Stockholms stad

GDPR Årsrapport

2024

S:t Erik Markutveckling AB

GDPR årsrapport
Januari 2025

Dnr: STEM 2025/19
Utgivningsdatum: 2025-01-17
Kontaktperson: Jessica Hillergård

Sammanfattning

I egenskap av S:t Erik Markutveckling AB:s dataskyddsombud, DSO, lämnar jag följande årsrapport.

År 2024 var året som AI-verktygen började implementeras i IT-tjänster där man minst kunnat ana det tidigare. Den nya lagen om AI, AI förordningen, antogs i EU under våren och kommer implementeras under de kommande åren i olika faser. Ur ett dataskyddsperspektiv blir frågorna än mer intressanta och komplexa i och med att AI:n skapar nya personuppgiftsbehandlingar och med det nya utmaningar. Det är också uppmärksammat att ett antal incidenter har skett i staden under året då nya AI:n implementerats av misstag i olika digitala verktyg vid uppdateringar. En av de granskningar jag prioriterar under 2025 är just AI och medföljande integritetsproblematik.

Samhället har under 2024 påverkats av flera uppmärksammade personuppgifts- och informationssäkerhetsincidenter, bland annat en större ransomware-attack hos TietoEvry i januari. Incidenten skapade stor oro och informationen var otydlig till en början i stadens verksamheter. Turligt nog klarade sig Stockholm stad i den attacken, men andra kommuner drabbades samtidigt mycket hårt.

Den granskning som skulle genomföras som uppföljning av ett personuppgiftsbiträde under 2024, blev utbyt mot livscykelhantering av information. Rekommendationen är att se över den processen under 2025 i samarbete mellan informationssäkerhetssamordnaren, handläggare och DSO.

Samarbetsgruppen mellan datsskyddshandläggare, informationssäkerhetssamordnare och dataskyddsombud har blivit än mer systematiskt under 2024. En av de aktiviteter som genomförts är en större övergripande riskanalys utifrån dataskydd och informationssäkerhet.

En rekommendation för att åtgärda en risk från dataskyddsombudets årsrapport 2023 har genomförts under år 2024. Risken innebar brister i kontinuitetshanteringen. Det har nu åtgärdats med en avbrottsplan. STEM är en liten väl fungerande organisation som hela tiden vill bli bättre och finna åtgärder på brister. Det gör det lättare och roligare för mig som dataskyddsombud att genomföra mitt uppdrag när organisationen är engagerad och vill förbättras!

Jessica Hillergård

Dataskyddsombud

Innehåll

1 Bakgrund

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

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

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

Denna årsrapport är således ett medel för styrelsen att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen. I rapporten får styrelsen insyn i vad dataskyddsombudets granskningar visat av verksamheten och status avseende integritet och dataskydd. Årsrapporten syftar till att styrelsen ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur styrelsen som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

2 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som personuppgiftsansvarig, PUA, som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är:

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter
- personuppgiftsincidenter

Nedan redogörs för bolagets status och dataskyddsombudets slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter dataskyddsombudets genomförda uppföljning och granskning.

2.1 Registerförteckning

2.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	15
Har nödvändiga uppdateringar gjorts?	JA
Bedöms registerförteckningen vara fullständig?	JA
Har verksamheten lämpliga rutiner för registerföring?	JA

2.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister eller register av register).

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att PUA får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna om individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete. Man kan styra insatserna där de gör störst nytta.

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

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

2.1.3 Resultat

2.1.3.1.1 DSO kontrollerar hur många behandlingar som registrerats

15 st.

2.1.3.1.2 DSO kontrollerar om nödvändiga uppdateringar gjorts

Ja, finns dokumenterat i wordlogg och spårbarhet i Samarbetsytan STEM GDPR.

2.1.3.1.3 DSO bedömer hur fullständig registerförteckningen är

STEM använder sig av en Excelfil på en samarbetsyta för registerförteckningen. Den har samtliga områden som ska dokumenteras ifyllda.

2.1.3.1.4 DSO bedömer om verksamheten har lämpliga rutiner för registerföring

I årshjulet finns aktivitet nedtecknad när registerförteckningen ska kontrolleras och uppdateras vid behov.

2.1.4 DSO anger hur allvarliga bristerna är på en skala

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

2.1.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets råd är att fortsätta uppdatera registerförteckningen enligt årshjulet.

2.2 Styrdokument

2.2.1 Sammanfattning

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

2.2.2 Syfte

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

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

En brist inom detta område bör förstås ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör lyftas fram till PUA. Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till bristande kvalitet i hur verksamheten utför aktiviteterna, men även till att verksamheten slösar värdefulla resurser när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

2.2.3 Resultat

S:t Erik Markutveckling har en GDPR-handbok där samtliga rutiner och kontaktpersoner finns beskrivna. Lokal anvisning för informationssäkerhet finns som kompletterande styrdokument och antogs samt implementerades 2023. Kontinuitets-/avbrottsplan har tagits fram 2024 av informationssäkerhetssamordnaren.

SLK har tagit fram en ny mall för lokal tillämpningsanvisning för informationssäkerhet hösten 2024. Mallen saknar dataskyddsperspektivet.

2.2.4 DSO anger hur allvarliga bristerna är på en skala

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

2.2.5 DSO ger råd och rekommendationer till PUA

När den nya mallen för lokal tillämpningsanvisning för informationssäkerhet ska appliceras på STEM behöver dataskyddsperspektivet omhändertas. Detta genom att text om dataskydd läggs till eller ett nytt eget tillämpningsdokument dokument skapas enbart för GDPR.

2.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

2.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Samtliga
Är klassade personuppgiftsbehandlingar aktuella?	JA

2.3.2 Syfte

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

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

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

Viktigt är också att notera att Dataskyddsombudet omhändertar den registrerades intresse och informationssäkerhetssamordnaren har fokus på verksamhetens krav på informationen i form av tillgänglighet, riktighet och konfidentialitet. Verktyget för DSO är i första hand registerförteckningen och dokumentationen där.

Informationssäkerhetssamordnaren har KLASSA som verktyg för att se till att verksamhetens krav efterlevs i form av dokumentation i förvaltningsplaner, systembeskrivningar etc.

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare. Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll.

2.3.3 Resultat

STEM har valt att ta fram en egen klassificeringsguide baserat på de lagkrav som man efterlever förutom GDPR. I registerförteckningen anges klassning utifrån guiden. Granskning av registerförteckningen har skett av dataskyddsombudet och dataskyddshandläggaren. Arbetet sker systematiskt efter årshjul.

2.3.4 DSO anger hur allvarliga bristerna är på en skala

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

2.3.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets råd är att vid den årliga genomgången av registerförteckningen också kontrollera att de tekniska och organisatoriska kraven efterlevs.

2.4 Konsekvensbedömningar

2.4.1 Sammanfattning

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

2.4.2 Syfte

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

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

2.4.3 Resultat

Under år 2024 har inga konsekvensbedömningar genomförts. Detta då inga nya högriskbedömningar enligt de kriterier som tagits fram av IMY, Integritetsskyddsmyndigheten, och EDPB, Europeiska dataskyddsstyrelsen. Vid varje avstämningsmöte mellan dataskyddshandläggare, dataskyddsombud och informationssäkerhetssamordnare lyfts frågan om nya personuppgiftsbehandlingar och eventuella behov av vidare analyser.

2.4.4 DSO anger hur allvarliga bristerna är på en skala

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

2.4.5 DSO ger råd och rekommendationer till PUA

Vid varje ny upphandling av tjänst eller system bör dataskyddsombudet rådfrågas om konsekvensbedömningsfrågan behöver lyftas in som ett hjälpmedel för att få rätt kravspecifikation.

2.5 Individens rättigheter

2.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	N/A

2.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

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

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

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningen krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från

Intetgritetsskyddsmyndighetens, IMY:s sida, med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

2.5.3 Resultat

I GDPR-handboken finns beskriven rutin för olika scenarion av begäran från en registrerad. Dock har det inte varit aktuellt med någon form av begäran av en registrerad under 2024.

2.5.4 DSO anger hur allvarliga bristerna är på en skala

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

2.5.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet ger som rekommendation att granska rutinen årligen för att hålla den uppdaterad.

2.6 Personuppgiftsincidenter

2.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	N/A
Hur många personuppgiftsincidenter har dokumenterats?	2
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	0

2.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

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

personers rättigheter ska de berörda registrerade personerna, utan dröjsmål underrättas.

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

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad osv.

2.6.3 Resultat

Då organisationen har en väldigt liten andel personuppgiftsbehandlingar med ett fåtal registrerade, så är det lätt att se om det sker personuppgiftsincidenter. Under 2024 har 2 incidenter skett. Dessa två drabbade samtliga organisationer i Stockholm stad och berodde på uppdateringar av tjänster som innehöll AI-verktyg som skapade nya personuppgiftsbehandlingar.

2.6.4 DSO anger hur allvarliga bristerna är på en skala

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

2.6.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att ha en information om vad en personuppgiftsincident innebär med personalen årligen, så att kunskapen inte glöms bort.

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskningar:

- *Uppföljning 2023 års granskning*

3.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

3.3 Genomförda granskningar och deras resultat

3.3.1 Granskning Uppföljning 2023 års granskning

I årsrapporten för 2023 skrev jag som dataskyddsombud:
”Bristen som kvarstår att granska till 2024 är att kommunikationsvägarna för registrerade d.v.s. den allmänna e-postadressen omhändertar frågor om dataskydd och eventuella begäran från registrerade fungerar.”

Under 2024 upphandlades förvaltarrollen och denna granskning blev istället för att kontrollera kommunikationsvägar, följa upp befintliga avtal för att eventuellt avsluta tjänsten. Detta perspektiv omhändertogs tillsammans med informationssäkerhetssamordnaren och dataskyddshandläggaren.

3.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation är att se över livscykelprocessen för hanteringen av informationsmängder och de system som behandlar dem.

4 Risker inom dataskydd

4.1 Sammanfattning

Relevanta risker inom verksamheten:

- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (STEM:s) objektförvaltning. (Ny)
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation. (Ny)
- Tredjelandsöverföringar (Kvarstår)
- Osäker e-posthantering med personuppgifter (Kvarstår)

4.2 Syfte

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

Under år 2024 har en riskanalys genomförts tillsammans med informationssäkerhetssamordnaren för att hitta gemensamma åtgärder.

Risk beräknas utifrån RISK= Sannolikhet x Konsekvens

Sannolikhet (1 låg - 5 hög):
Låg risk - Inte trolig att inträffa
Hög risk - Kommer med all sannolikhet att inträffa

Konsekvens (1 liten - 5 stor):
Liten konsekvens - Ingen större påverkan
Stor konsekvens - Omfattande, dyrt kan ändra förutsättningarna dramatiskt

Riskvärde
Låg < 4 (riskerna skall bevakas)
Medel 5-14 (riskerna skall hanteras eller elimineras)
Hög > 15 (riskerna skall elimineras)

4.3 Resultatet av riskkartläggningen

4.3.1 Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (STEM:s) objektförvaltning

Som tidigare nämnt flera kapitel har det uppstått problem i införande av nya tjänster beroende på resursbrist hos central förvaltning. Detta påverkar implementation av nya gemensamma IT-tjänster och det systematiska arbetet som ska ske löpande i den egna lokala organisationen. En av de anledningar att exempelvis ”Säkra meddelanden” inte införts är då det saknas centralt utsedda ansvarsroller och åtgärder som ska införas inte följs upp eller återrapporteras att de genomförts.

	Hög > 15 (riskerna skall elimineras)
X	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.3.2 Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation

Under år 2024 växte efterfrågan på AI och möjligheten att effektivisera arbetet. Då området är nytt och så även lagstiftningen behövs tydlig och transparent dokumentation när en sådan tjänst ska införas. Tyvärr brister ofta dokumentationen från leverantörerna och den som upphandlar verktyget behöver utbilda dem genom kravställning och möten.

Integritetsriskerna är stora då effektiviteten och möjligheten att ta fram ”smarta lösningar” tenderar att gå först i hela samhället. Mitt arbete som dataskyddsombud blir då i dessa införanden än mer viktigt att agera ombud och skydda de registrerades intressen.

En del i denna risk är också att nya funktioner införs i redan befintliga tjänster. Ett exempel på detta är en transkriberingstjänst vid digitala möten. Efter mötet är klart kommer direkt ett AI-genererat protokoll med sammanfattning, beslutspunkter och

åtgärder. Det låter bra, men frågorna vi måste ställa oss då är vart sammanställdes informationen? Vem kan ta del av den? Hur känsligt blev materialet i det nya formatet? Osv. AI är ett oerhört bra och kraftfullt hjälpmedel som vi måste använda medvetet och till rätt saker.

	Hög > 15 (riskerna skall elimineras)
X	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.3.3 Tredjelandsöverföringar

Det nya inriktningsbeslutet från stadsledningskontoret som kom under hösten 2023 innebar en öppning för bolaget att använda leverantörer som använder sig av tredjelandsöverföringar. Förutsättningen är att verksamheten har en väl utformad exit-plan om överföringsmekanismen ”Data Privacy Framwork” ogiltigförklaras likt ”Privacy Shield” gjorde år 2020 och ”Safe Harbour” innan dess. I och med presidentvalet i november 2024, finns risk att den tidigare överenskommelsen med USA slås upp av den nytillträdande republikanske presidenten Donald Trumph. Flertalet leverantörer har därför börjat luta sig mot andra former av avtal för överföring till tredjeland som resultat av denna osäkra mekanism. Det i sig kräver att leverantörerna är mogna och har förberett sin dokumentation.

Flertalet leverantörer erbjuder idag endast molntjänster och de stora leverantörerna av sådana är amerikanskägda. Därav är detta en risk som behöver uppmärksammas extra.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.3.4 Risk 3 Osäker e-posthantering med personuppgifter

Varje personuppgift som ska hanteras måste behandlas säkert. När en personuppgift e-postas med någon av stadens leveranser sker

själva överföringen krypterat, men är okrypterad i in- och utboxen. Det är också inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras på ett tillräckligt bra sätt.

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” eller ”TDialog”. Kvarstående aktivitet för verksamheten, är att se över och bedöma vad tjänsten kan användas till.

Jag som DSO kan inte rekommendera i dagsläget att tjänsten används efter att jag tagit del av analysmaterialet. Samtidigt är behovet kvarstående från verksamheten att möjligheten att e-posta personuppgifter säkert och krypterat.

När årsrapporten skrevs 2023 hade projektet med arbetet av dokumentationen för Säkra meddelanden startat på SLK. Detta för att kunna besvara de risker som framkommit inom de verksamheter som gjort ena konsekvensbedömningar och riskanalyser. Work-shops genomfördes sommaren 2024.

Rekommendationen kvarstår att inte använda tjänsten utan att analysmaterialet finns färdigt. Riskerna har inte besvarats av central förvaltning och informationsmängderna som ska skickas i det är så pass känsligt och skyddsvärt.

	Hög > 15 (riskerna skall elimineras)
X	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.4 DSO ger råd och rekommendationer till PUA

Att ge råd om hur den centrala organisationen ska få mer resurs att utföra sitt arbete är svårt. Men, vi kan belysa utifrån STEM:s perspektiv att det blir svårt att arbeta effektivt när den brister och det tenderar att bygga flaskhalsar.

Som DSO rekommenderar jag att ni fortsätter vara nyfikna på ny teknik och våga satsa på den. Men, rekommendationen är att göra det med stor medvetenhet och arbeta efter den metod som finns framtagen för informationsklassning, riskanalys och konsekvensbedömning.

Risken att tredjelandsöverföringsproblematiken kommer att uppstå igen är sannolikt stor. Överföringsmekanismen bygger idag på en demokratisk presidentorder vilken kan rivas upp av den tillträdande republikanske presidenten under sin mandatperiod 2025-2029. Styrelsen rekommenderas att ta höjd för risken och bestämma aptiten för vad man är villig att riskera när man ingår nya avtal med leverantörer där överföringar till tredjeland sker. Rådet är också att ha en tydlig exitplan och genomlysa marknaden i förstahand inom Sverige och EU/EES.

Dataskyddsombudet rekommenderar att fortsätta efterfråga dokumentation och åtgärder för att kunna starta tjänsten säkra meddelanden.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Implementation av AI och AI-tjänster*

5.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett *riskbaserat synsätt*, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

5.3 Planerade granskningar

Granskning Implementation av AI och AI-tjänster
Under år 2024 har flertalet AI-tjänster tillkommit inom IT-världen. Erbjudanden kommer titt som tätt och är av skiftande karaktär och seriositet. Utifrån integritetsperspektivet är det en komplicerad fråga där den registrerades behov av skydd behöver ställas mot en organisationens krav på digitalisering, effektivisering och utveckling.

Syftet är att följa upp hur processen för tjänster som skjuts ut automatiskt från central IT-förvaltning, inte innehåller AI-verktyg som informationsklassificerats och riskbedömts av STEM.