuppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifter behandlas.

Det är av stor vikt att kommunstyrelsen inte behandlar, till exempel lagrar, personuppgifter under en längre tid än nödvändigt. Det behöver finnas goda interna rutiner för gallring av de personuppgifter som inte längre är nödvändiga för ändamålet och där det inte finns ett särskilt beslut om att uppgifterna ska bevaras.

Kommunstyrelsen behandlar stora mängder personuppgifter hos personuppgiftsbiträden och i enlighet med både dataskyddsförordningen (kraven på tillräcklig säkerhet i artikel 32 GDPR) och informationssäkerhetsregelverket ställs det dessutom krav på upprättande av säkerhetskopior och bevarande av loggar och liknande systemdokumentation, vilka ofta innehåller personuppgifter. Dataskyddsombudet vill betona vikten av att kommunstyrelsen, i egenskap av personuppgiftsansvarig, löpande säkerställer att personuppgiftsbiträden endast behandlar de personuppgifter som är nödvändiga för den behandling som de enligt personuppgiftsbiträdesavtalet ska utföra för stadens räkning *och* att personuppgiftsbiträden inte behandlar personuppgifter under längre tid än vad som är nödvändigt.

Dataskyddsombudets rekommendation: Kommunstyrelsen behöver förse samtliga personuppgiftsbiträden med tydliga instruktioner gällande dess skyldigheter att gallra/radera eller avidentifiera personuppgifter i erforderlig omfattning. Kommunstyrelsen bör även ha interna rutiner som säkerställer en regelbunden uppföljning av att kommunstyrelsens instruktioner gällande gallring hos personuppgiftsbiträdet efterlevs på ett adekvat sätt.

3.1.4 Samverkan kring dataskydd inom stadsledningskontoret samt inom staden

Dataskyddsombudet vill generellt rekommendera en ökad samverkan kring dataskyddsfrågor mellan avdelningarna vid stadsledningskontoret och mellan kommunstyrelsen och övriga nämnder och bolag inom staden. En ökad samverkan är framför allt nödvändig vid utredning och bedömning av personuppgiftsansvar. Utformning av överenskommelser om gemensamt personuppgiftsansvar samt stadeninterna instruktioner bör hanteras i en nära dialog mellan olika verksamheter, med stöd av nämndernas och bolagens dataskyddsombud.

4 Genomförda och planerade aktiviteter

4.1 Genomförda aktiviteter under 2025

Under 2025 har dataskyddsombudet prioriterat att ge råd och stöd i kommunstyrelsens pågående och löpande dataskyddsarbete. Dataskyddsombudet har medverkat vid genomförandet av flera konsekvensbedömningar, deltagit vid informationsklassningar, bistått med råd och stöd inom ramen för större projekt, granskat flera personuppgiftsbiträdesavtal

samt medverkat i flera informationsinsatser inom området för dataskydd. Dataskyddsombudet har stöttat verksamheterna i hanteringen av personuppgiftsincidenter, medverkat i arbetet med att ta fram informationstexter om personuppgiftsbehandling samt bistått i arbetet med att ta fram en ny rutin för stadsledningskontorets hantering av personuppgiftsincidenter.

I 2024 års rapport redogjorde dataskyddsombudet för införandet av nya dokumentationsmallar för intern uppföljning av dataskydd. Dataskyddsombudet genomför löpande uppföljningar, både i form av stickprovskontroller och särskilda granskningar på förekommen anledning (till exempel vid misstanke om brister eller som uppföljning på klagomål). Syftet med de interna uppföljningarna är uteslutande att identifiera förbättringsområden och därmed kunna ge ett gott och ändamålsenligt stöd till avdelningarna. För att uppnå en förutsägbarhet och enhetlighet i dokumentationen av uppföljningarna skulle underlag i form av två olika dokumentationsmallar tas fram under första kvartalet 2025. Ändamålet med den nya dokumentationsmallen är att på ett enkelt och effektivt sätt tydliggöra identifierade behov och risker beträffande en viss personuppgiftsbehandling och förmedla dessa till ansvarig funktion.

En mall för intern uppföljning enligt ovan har tagits fram under 2025 och dataskyddsombudet kommer från och med första kvartalet 2026 att dokumentera interna uppföljningar i form av både stickprovskontroller och uppföljning på förekommen anledning. Uppföljningarna tar främst sikte på att identifiera brister i efterlevnad av de grundläggande principerna i dataskyddsförordningens artikel 5 GDPR.

I föregående års rapport redogjordes även för det planerade införandet av ett årshjul som tydligt illustrerar det övergripande planerade arbetssättet med interna uppföljningar vid kommunstyrelsen. Ett sådant årshjul kommer att tas fram i samverkan med stadsledningskontorets berörda funktioner.

4.2 Planerade aktiviteter under 2026

Dataskyddsombudet har för avsikt att under 2026 fortsätta arbeta för att på ett ändamålsenligt och strukturerat sätt bistå till en god intern kompetensutveckling gällande dataskydd för kommunstyrelsens medarbetare. Innehåll och format behöver avgöras utifrån avdelningarnas specifika behov, identifierade riskområden och förutsättningar utifrån rättsläget. Dataskyddsombudet deltar gärna i fler kompetensutvecklande insatser än vad kommunstyrelsens avdelningar har efterfrågat hittills och välkomnar samtliga chefer och medarbetare att ta kontakt när behov identifieras.

Dataskyddsombudet kommer fortsätta att stötta samtliga avdelningar i både löpande dataskyddsarbete och genom medverkan i större projekt, bland annat konsekvensbedömningar för GSIT3 och i påbörjade initiativ som rör personuppgiftsansvar och dataskydd. Dataskyddsombudet kommer även att stötta i de aktiviteter gällande dataskydd som ingår i juridiska avdelningens och säkerhetsavdelningens planering inför 2026, bland annat uppdatering av befintliga vägledande dokument inom dataskydd (bland annat stadens mall för personuppgiftsbiträdesavtal samt processen för konsekvensbedömning) samt framtagande av metodstöd/vägledning för bedömning av personuppgiftsansvar.