Stockholms stad

Bilaga 7

Dataskyddsombudets årsrapport

2024

Kommunstyrelsen

Dataskyddsombudets årsrapport
December 2024

Dnr: KS 2024/1074
Kontaktperson: Diana Färje, dataskyddsombud

1 Inledning

Stockholms stad behandlar dagligen stora mängder personuppgifter om bland annat kommunmedlemmar och anställda. 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 och integritet är omfattande och föränderligt. Ny lagstiftning och praxis på området föranleder ett ständigt pågående arbete inom staden för att se över och utveckla arbetssätt, ta fram vägledningar och andra stöddokument i syfte att uppnå en god systematik och tydliga processer som underlättar för verksamheterna. Ny teknik, t.ex. användning av AI, skapar nya möjligheter för utveckling och förbättring, men även utmaningar som behöver adresseras på ett ändamålsenligt sätt, bl.a. vad gäller dataskydd.

Varje nämnd och bolagsstyrelse inom Stockholms stad är ansvarig för den behandling av personuppgifter som sker i verksamheten (*personuppgiftsansvarig*) och således ytterst ansvarig för att verksamheten följer gällande dataskyddslagstiftning, bl.a. dataskyddsförordningen[1]. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen.

Varje nämnd och bolagsstyrelse i Stockholms stad har ett utnämnt dataskyddsombud. Dataskyddsombudet har till uppgift att övervaka verksamhetens efterlevnad av dataskyddsförordningen samt informera och ge råd till den personuppgiftsansvarige. Dataskyddsombudet ska rapportera direkt till högsta förvaltningsnivå.

En årlig rapportering från dataskyddsombudet är ett tillvägagångssätt genom vilket kommunstyrelsen ges insyn i verksamhetens arbete med dataskydd och därtill relaterade frågor samt får råd och rekommendationer från dataskyddsombudet. Årsrapporten syftar således till att skapa medvetenhet, vilket

[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)

underlättar vid fullgörande av det ansvar som åligger kommunstyrelsen som personuppgiftsansvarig.

Årsrapporten ger kommunstyrelsen förutsättningar att fatta adekvata beslut om prioriteringar, resurser och initiativ inom området för integritet och dataskydd.

I denna årsrapport beskrivs lite bakgrund kring respektive rapporteringsområde, 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 2024. Därtill ger dataskyddsombudet rekommendationer kring hur kommunstyrelsen bör arbeta med respektive område under 2025.

Under året har kommunstyrelsen rekryterat ett nytt dataskyddsombud och en ny informationssäkerhetssamordnare.

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

Innehåll

2 Sammanfattning

Under 2024 har dataskyddsarbetet inom kommunstyrelsen till stora delar fortgått väl och det har fallit naturligt att fortsätta med det arbete som gjorts och de arbetssätt som tillämpats under föregående år.

I Dataskyddsombudets årsrapport 2024 läggs huvudsakligen fokus på de sex årliga rapporteringsområdena (avsnitt 3), där stora delar av dataskyddsregelverket och således stora delar av kommunstyrelsens dataskyddsarbete inryms.

Ett av de områden där det bedöms finnas ett särskilt behov av översyn och åtgärder under kommande år är hanteringen av kommunstyrelsens register över personuppgiftsbehandling. Utöver förtydligande vägledning som underlättar vid kommande registreringar, behöver det vidtas åtgärder som tillser att registret är korrekt och heltäckande.

Det har identifierats ett behov av förtydliganden i vissa styrdokument som rör dataskydd, bland annat vad gäller kommunstyrelsens hantering av personuppgiftsincidenter. Dataskyddsombudet föreslår även att vissa mer generella stöddokument, t.ex. gällande dataskyddsförordningens grundläggande principer (som ska beaktas vid all personuppgiftsbehandling), behöver finnas tillgänglig för samtliga anställda vid kommunstyrelsen.

En av de grundläggande principerna i dataskyddsförordningen rör den personuppgiftsansvariges skyldighet att informera de registrerade om den personuppgiftsbehandling som utförs. Här finns utrymme för översyn och förbättringar, särskilt vad gäller information som riktar sig till kommunstyrelsens anställda och förtroendevalda. Även på andra områden kan informationsskyldigheten medföra vissa arbetsinsatser framöver, särskilt vad gäller införandet av ny teknik, t.ex. användning av AI.

Eftersom AI är ett aktuellt område i alla sektorer i samhället, och således även inom staden, har dataskyddsombudet valt att rapportera översiktligt kring hur regelverket kring dataskydd påverkar utveckling, upphandling och implementering av tjänster som innebär användning av AI.

3 Årliga rapporteringsområden

I denna årsrapport redogörs för sex rapporteringsområden som stadens dataskyddsombud rapporterar om samt följer upp årligen. Dessa rapporteringsområden är:

- Register över personuppgiftsbehandling
- Styrdokument
- Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- Konsekvensbedömningar
- De registrerades rättigheter
- Personuppgiftsincidenter

I egenskap av personuppgiftsansvarig bör kommunstyrelsen ha god kännedom om verksamhetens arbete med dessa områden, både avseende förevarande år och över tid.

3.1 Register över personuppgiftsbehandling (registerförteckning)

3.1.1 Allmänt om registerförteckning

I enlighet med artikel 30 dataskyddsförordningen 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 huvudsakliga syftet med registerförteckningen är att ge den personuppgiftsansvarige en god kontroll över de personuppgiftsbehandlingar som utförs under dess ansvar. Registerförteckningen skapar förutsättningar för en intern synlighet och förståelse för vilka personuppgifter som behandlas och hur de hanteras. En heltäckande och uppdaterad registerförteckning leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete.

Registerförteckningen är dataskyddsarbetets centrala utgångspunkt och säkerställer bland annat att verksamheterna kan tillse att det finns en laglig grund för all personuppgiftsbehandling 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.

3.1.2 Årlig uppföljning gällande kommunstyrelsens registerförteckning

Uppföljning	Svar/bedömning
Antal behandlingar som är registrerade?	171 st. varav: 4 st. *godkända* 119 st. *under bearbetning* 45 st. *redo för granskning* 3 st. *under granskning*
Har nödvändiga uppdateringar gjorts?	Det pågår ett arbete med att inventera och kvalitetssäkra registerförteckningen.
Bedöms registerförteckningen vara fullständig?	Se ovan.
Har verksamheten lämpliga rutiner för registerföring?	Befintlig rutin behöver förtydligas, särskilt vad gäller ansvar för registerförteckning samt registerförteckning av personuppgiftsbehandlingar som kommunstyrelsen utför i egenskap av personuppgiftsbiträde.

3.1.3 Uppföljning av föregående års rekommendationer gällande kommunstyrelsens registerförteckning

I 2023 års rapport föreslog dataskyddsombudet att stadsledningskontoret tar fram en gemensam process för att säkerställa att kommunstyrelsens registerförteckning uppdateras och inventeras enligt gällande lagkrav. Juridiska avdelningen har tagit ställning till förslaget och kommit fram till att en gemensam process inte bedöms nödvändig. Utöver att området är reglerat i lag kan det framhållas att genomförandet av registerförteckning utgör ett dokumenterat steg som ska fullgöras inom ramen för informationsklassningen.

Utöver en gemensam process för hantering av registerförteckningen föreslog dataskyddsombudet att det utses en dataskyddskontakt per avdelning som löpande stödjer sin avdelning i hanteringen av registerförteckningen. Det har under hösten 2024 initierats en dialog med avdelningarna kring en sådan lösning.

Slutligen rekommenderade dataskyddsombudet att det behöver tillses att alla avdelningars personuppgiftsbehandlingar är införda i registerförteckningen, lämpligen utifrån en jämförelse med vad som är informationsklassat (se avsnitt 3.3.1 nedan). Behandlingar som rör automatiserat beslutsfattande, internet of things (IoT), AI och skyddade personuppgifter bör prioriteras i detta arbete. Det pågår för närvarande (december 2024) dialoger med avdelningarna i frågan, i syfte att utreda behovet av åtgärder.

3.1.4 Dataskyddsombudets rekommendationer gällande kommunstyrelsens registerförteckning

- Det finns ett behov av att genomföra en översyn av kommunstyrelsens registerförteckning. Varje avdelning bör inventera sina personuppgiftsbehandlingar och tillse att de är korrekt inlagda i registerförteckningen (Draftit).

- Kommunstyrelsen behöver se till att varje personuppgiftsbehandling som kommunstyrelsen utför *i egenskap av personuppgiftsbiträde* läggs in i registerförteckningen.

- För att underlätta avdelningarnas hantering av registerförteckningen bör kommunstyrelsen ta fram en dokumenterad rutin som säkerställer att kommunstyrelsens registerförteckning uppdateras och även i övrigt hanteras enligt gällande lagkrav. Rutinen bör förtydliga
  - att varje personuppgiftsbehandling som sker inom ramen för avdelningarnas ansvar ska dokumenteras i registerförteckningen samt hur registreringen går till
  - att och hur avdelningarnas befintliga registreringar ska följas upp och uppdateras regelbundet (t.ex. en gång per år) samt löpande vid behov
  - vilken roll/funktion vid varje avdelning som är ytterst ansvarig för avdelningens registerförteckning i Draftit.

- Kommunstyrelsen bör, utifrån de pågående dialogerna med avdelningarna, se över behovet av att utse en dataskyddskontakt per avdelning som, i samverkan med informationssäkerhetssamordnare (ISAM) och dataskyddsombud, kan stötta avdelningarna i arbetet med registerförteckning.

3.2 Styrdokument

3.2.1 Allmänt om styrdokument gällande dataskydd och integritet

Genom styrdokument inom området för dataskydd och integritet kan kommunstyrelsen tillse att hela organisationen har goda förutsättningar för hantering av personuppgifter på ett sätt som är förenligt med gällande dataskyddslagstiftning. I styrdokumenten tydliggörs för förutsättningarna för personuppgiftsbehandling och vad som förväntas av medarbetarna när de hanterar personuppgifter. Styrdokument utgör grunden för ett systematiskt dataskyddsarbete.

I enlighet med artikel 5.2 dataskyddsförordningen ska den personuppgiftsansvarige ansvara för och kunna *visa* att organisationen följer de grundläggande principerna i förordningen (ansvarsskyldighet). Nedtecknade, beslutade och kommunicerade styrdokument utgör en väsentlig del av detta ansvar.

I Stockholms stad hanteras frågor som rör dataskydd inom ramen för det övergripande informationssäkerhetsarbetet. Som en följd härav utgör riktlinjer och vägledningar som rör dataskydd en del av

de mer övergripande styrdokument som rör informationssäkerhet, dvs. hantering av information i ett bredare perspektiv.

Utöver de centrala stadsövergripande styrdokumenten, riktlinje för informationssäkerhet i Stockholms stad samt tillhörande tillämpningsanvisning, finns det vid kommunstyrelsen en *lokal anvisning för informationssäkerhet* och en *lokal rutin för incidenthantering.* Båda dessa lokala dokument innehåller vägledning och rutiner som rör dataskydd och integritet. I t.ex. den lokala rutinen för incidenthantering redogörs således även för hantering av personuppgiftsincidenter.

3.2.2 Årlig uppföljning gällande styrdokument

Uppföljning	Svar/bedömning
Finns lämplig styrande dokumentation på plats?	Det finns behov av förtydliganden, bl.a. gällande hantering av personuppgiftsincidenter.
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Det finns behov av förtydliganden i vissa delar.
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Se ovan.
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.3 Uppföljning av föregående års rekommendationer gällande styrdokument

I årsrapporten för 2023 rekommenderade dataskyddsombudet en förstärkande insats gällande skriftliga rutiner och instruktioner samt att intranätet ska användas för publicering av dessa. Det pågår för närvarande (december 2024) ett arbete med att se över de tre sidor på intranätet som uteslutande rör dataskydd/GDPR. Förslagsvis kompletteras dessa sidor med kort information om samt länkar till aktuella styrdokument, som annars bara finns att hitta via sidorna om informationssäkerhet. En av flera förstärkande insatser som

initierats under året rör processen för hantering av registerutdrag, som juridiska avdelningen för närvarande (december 2024) ser över.

Dataskyddsombudet rekommenderade även att verksamheten slutför det pågående arbetet med framtagande av instruktion för hur personuppgifter får behandlas i e-post. Under 2024 har det tagits nya initiativ i frågan, då avdelningen för it och digitalisering arbetar med att ta fram en mer heltäckande vägledning som rör informationshantering i flera olika tjänster, bl.a. e-post, samarbetsytor och hemkataloger. Arbetet med vägledningen pågår.

Slutligen föreslogs att det ska utses ansvariga för framtagande av rutiner och instruktioner. Det har under hösten 2024 initierats en dialog med avdelningarna kring detta.

3.2.4 Dataskyddsombudets råd och rekommendationer gällande styrdokument

Det är angeläget att det är enkelt för medarbetare att hitta gällande styrdokument inom området för dataskydd, både stadsövergripande och lokala. Det är lämpligt att hänvisa till styrdokumenten via sidorna på intranätet.

Riktlinjer kring hantering av personuppgiftsincidenter återfinns idag som en del i stadsledningskontorets rutin för hantering av informationssäkerhetsincidenter. Nuvarande rutin berör främst personuppgiftsincidenter av systemmässig karaktär, t.ex. gällande ett verksamhetssystem, applikation eller it-infrastruktur. Rutinen bör kompletteras med tydligare vägledning kring personuppgiftsincidenter av annan karaktär, t.ex. sådana som beror på mänskliga faktorn eller brist i organisatoriska rutiner eller processer (dvs. den mest förekommande typen av personuppgiftsincidenter).

Överlag bör beaktas att bestämmelser och principer i dataskyddsförordningen inte motsvarar regelverket för informationssäkerhet. Även om det finns en strävan att samordna de bägge områdena i gemensamma processer går det inte att ersätta vägledning som baseras på dataskyddsförordningen med vägledning som baseras på regelverket för informationssäkerhet. Exempelvis skiljer sig de bedömningar som behöver göras vid hantering av personuppgiftsincidenter från de som behöver göras vid informationssäkerhetsincidenter. I den mån vägledning baserad på

dataskyddsförordningen inte ges utrymme i rutiner och riktlinjer som rör informationssäkerhet, måste sådan vägledning tillgängliggöras i annan stöddokumentation.

Dataskyddsförordningen innehåller ett antal grundläggande principer som gäller för all personuppgiftsbehandling och sätter de yttersta ramarna för vad som är en tillåten behandling. Det är angeläget att de grundläggande principerna genomsyrar all hantering av personuppgifter och således att de är väl kända för alla anställda inom kommunstyrelsen.

- Kommunstyrelsen bör se över och komplettera befintlig rutin för hantering av personuppgiftsincidenter. Det är angeläget att rutinen omfattar alla slags personuppgiftsincidenter. Rutinen bör även innehålla en förteckning över de många faktorer som ska beaktas vid bedömningen av en personuppgiftsincidents allvarlighetsgrad, vägledning kring när de registrerade behöver informeras om en inträffad incident samt vilka uppgifter en sådan information behöver innehålla. Det behöver vara tydligt vilken roll/funktion som ansvarar för vad inom ramen för utredningen av en personuppgiftsincident. Om ansvaret varierar beroende på incidentens karaktär bör vägledningen på detta område vara särskilt tydlig. Det är angeläget att rutinen även ger en god vägledning kring hur kommunstyrelsen ska agera för det fall att en personuppgiftsincident sker i en personuppgiftsbehandling för vilken kommunstyrelsen utgör personuppgiftsbiträde till en annan nämnd eller bolag.

- Dataskyddsombudet rekommenderar att kommunstyrelsen tar fram en vägledning som översiktligt redogör för kommunstyrelsens regler och processer kring dataskydd och personuppgiftsbehandling (en intern integritetspolicy eller motsvarande). Vägledningen bör innehålla grundläggande information om förutsättningarna för behandling av personuppgifter, bl.a. vad gäller rättslig grund och de grundläggande principerna (artikel 5 dataskyddsförordningen) som ska tillämpas vid all personuppgiftsbehandling.

- Dataskyddsombudet rekommenderar att kommunstyrelsen följer upp huruvida befintlig stöddokumentation ger kommunstyrelsens anställda tillräcklig vägledning kring hur de ska behandla personuppgifter i det dagliga arbetet.

Avsaknad vägledning, särskilt sådan som har bäring på de grundläggande principerna i artikel 5 dataskyddsförordningen, bör skyndsamt tas fram.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Allmänt om tekniska och organisatoriska åtgärder

Personuppgiftsansvariga ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med personuppgiftsbehandlingen. 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 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 den personuppgiftsansvarige att säkerställa samt löpande följa upp säkerheten i den personuppgiftsbehandling som sker hos personuppgiftsbiträden.

För att kunna skydda information (inklusive personuppgifter) med rätt slags skyddsåtgärder ska verksamheterna informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Inom ramen för informationsklassningen tas det fram en handlingsplan enligt vilken lämpliga tekniska och organisatoriska åtgärder identifieras.

Informationsklassning görs inom ramen för kommunstyrelsens informationssäkerhetsarbete. Informationssäkerhetssamordnaren och dataskyddsombudet bör samverka kring planering och uppföljning av verksamhetens informationsklassningar och i det övriga arbetet som rör skyddet av personuppgifter.

3.3.2 Årlig uppföljning gällande tekniska och organisatoriska åtgärder

Uppföljning	Svar/bedömning
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	113 st. (från 2020 och framåt)
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.3 Uppföljning av föregående års rekommendationer gällande tekniska och organisatoriska säkerhetsåtgärder

I 2023 års rapport beskrivs ett rekommenderat införande av en ny process i form av s.k. integritetsskyddsanalyser. Efter att ha utrett bakgrunden till och avsikten med denna rekommendation har verksamheten kommit fram till att de bedömningar som var avsedda att göras inom ramen för integritetsskyddsanalyserna redan görs idag inom ramen för befintliga processer, bl.a. genom upprättandet av riskanalyser och konsekvensbedömningar. Rekommendationen betraktas således som omhändertagen.

I föregående års rapport beskrevs risken med att dataskyddsombuden inte längre involveras i förankringsprocessen för den stadsövergripande funktionen för informationssäkerhet. Inom kommunstyrelsen omhändertas denna risk delvis genom att man har säkerställt att dataskyddsombudet deltar på de regelbundna nätverksträffarna för informationssäkerhetssamordnare samt ingår i sändlistan för nätverkets nyhetsbrev.

3.3.4 Dataskyddsombudets råd och rekommendationer gällande tekniska och organisatoriska åtgärder

Inom kommunstyrelsen är det objektägare som, i enlighet med stadsledningskontorets lokala anvisning om

informationssäkerhet, har ett ansvar för att klassning, riskanalys och eventuell konsekvensbedömning avseende dataskydd genomförs avseende objektet (it-systemet eller motsvarande). I den lokala anvisningen redogörs för de omfattande antal moment i detta arbete som objektägaren ansvarar för, vilket inkluderar bl.a. identifiering och implementering av skyddsåtgärder, uppföljning av skyddsåtgärderna samt beslut om behörighetstilldelning.

- För en korrekt och ändamålsenlig informationsklassning samt identifiering av adekvata tekniska och organisatoriska säkerhetsåtgärder är det av vikt att objektägare omsorgsfullt bedömer vilka roller och funktioner som ska delta i arbetet med informationsklassningar och riskanalyser. Framtagande av handlingsplan för behandling av känsliga personuppgifter, eller andra s.k. särskilda kategorier av personuppgifter, bör ske i samråd med dataskyddsombudet.

3.4 Konsekvensbedömningar

3.4.1 Allmänt om konsekvensbedömningar

Genomförandet av konsekvensbedömningar hjälper en organisation att identifiera och minimera integritetsriskerna vid personuppgiftsbehandlingar som, utifrån kriterierna i artikel 35 dataskyddsförordningen, bedöms medföra en hög risk för de registrerades fri- och rättigheter. 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. Utifrån en analys av de identifierade riskerna identifieras riskförebyggande åtgärder som behöver vidtas för att personuppgiftsbehandlingen ska kunna ske på ett tillräckligt säkert sätt.

Staden har en mall samt ett metodstöd för konsekvensbedömning. För närvarande (december 2024) pågår ett arbete vid juridiska avdelningen med att uppdatera mallen samt att ta fram en vägledning för bedömningen av huruvida en konsekvensbedömning behöver upprättas eller ej (s.k. tröskelanalys). Inom kort kommer Integritetsskyddsmyndigheten (IMY) att publicera en vägledning gällande konsekvensbedömning varför stadsledningskontoret avvaktar publicering av ny mall och stöddokumentation tills IMY har publicerat sin vägledning.

3.4.2 Årlig uppföljning gällande konsekvensbedömningar

Uppföljning	Svar/bedömning
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Kan utläsas av kommunstyrelsens register över personuppgiftsbehandlingar
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej, arbete med att genomföra kvalitativa konsekvensbedömningar pågår löpande
Är de genomförda bedömningarna aktuella?	Ja

3.4.3 Uppföljning av föregående års rekommendationer gällande konsekvensbedömning

I 2023 års rapport föreslog dataskyddsombudet att det tas fram en dokumenterad process för att genomföra referenskonsekvensbedömning avseende dataskydd inom staden. Juridiska avdelningen har under året tagit fram en sådan dokumenterad process, som även har testats och visat sig fungera väl.

I föregående års rapport lämnade dataskyddsombudet råden att genomförande av konsekvensbedömningar behöver ske i större omfattning samt att respektive avdelning på stadsledningskontoret behöver kartlägga behoven av konsekvensbedömningar. Under 2024 har flera konsekvensbedömningar genomförts och fler planeras att genomföras under kommande år allteftersom behov identifieras. Det förs en pågående dialog med avdelningarna i syfte att identifiera behovet av konsekvensbedömningar samt kring det stöd som erbjuds för genomförandet. Sammantaget bedöms det ha skett en god utveckling gällande arbetet med konsekvensbedömningar under året.

3.4.4 Dataskyddsombudets råd och rekommendationer gällande konsekvensbedömning

- Dataskyddsombudet rekommenderar att arbetet med att identifiera behovet av konsekvensbedömningar samt genomförandet av konsekvensbedömningar fortsätter under 2025.

- Kommunstyrelsen bör prioritera att upprätta konsekvensbedömningar gällande personuppgiftsbehandlingar som innebär automatiserat beslutsfattande, användning och utveckling av AI samt vid behandling av särskilda kategorier av personuppgifter (t.ex. uppgifter om hälsa eller biometriska uppgifter) samt skyddade personuppgifter.

- Konsekvensbedömningar som rör användning av AI medför flera utmaningar, framför allt vad gäller analys och beskrivning av hur personuppgifterna behandlas i verktyget samt avvägningar kring ändamålsbegränsning och uppgiftsminimering. För att underlätta arbetet bör kommunstyrelsen ta fram en vägledning på detta område.

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

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

3.5 De registrerades rättigheter

3.5.1 Allmänt om de registrerades rättigheter

De registrerade (de vars personuppgifter behandlas, t.ex. medborgare och anställda) har enligt dataskyddsförordningen ett flertal rättigheter som på olika sätt ska garantera att den registrerade har insyn i hur dennes personuppgifter behandlas. En registrerad har t.ex. rätt till tillgång till sina personuppgifter (s.k. registerutdrag), rätt till rättelse och i vissa fall rätt till begränsning och radering.

Den personuppgiftsansvarige måste besvara en registrerads önskemål om registerutdrag 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. Det kan även leda till tillsyn med sanktioner som följd.

I enlighet med principen om öppenhet (art. 5.1 a dataskyddsförordningen) ska personuppgifter behandlas på ett öppet sätt i förhållande till den registrerade. Den registrerade (den vars personuppgifter behandlas, t.ex. medborgare eller anställd) har rätt till klar och tydlig information om kommunstyrelsens behandling av deras personuppgifter samt hur den ska gå tillväga för att tillvarata sina rättigheter enligt dataskyddsförordningen. Vid juridiska avdelningen pågår för närvarande ett arbete med att se över den information om personuppgiftsbehandling som riktar sig till medborgare (som huvudsakligen tillhandahålls genom stadens externa hemsida).

3.5.2 Årlig uppföljning gällande de registrerades rättigheter

Uppföljning	Svar/bedömning
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Två begäran om registerutdrag och två begäran om radering
Hur många av dessa begäranden har hanterats av verksamheten inom 30 dagar?	Samtliga

3.5.3 Uppföljning av föregående års rekommendationer gällande de registrerades rättigheter

I föregående års rapport rekommenderade dataskyddsombudet att metodstödet för de registrerades rättigheter ses över och uppdateras. Det pågår för närvarande (december 2024) ett arbete med att se över informationen om de registrerades rättigheter som finns på

stadens externa hemsida. Juridiska avdelningen arbetar dessutom med att ta fram ett webformulär genom vilket de registrerade på ett enkelt sätt kan tillvarata sina rättigheter, t.ex. begära registerutdrag. Juridiska avdelningen är dessutom i slutskedet av ett arbete med att förbättra den interna processen för hantering av begäran om registerutdrag.

I 2023 års rapport gav dataskyddsombudet rådet att kommunstyrelsen bör fortsätta det pågående arbetet med att uppdatera informationstexter till de registrerade kring hur personuppgifter behandlas inom kommunstyrelsen samt kartlägga behoven av ytterligare informationstexter. Det har vid juridiska avdelningen initierats ett arbete med att ta fram en informationstext som riktar sig till kommunstyrelsens anställda och förtroendevalda. Informationen tas fram i samråd med personalstrategiska avdelningen. Avsikten är att ha en första version klar för publicering under första kvartalet 2025. Det har även initierats ett arbete med att kartlägga och följa upp avdelningarnas behov av att ta fram ytterligare informationstexter.

Slutligen gav dataskyddsombudet rådet om att det bör tas fram en process som beaktar personuppgifts- och behandlingsbegreppets vida tolkning, gärna digital, som följer EDPB:s riktlinje 01/2022 om registrerades rättigheter. En process har tagits fram och förankrats med samrådsgruppen för strategiska stadsövergripande informationssäkerhetsfrågor.

3.5.4 Dataskyddsombudets råd och rekommendationer gällande de registrerades rättigheter

- Dataskyddsombudet rekommenderar att kommunstyrelsen skyndsamt färdigställer och tillgängliggör information om personuppgiftsbehandling som riktar sig till kommunstyrelsens anställda och förtroendevalda. Den information som lämnas ska vara förenlig med art. 12-14 dataskyddsförordningen. Informationen bör tillhandahållas i anslutning till nyanställning, men det är angeläget att den även är lätt att hitta under anställningens gång.

- Kommunstyrelsen bör generellt prioritera att löpande följa upp att god och tydlig information om

personuppgiftsbehandling lämnas till de registrerade i adekvat omfattning, både internt (anställda, förtroendevalda m.fl.) och externt (medborgare och andra externa parter). Endast genom klar och tydlig information om den personuppgiftsbehandling som sker hos kommunstyrelsen kan de registrerade tillvarata sina rättigheter på ett integritetssäkert och tryggt sätt.

3.6 Personuppgiftsincidenter

3.6.1 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 dataskyddsförordningen).

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 Integritetsskyddsmyndigheten.

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 hanteringen 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 verksamhetens 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 incidenten. Varje annan personuppgiftsansvarig nämnd eller bolag måste skyndsamt informeras, oavsett om kommunstyrelsen identifierat en incident i rollen som personuppgiftsansvarig eller personuppgiftsbiträde.

3.6.2 Årlig uppföljning gällande personuppgiftsincidenter

Uppföljning	Svar/bedömning
Hur många personuppgiftsincidenter har dokumenterats?	Fem
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Inga
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	-

3.6.3 Uppföljning av föregående års rapportering gällande personuppgiftsincidenter

I 2023 års rapport redogjorde dataskyddsombudet för flera rekommendationer kring hantering av personuppgiftsincidenter. Bl.a. föreslogs förtydliganden i processen, tydligare vägledning kring ansvarsförhållanden och att dokumentationsskyldigheten ses över. Dataskyddsombudet rekommenderade också att kommunstyrelsen i utformningen av vägledning beaktar de olika ansvarsrollerna (personuppgiftsansvarig respektive personuppgiftsbiträde) som kommunstyrelsen har inom staden. Några större justeringar i processen har inte gjorts under året.

3.6.4 Dataskyddsombudets råd och rekommendationer gällande hantering av personuppgiftsincidenter

- Vid inträffad personuppgiftsincident är det angeläget att det är helt tydligt för samtliga avdelningar vem som förväntas agera och hur. Oklarheter härom utgör en stor risk ur ett integritetsperspektiv och således för kommunstyrelsen. En rekommendation kring översyn av styrdokument och processer för hantering av personuppgiftsincidenter finns i avsnitt 3.2.4 ovan.

- Det är angeläget att dataskyddsombudet involveras vid samtliga identifierade personuppgiftsincidenter.

- Rutinerna för hur kommunstyrelsen ska agera vid personuppgiftsincidenter som berör andra personuppgiftsansvariga inom staden bör förtydligas, särskilt vad gäller informationsöverföring.

- 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 efter utredning bedöms ha utgjort en låg risk (och således inte anmälts till IMY).

4 Genomförda och planerade granskningar

4.1 Genomförda granskningar under 2024

Under 2024 har dataskyddsombudet, liksom föregående år, prioriterat att ge råd och stöd i kommunstyrelsens pågående dataskyddsarbete. Några riktade granskningar har inte utförts, utöver sådana som har identifierats och genomförts löpande i specifika frågor, t.ex. vid upprättande av nya avtal, konsekvensbedömningar eller inom ramen för pågående projekt.

4.2 Planerade granskningar under 2025

Under 2025 planerar dataskyddsombudet att initiera ett nytt arbetssätt enligt vilket granskningar kommer att genomföras både i form av stickprovskontroller och särskilda granskningar på förekommen anledning (t.ex. vid misstanke om brister eller som uppföljning på klagomål). För att uppnå en förutsägbarhet och enhetlighet i uppföljningen kommer underlag i form av två olika formulärsmallar att tas fram under första kvartalet 2025. Avsikten med granskningarna, som lämpligen ska benämnas ”interna uppföljningar”, är uteslutande att på bästa sätt identifiera förbättringsområden och därmed kunna ge ett gott och ändamålsenligt stöd till avdelningarna.

4.2.1 Dataskyddsombudets årshjul

Under första kvartalet 2025 kommer dataskyddsombudet att ta fram ett årshjul som tydligt illustrerar det övergripande planerade arbetssättet med interna uppföljningar (enligt avsnittet ovan) vid kommunstyrelsen.

5 Övrigt att rapportera

5.1 AI (artificiell intelligens)

För närvarande är artificiell intelligens (AI) ett område som är under snabb utveckling och som används – eller kommer att användas – inom ramen för många it-produkter, applikationer och tjänster. AI-förordningen (EU:s allmänna reglering av AI) trädde i kraft i augusti 2024 och ska tillämpas fullt ut i Sverige från och med augusti 2026.

Tekniken bakom AI väcker flera integritets- och dataskyddsfrågor. Utveckling, träning och användning av AI kräver i regel stora mängder data. I den mån det data som hanteras i AI-systemet utgör personuppgifter, antingen oberoende eller kombinerat med annan data, ska regleringen i dataskyddsförordningen tillämpas.

5.1.1 Utmaningar med AI ur ett dataskyddsperspektiv

Ur ett dataskyddsperspektiv väcks primärt kraven på ändamålsbegränsning och uppgiftsminimering, men även vikten av att vara vaksam kring riskerna för kvalitetsbrister i algoritmer (t.ex. data som påverkats av bias) som, beroende på hur AI används, skulle kunna leda till att inadekvata personuppgifter behandlas, vilket är oförenligt med dataskyddsförordningens princip om korrekthet.

För att det ska vara tillåtet att behandla redan insamlade personuppgifter för ett annat ändamål än det ursprungliga (t.ex. träning av AI-modell) får det nya ändamålet inte vara oförenligt med det ursprungliga ändamålet. Den personuppgiftsansvarige måste göra en samlad bedömning kring huruvida ändamålet med den nya personuppgiftsbehandlingen är förenlig med det ursprungliga ändamålet. I bedömningen ska man bl.a. beakta kopplingarna kring ändamålen, i vilket sammanhang uppgifterna har samlats in, vilken slags uppgifter som behandlas och vad den registrerade rimligen kan förvänta sig. Om behandlingen inte bedöms förenlig med det ursprungliga ändamålet med behandlingen krävs en ny giltig rättslig grund för personuppgiftsbehandlingen.

Principen om uppgiftsminimering medför framför allt utmaningar vid träning av en AI-modell. Ju mer data en modell tränas med, ju mer korrekt blir den. Samtidigt kräver dataskyddsförordningen att personuppgiftsbehandlingen är adekvat, relevant och inte för omfattande i förhållande till ändamålet. Det behöver göras en proportionalitetsbedömning där man säkerställer att integritetsrisken med behandlingen är rimlig i förhållande till nyttan med behandlingens ändamål. Samtliga bedömningar behöver dokumenteras. Dokumentation sker lämpligen inom ramen för konsekvensbedömningen.

En annan utmaning för personuppgiftsansvariga utgörs av den s.k. ’black box’-problematiken, enligt vilken komplexiteten i vissa AI-modeller medför att det är nästintill omöjligt för en fysisk person att få en adekvat bild av *hur* personuppgifter (indata) behandlas för att producera ett utfall (utdata). Utöver att den personuppgiftsansvarige behöver ha en dokumenterad förståelse för personuppgiftsbehandlingen föreligger dessutom en skyldighet att informera de registrerade om behandlingen samt även i övrigt tillgodose deras rättigheter enligt dataskyddsförordningen.

Regeringen har gett Myndigheten för digital förvaltning (Digg) och Integritetsskyddsmyndigheten (IMY) i uppdrag att ta fram vägledande riktlinjer för användning av generativ artificiell intelligens (AI) inom den offentliga förvaltningen. Redovisning av uppdraget sker i januari 2025.

Till *Stockholm stads plan och inriktning för Artificiell intelligens (AI)*[2] finns bilagan *Rättsliga frågor vid användning av AI*, i vilken det redogörs för stora delar av ovanstående utmaningar.

5.1.2 Automatiserat, individuellt beslutsfattande

Automatiserat, individuellt beslutsfattande innebär att beslut fattas utan att en fysisk person är inblandad. Som huvudregel är automatiserat, individuellt beslutsfattande, t.ex. beslut som i sin helhet fattas av AI, förbjuden (se artikel 22 dataskyddsförordningen). Vissa begränsade undantag finns.

5.1.3 Sammanfattning AI

Dataskyddsombudet vill sammanfattningsvis betona vikten av att utveckling, upphandling och implementering av tjänster som innebär användning av AI görs med noggrant beaktande av gällande dataskyddslagstiftning. Det är ofta en god idé börja i en mindre omfattning och öka successivt.

5.2 Intern kompetensutveckling

Dataskyddsombudet har för avsikt att under 2025 se över förutsättningarna för att initiera ett upplägg om regelbunden intern kompetensutveckling. Innehåll och format behöver avgöras utifrån rättsläge, identifierade risker samt avdelningarnas specifika behov.

[2] Dnr: KS 2021/1208

6 Dataskyddsombudets roll och ställning

6.1 Allmänt om dataskyddsombudet

Dataskyddsombudets roll och ställning regleras i dataskyddsförordningen enligt vilken dataskyddsombudets uppgifter bl.a. är att informera och ge råd till kommunstyrelsen och dess stadsledningskontor i syfte att uppnå en god efterlevnad av gällande dataskyddslagstiftning.

Dataskyddsombudet ska kontrollera att dataskyddslagstiftningen följs inom organisationen och löpande tillhandahålla informations- och utbildningsinsatser.

Kommunstyrelsen ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som hanteras på kommunstyrelsens uppdrag som rör skyddet av personuppgifter. Dataskyddsombudet ska involveras i personuppgiftsfrågor där kommunstyrelsen agerar, både lokalt och stadsövergripande samt i egenskap av rollen som personuppgiftsansvarig respektive personuppgiftsbiträde.

Dataskyddsombudet har inget eget ansvar för att kommunstyrelsen följer dataskyddsförordningen. Det ansvaret ligger alltid hos kommunstyrelsen, oavsett om kommunstyrelsen agerar i egenskap av personuppgiftsansvarig eller personuppgiftsbiträde.

Dataskyddsombudet har således en roll som bistår organisationen med råd, information och utbildning för att skapa en integritetskultur som är förenlig med gällande lagstiftning. Dataskyddsombudet ska i utförandet av sitt uppdrag bidra till att kommunstyrelsen, genom stadsledningskontoret, kan prioritera och omsätta de rekommendationer som lämnas i denna rapport till faktiska aktiviteter som ytterst ska värna stockholmarnas och de anställdas grundläggande rättigheter och friheter när det gäller skyddet av personuppgifter.

6.2 Samordnad åtgärd avseende dataskyddsombudsrollen (uppföljning från 2023 års rapport)

I föregående års rapport beskrivs den samordnade åtgärd för att undersöka dataskyddsombudens roll och ställning som initierades av Europeiska dataskyddsstyrelsen (EDPB) i början av 2023. 26 dataskyddsmyndigheter deltog i den samordnade åtgärden, däribland Integritetsskyddsmyndigheten (IMY).

Inom ramen för den samordnade åtgärden inledde IMY en tillsyn avseende cirka 40 verksamheter i Sverige, både offentliga och privata. Frågor som utretts inom ramen för tillsynen rör bl.a. huruvida organisationens ledning tydligt har definierat och gett en skriftlig beskrivning av dataskyddsombudets uppgifter, vilka arbetsuppgifter dataskyddsombudet har och om dataskyddsombudet har tillräckliga resurser för att utföra dessa arbetsuppgifter.

Fem av tillsynsobjekten, däribland socialnämnden i Stockholms stad, har granskats med fokus på hur verksamheterna hanterar eventuella intressekonflikter för dataskyddsombuden. I ärendet gällande socialnämnden i Stockholms stad (IMY-2023-7957) tog IMY ställning till huruvida det föreligger en intressekonflikt mellan rollen som dataskyddsombud för socialnämnden och rollen som förvaltningsjurist vid socialförvaltningen i Stockholms stad. Rollen som förvaltningsjurist innebär främst rådgivande arbetsuppgifter som främst rör förvaltningsjuridiska frågor och innebär inte i normalfallet att frågor om dataskydd aktualiseras och hanteras. I den mån dataskyddsfrågor skulle aktualiseras ser IMY en möjlig intressekonflikt genom att dataskyddsombudet i dessa fall skulle involveras i det dataskyddsarbete som denne i rollen som dataskyddsombud har i uppdrag att granska. Socialnämnden uppgav i ärendet att när nämnden har identifierat en sådan risk har åtgärder vidtagits genom att t.ex. en enhetschef eller annan avdelning inom organisationen har hanterat de arbetsuppgifter som rör dataskydd. Mot bakgrund härav bedömer IMY i beslut 2024-06-27 att det inte föreligger en intressekonflikt mellan rollerna.

I ett motsvarande ärende gällande Region Västerbotten (IMY-2023-7987) granskade IMY ett upplägg där dataskyddsombudet även innehade tjänsten som regionsjurist vid regionens ledningsstab. Regionen anförde att varken rollen som dataskyddsombud eller regionjurist innebär att man arbetar operativt med dataskyddfrågor, utan endast med rådgivning och stöd. IMY kom trots det fram till att dessa två uppdrag medförde en intressekonflikt som är oförenlig med dataskyddsförordningen.

En slutsats utifrån praxis är att IMY har lagt särskild vikt vid huruvida det funnits tydliga rutiner och mekanismer för att minska risken för intressekonflikter.

Det kan dock konstateras att gränsdragningen kring bedömningen av huruvida det föreligger en intressekonflikt inte är helt tydlig. I ett av besluten (IMY-2023-7956, gällande PostNord) skriver IMY: *Av redogörelsen framgår att arbetsuppgifterna inte medför ett ansvar som leder till delaktighet i beslut rörande ändamål och medel för personuppgiftsbehandlingar. Inte heller framgår det av beskrivningen att uppgifterna innebär ett ansvar för att i övrigt, t.ex. genom råd eller stöd, hantera dataskyddsrättsliga frågor. IMY finner mot den bakgrunden att utredningen i ärendet inte visar att det föreligger en intressekonflikt i strid med dataskyddsförordningen genom att inneha de beskrivna uppgifterna vid sidan av rollen som dataskyddsombud.*

Eftersom det rimligen inte är uteslutet (snarare lämpligt) att dataskyddsombud lämnar råd och stöd i dataskyddsrättsliga frågor, så framstår skrivningen ovan som något oklar. Det finns skäl att hålla sig informerad om kommande praxis och vägledning på området.

Sammanfattningsvis kan det konstateras att viss försiktighet bör iakttas, men framför allt att det är eftersträvansvärt med dokumenterade instruktioner och arbetssätt som visar hur organisationen arbetar för att motverka intressekonflikter för dataskyddsombudet.