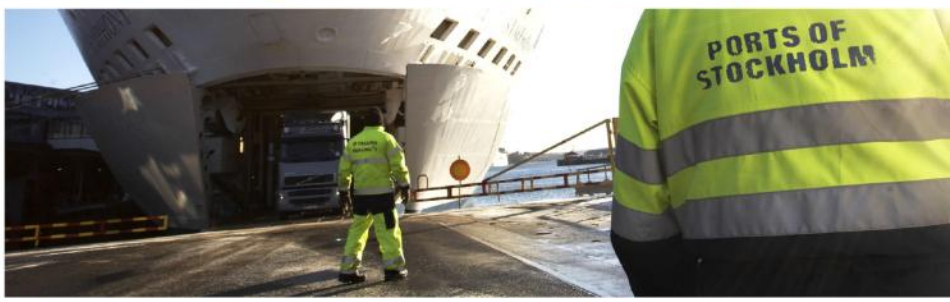
Dataskyddsombudets Årsrapport år 2024 för Stockholms Hamnar

Diarienummer SH 2025/30



Sammanfattning

I egenskap av ert dataskyddsombud 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.

En av granskningarna som tas upp i rapporten är statistik för deltagare på de obligatoriska utbildningarna i informationssäkerhet och dataskydd. Siffrorna är låga, båda 33-34 % och är underkänt. Ett riktvärde på ett bra deltagande är 75 %. Det som tyder på att kunskapen om dataskydd i organisationen är mindre moget och implementerat, är att det anmäls och uppmärksammas få personuppgiftsincidenter.

Det är bra och positivt att dataskydd- och informationssäkerhetshandläggargruppen har kommit igång igen. Under 2024 har fyra träffar genomförts och förbättringar finns inför 2025. Varje träff har ett tema där en mix av kunskapsöverföring och aktiviteter har lyfts fram.

Jessica Hillergård

Dataskyddsombud

Innehåll

1 Inledning

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

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

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett dataskyddsombud DSO. 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 styrelsen att visa hur de 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 styrelsens 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?	108
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

Registerförteckningen i finns i ett digitalt verktyg kallat DraftIt och består av ett frågeformulär per personuppgiftsbehandling vilket i sin tur blir funktionen av en checklista att alla krav i GDPR dokumenteras korrekt. Under 2024 har en översikt av registerförteckningen gjorts och anpassats mot den hanteringsanvisning med processer som Stadsarkivet har tagit fram. Kompletteringar har skett där det saknats information till vissa delar. Processbeskrivningarna i hanteringsanvisningen är inte helt anpassade mot verkligheten och det pågår ett sådant arbete inom Stockholms hamnar att förbättra dem.

I nätverket för dataskyddshandläggare inom Stockholms hamnar har ett förbättringsarbete skett under året angående vem och hur arbetet ska ske med registerförteckningen. Önskemål som framkommit var att arbeta direkt i verktyget DraftIT registerförteckning samt byta ut och lägga till andra nyckelpersoner som ansvariga. Detta tyder på att organisationen av dataskyddshandläggare börjar bli mer mogen sin arbetsuppgift. Övrig

organisation är mer omogen och behöver bli bättre på att fånga upp när dataskyddshandläggaren ska kontaktas för uppdateringar.

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

2.1.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet ger rådet att fortsätta med processkartläggningen och uppdatera registerförteckningen med resultatet. Med fördel kan då också ansvaret bli än tydligare för personuppgiftsbehandlingarnas uppdateringar. Under 2025 rekommenderas organisationen att utbilda dataskyddshandläggarna i DraftIT.

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

Organisationen arbetar efter en systemförvaltningsmodell och har flertalet styrande dokument där dataskydd omhändertas. Separat har verksamheten tagit fram rutiner för personuppgiftsincidenter, registerutdrag etc.

Den externa webben har information om personuppgiftshantering inom hamnarna. Den är dock svår att hitta då det krävs att:

1. Klicka på Om oss
2. Klicka på bolagsfakta
3. Behandling av personuppgifter – GDPR

Ett bättre alternativ är att ha länk till sidan redan längst ner på startsidan.

En ny mall för lokal tillämpningsanvisning har tagits fram på SLK, Stadsledningskontoret. Den omhändertar inte dataskyddet och dess ansvarsroller på samma sätt som tidigare.

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

Dataskyddsombudet rekommenderar att flytta/ synliggöra länken till information om personuppgiftsbehandlingar på externwebben. Det till mer lätt funnen länk längst ner på första sidan vilket är mer eller mindre standard på webbsidor. När uppdateringar görs med ny mall för lokal tillämpningsanvisning ges rådet att se över att antigen lägga till informationen där, eller skapa ett nytt dokument för dataskydd.

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?	DraftIT 108
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, ska 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

Under år 2024 har fortsatt arbete skett med förklassningsprotokoll och då i tre steg vilka är: A-klassning i designfasen, B-klassning vid införandet och C-klassning vid årlig uppföljning. Protokollet från dessa ska signeras av informationsägaren och har konkretiserat skyddsvärdet för informationen och då även personuppgifterna som kan ingå i dessa. Dataskyddsombudet har blivit inbjuden till sådana vid några tillfällen. Organisationen är *inte* självgående i klassningsarbetet utan det är individberoende.

Samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Detta kan vara behörighetsbegränsning, skydd av lösenord på dokument osv. Detta dokumenteras i DraftIT. En klassificeringsstruktur med märkning av dokument finns inte

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

2.3.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att se över så samtliga dokument inom förvaltningsmodellen också stämmer överens med tillämpningsanvisningen och vice versa samt att klassningsarbetet blir mindre avhängt att ISAM driver frågan utan sköts av organisationen med *stöd* av ISAM och DSO.

I det identifierande arbetet med processer och dess beskrivningar kan man med fördel lyfta in informationsklassning av informationsmängden och dataskyddskrav, detta för att få en helhetssyn och inte endast informationsbäraren (IT-systemet/ tjänsten) som klassas individuellt.

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

Organisationen arbetar med konsekvensbedömningar, bland annat som ett verktyg för att få fram krav innan upphandling sker. Arbetet sker gemensamt med andra organisationer i staden men också endast inom Stockholm Hamnar. Rutin finns och Hamnens bedömning är **GRÖN**.

Ett område som tidigare belysts i årsrapporterna från dataskyddsombudet, är avsaknaden av en process för när det ska ske gemensamma konsekvensbedömningar i staden. Det kan exempelvis bli aktuellt vid en central upphandling av ett IT-system som ska användas av flera organisationer inom staden. Då ingen tydlig process finns angiven från SLK blir det otydligt vem som ska sköta vad och ha ledartröjan i frågorna som uppstår i konsekvensbedömningarna. I dagsläget löser organisationerna ut det ad hoc med upparbetade inofficiella nätverk, men fastnar ofta i slutfaserna då det inte går att färdigställa dokumentationen då riskåtgärder och kravmassa har svårt att omhändertas centralt. En tydlig process ger effektivare, billigare upphandlingar. Det resulterar i en bättre beställarorganisation där organisationens krav på säkerhetsåtgärder och verksamhetens önskemål och behov omhändertas på ett korrektare sätt. Höga och okontrollerade kvarstående risker utan åtgärder kan leda till sanktioner om en konsekvensbedömning inte omhändertas korrekt. Det är också ibland oklart vem som har mandat att fatta beslut om risker vid sådana här gemensamma upphandlingar vilket är en risk. Detta ger en **GUL** bedömning.

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
X	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

Dataskyddsombudets råd är att fortsätta sprida kunskapen om konsekvensbedömningen som verktyg till upphandling och IT-projektledare. Eftersom det är ett individberoende i dagsläget så är det av vikt att flera förstår det. Konsekvensbedömningen som verktyg skapar bättre kravställningar redan i designstadiet och förenklar/förtydligar i avtal och kommunikation med leverantörer.

Styrelsen behöver också fortsatt arbeta för att process för gemensamma konsekvensbedömningar i staden implementeras, därav den gula bedömningen

2.5 Individens rättigheter

2.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Kan ej anges då endast nekande registreras enligt Stadsarkivariens gallringsregler.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Inga avvikelser har framkommit

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

Organisationen har en tydlig rutin för hur registerutdrag och andra frågeställningar av individer ska tas fram och en ägare av denna rutin finns.

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

Rekommendationen är att fortsatt hålla rutinerna uppdaterade. Under 2025 kommer en nyanställda registrator tillträda. Rådet är att passa på att se över om det fungerar för hen att arbeta på sättet framtaget av den tidigare.

2.6 Personuppgiftsincidenter

2.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom att egen personal uppmärksammar incidenter
Hur många personuppgiftsincidenter har dokumenterats?	4
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

Totalt har 4 st. incidenter med personuppgifter anmälts enligt gällande rutiner under år 2024. Av dessa består 2 av egna identifierade incidenter och 2 av centralt uppmärksammade som berört alla i Stockholm stad. Detta är en minskning sedan tidigare år och i jämförelse med andra organisationer.

Under året har en ny typ av incidenter uppmärksammats. Detta genom att AI-funktioner har implementerats vid centrala uppdateringar utan föregående konsekvensbedömningar. Risker som uppstått är t.ex. att mötesprotokoll genereras automatiskt med hjälp av ett AI där nya personuppgiftsbehandlingar skapas omedvetet och lagras utan tillräckligt skydd. AI- genererade sammanfattningar och utan kritisk granskning, kan göra att en tidigare harmlös personuppgiftsbehandling med tydlig rättslig grund plötsligt är känslig och olaglig.

Vid uppkomna incidenter som berör flera verksamheter inom hela Stockholm stad under året, har det varit tydligt att det inte fungerar med den CERT-funktion som startats centralt. Ett exempel på detta var den stora TietoEvry incidenten i januari som uppmärksammades i media. Lärdomen är att det blir snabbt ryktesspridning om inte tydlig kommunikation med korrekt, transparent och trovärdig information kommer ut vid en incident. Detta kan leda till att stadsförvaltningen inte kan göra relevanta bedömningar och åtgärder. Detta ger en GUL bedömning utifrån det centrala arbetet där organisationen påverkas negativt pga. andra organisationers brister.

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

2.6.5 DSO ger råd och rekommendationer till PUA

Styrelsen ges rådet att fortsätta påverka och uppmuntra det centrala arbetet att utveckla CERT-funktionen vid SLK. Detta för att skapa transparent information och tydliga kontaktvägar vid incidenter. Kunskap om vad och hur man hanterar personuppgiftsincidenter är en färskvara. Det finns en tydlig korrelation mellan att personalen haft utbildning i Dataskyddsförordningen och en ökad benägenhet att anmäla personuppgiftsincidenter.

Styrelsen rekommenderas att ta fram en organisation att omhänderta lessons learned. Det är en naturlig del av det förbättringsarbete som en mer mogen verksamhet kan ta nästa steg emot.

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskningar:

- Biträde
- Digitala utbildningar uppföljning

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

Granskning 1 Biträde

Under 2024 har ett biträde utvärderats vid tecknade av nytt avtal. Leverantören levererar tjänst för nyhetsbrev och CRM. Tjänsterna bygger till viss del på tredjelandsöverföring. Vid granskningen har det inte framkommit några avvikelser och dokumentationen leverantören hänvisar till är fyllig och har ett fullgott innehåll.

	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

Granskning 2 Digitala utbildningar uppföljning

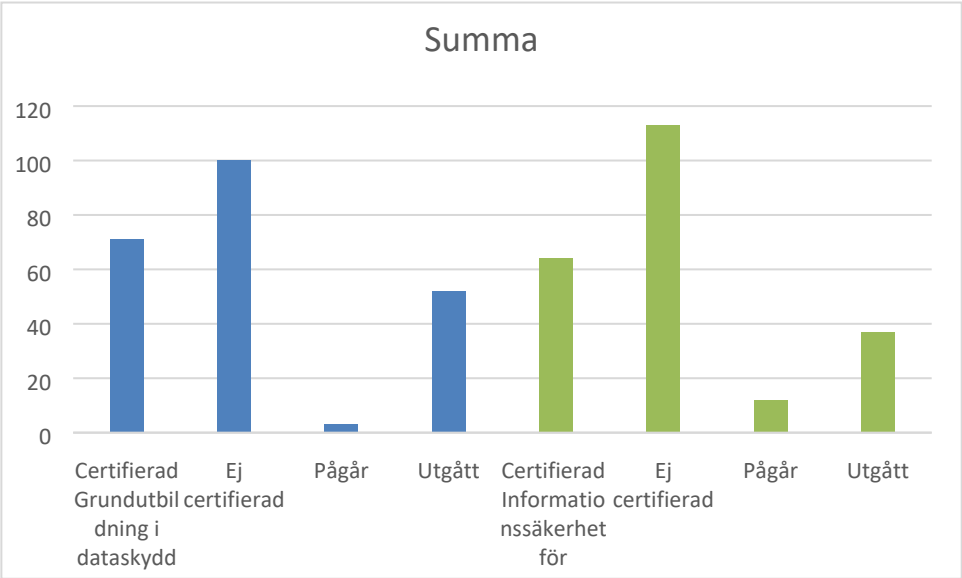
I rapporten från föregående år har jag rapporterat en uppföljning av de digitala utbildningarna i informationssäkerhet och dataskydd. I år har statistik inhämtats för 226 medarbetare (både tillsvidareanställda och konsulter) som ska ha gått de *obligatoriska* utbildningarna.

Vid jämförelse av antalet som genomgått utbildningarna under åren 2022-2024 så är deltagarantalet väldigt lågt. En acceptabel nivå och riktvärde för 2025 borde vara 75 %. Ett minskat antal personuppgiftsincidenter tyder också på att kunskapen börjar gå förlorad i organisationen.

Utbildning	Grundkurs dataskydd	Grundkurs informationssäkerhet
2022	24%	46%
2023	57%	49%
2024	33%*	34%*

*Även inräknat pågår.

Diagrammet visar hur många som certifierats under 2024. Syftet med certifiering är att det automatiskt ska gå ut en påminnelse årligen till medarbetarna från utbildningsplattformen. Utgått betyder att medarbetaren inte gått om kursen enligt plan. Ej certifierad betyder att ingen kurs gått alls.



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

3.4 DSO ger råd och rekommendationer till PUA

För granskningen av biträdet rekommenderas att organisationen följer upp tredjelandsöverföringens giltighet vid eventuella nya förutsättningar efter nya presidentens tillträde i januari 2025. Omvärldsbevakning behöver ske och en ny bedömning tas om överföringsmekanismerna underkänns.

Då fler indikatorer på att kunskapsnivån inom organisationen är låg. Det syns bland annat på frekvensen av incidentanmälningar och personberoendet vid vissa aktiviteter kopplade till dataskydd och

informationssäkerhet. Under 2025 behöver ett krafttag tas att fler går den obligatoriska utbildningen. En acceptabel nivå är 75 %.
Dataskyddsombudets rekommendation är att varje chef tar tid vid ett avdelningsmöte, och avsätter tid, ca 15 min. till att alla genomför utbildningarna.

4 Risker inom dataskydd

4.1 Sammanfattning

Prioriterade risker inom verksamheten:

- Osäker e-posthantering med personuppgifter (Kvarstår)
- Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)
- Tredjelandsöverföringar (Kvarstår)
- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (bolagets) objektförvaltning (Ny)
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Ny)

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.

4.3 Resultatet av riskkartläggningen

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)

4.4 Resultatet av riskkartläggningen

4.4.1 Risk 1 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.

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

4.4.2 Risk 2 Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)

Vid arbete med KLASSA, vilket har varit fokus för bolagen i år, framkommer det att det saknas dokumentation (både gemensam och lokal). Vid förfrågan kan sällan förvaltningsplan, systemdokumentation etc. tas fram av leverantören eller den egna förvaltningen. Denna brist är allvarlig och gemensamma mallar för hur och vad dessa dokument ska innehålla behöver tas fram centralt. Risken är att man idag förutsätter det finns dokumentation för att det ”borde finnas” eller man ”antar” att det är på plats.

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

4.4.3 Risk 3 Tredjelandsöverföringar (Ny)

Vid tidigare årsrapporter har risken med tredjelandsöverföringar lyfts upp. Denna risk uppmärksammas så även i år. Detta beror på att flertalet leverantörer av IT-tjänster numera går över till att endast vara molntjänstbaserade och dessa oftast är kopplade till amerikanska företag. Med den nya presidentens tillträde den 20:e januari finns en farhåga att de nuvarande överföringsmekanismerna ska ryckas upp och att det kan finnas integritetsrisker med att använda dessa tjänster.

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

4.4.4 Risk 4 Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (bolagets) objektförvaltning (Ny)

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.

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

4.4.5 Risk 5 Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Ny)

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? AI är ett oerhört bra och kraftfullt hjälpmedel som vi måste använda medvetet och till rätt saker.

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

4.5 DSO ger råd och rekommendationer till PUA

1. Dataskyddsombudets rekommendation för att minimera risken att personuppgifter e-postas utan tillräckligt skydd, är att de risker som

kommit fram under projektet att införa tjänsten ”Säkra meddelanden” åtgärdas.

2. Genom att ta fram, implementera och kommunicera tillämpningsanvisningarna för informationssäkerhet och dataskydd kommer ansvaret bli tydligare för vem som ska ta fram dokumentationen som i dag saknas.

3. 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. Rutiner för att genomföra TIA, Transfer Impact Assessment, behöver också tas fram.

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

5. 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. Genvägar blir kostsamma både utifrån sanktioner (både GDPR och AI-förordningen kan ge sanktioner var för sig) men också individens rättigheter får aldrig förminskas eller glömmas bort.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Implementation av AI och AI-tjänster
- Kamerabevakning

5.2 Syfte

Som nämnts tidigare 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

5.3.1 Granskning 1 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.

Som en del av granskningen har diskussioner förts med projekt där AI kan vara av intresse att implementera. Tydligt är att en styrelse idag behöver

ha en god insyn i riskarbetet och bestämma vilken riskaptit[1] organisationen ska ha genom styrelsens inriktningsbeslut. Med nya AI förordningen tillkommer också krav på leverantörer av dessa AI-tjänster och att de kan leverera de dokument som krävs för att hamnen ska kunna göra rätt värderingar och analyser.

Ett gott steg i rätt riktning är arbetet med att ta fram egna lokala styrdokument utifrån informations-, dataskydds- och IT-säkerhetsperspektivet. Genom att börja hitta gemensamma vägar att låta informationssäkerheten styra genom krav på designen, kommer också individen att skyddas med rätt typ av säkerhet och projekten bli mer kostnadseffektiva.

5.4 Kamerabevakning

Kamerabevakning är ett område som regleras av dels dataskyddsförordningen, dels den svenska kamerabevakningslagen. Hamnen har flera platser där kamerabevakning används. En granskning kommer genomföras under 2025 för att säkerställa att:

- Granska om den kamerabevakning som idag genomförs omhändertar dataskyddsförordningen när det behövs.
- Granska att rutinerna för kamerabevakning innefattar dataskyddsförordningen.
- Granska att den information som ges på skyltar och webb ger korrekt information om personuppgiftsansvar etc.

[1] Riskaptit- den nivå av risktagande som en organisation anser sig kunna acceptera innan den sätter in motåtgärder.

6 Övrigt att rapportera

6.1 Intern arbetsgrupp informationssäkerhet och dataskydd

I rekommendationen år 2023 angavs behovet av att omstarta gruppen med dataskydd och informationssäkerhetshandläggare. Dessa ska fungera som förlänga öron och ögon inom organisationen till informationssäkerhetssamrodnaren och dataskyddsombudet. Under 2024 har fyra stycken sådana möten hållits efter en nystart Q1 2024. Arbetet har genomgått en diskussion om förbättringar vid det fjärde mötet och det kommer vägas in under 2025-års handläggarmöten. Varje möte har haft ett eget tema utifrån det årshjul som dataskydd och informationssäkerhet arbetar utifrån.