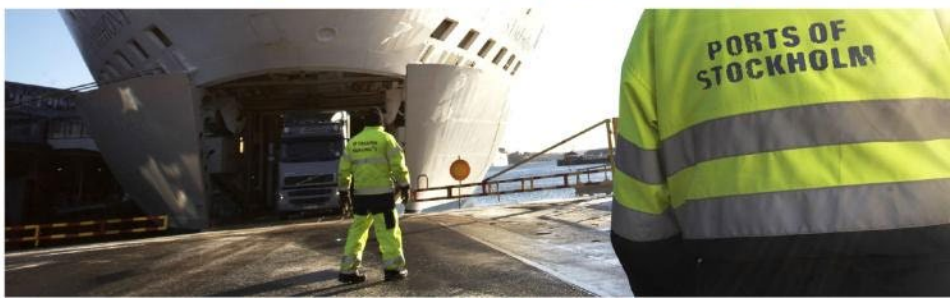
Dataskyddsombudets Årsrapport år 2025 för Stockholms Hamnar

Diarienummer SH 2026/19



Sammanfattning

I egenskap av ert dataskyddsombud lämnar jag följande årsrapport.
Den personuppgiftsansvariga, Hamnarnas styrelser, behöver ha god insikt i dataskyddsarbetet. Ett sätt att hålla sig informerad om risker och trender är den här årsrapporten.

Dataskyddsåret 2025 har varit fyllt av utmaningar men också möjligheter. En av nyheterna är att IMY, Integritetsskyddsmyndigheten, nu vill fokusera mer på vägledning än bestraffning. Det var med stor glädje vi mottog tydlig vägledning i både hur konsekvensbedömningar ska vara utformade och hur arbetet med AI-förordningen ska gå till.
Ett av de förbättringsområden jag vill belysa är utbildning och dataskyddskompetens inom organisationen. Det är ett lågt deltagande i de obligatoriska digitala utbildningarna och det avspeglar sig ibland annat det systematiska dataskyddsarbetet som är mycket personberoende. Jag har valt att i år belysa detta som en ny risk.

En möjlighet som presenterades hösten 2025, är det nya förbättrade digitala verktyget för registerförteckningen. Det nuvarande utseendet har varit svårt att arbeta med för medarbetarna och det positiva är att leverantören lyssnat och gjort det mer användarvänligt. Projektet med att implementera detta sker under första kvartalet 2026.
Ett stort plus ska också ges till dataskyddshandläggarna och ISAM som kommer med bra inputs i dataskyddsarbetet!

En omvärldsbevakning från mig som DSO, är att tillsynsmyndigheten vill lägga mer fokus under 2026 på riskarbete inom dataskydd. Några av de riskområden som jag vill belysa i min årsrapport är:

- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Stockholms Hamnars) objektförvaltning.
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation.
- Tredjelandsöverföringar
- Osäker e-posthantering med personuppgifter
- Lagringsytor utan kontroll
- Deltagande i utbildning

Vi står inför en tid av mycket osäkerheter där vem som är allierad och riskerna inom cybersäkerhet och informationssäkerhet förändras fort. Min uppgift som DSO är att se till att de registredes skyddas på ett adekvat och tryggt sätt. Med det hoppas jag at vi får ett lagom spännande dataskyddsår 2026.

Jessica Hillergård
Dataskyddsombud

Innehåll

1 Inledning

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

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

1.1. Beskrivning och förklaring av granskningsmetod och resultat

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete utifrån sex obligatoriska områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten, IMY, utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del som kräver åtgärder.

Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.

1.2. 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
- Tekniska och organisatoriska säkerhetsåtgärder i samband med personuppgifts behandling[1]
- Konsekvensbedömningar
- Överföring till tredje land
- Individens rättigheter

[1] I tidigare årsrapporter är denna punkt uppdelat i rubrikerna ”tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar” och ”styrdokument”

- Personuppgiftsincidenter

Utöver dessa obligatoriska områden rapporteras även om de fördjupade granskningar som skett under föregående år samt planerade granskningsaktiviteter för år 2026. Ett specifikt kapitel om risker och omvärldsbevakning är också prioriterat i rapporten för att underlätta beslut angående dataskyddsarbetet framåt för personuppgiftsansvarig.

2 Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

2.1 Registerförteckning

2.1.1 Syftet med området

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgiftsbehandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att beskriva om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

2.1.2 Resultat

I årsrapporten från 2024 rekommenderades verksamheten, att påbörja kartläggningen av processägare och processer och det har skett under 2025, främst med fokus mot NIS2 och andra nya EU-direktiv. Registreringarna i registerförteckningen utgår från Stadens gemensamma hanteringsanvisning och dess processer men det kan finnas andra inom Stockholm Hamnar som ännu inte identifierats i och med att processkartläggningen är pågående vid rapportens framtagande.

Enligt årshjulet ska registerförteckningen uppdateras mellan möte 2 och 3 för dataskyddshandläggarna. Förteckningen finns idag i ett digitalt verktyg kallat DraftIT. Vid 2025-års uppdatering inkom flera felrapporter om verktyget. Det gick inte att sända in för granskning och slutföra registreringar. Felanmälan gjordes och förklaringen var att en ny version av DraftIT var under framtagande.

I kvartal 3 år 2025 släpptes den nya versionen av plattformen DraftIT. Stockholm Hamnar har bestämt att under 2026 gå över till den nya plattformen då denna kommer bättre svara mot behovet organisationen har och kommer lösa delar med behörighetsproblematiken som finns i dagens verktyg.

2.1.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		*105*
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		*Verksamheten har rutiner och utpekat ansvar att uppdatera.*
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		*Registerförteckningen saknar uppdateringar på en del områden. Uppdateringar sker efter aktiviteter i årshjulet.* *Det är bra att hänvisning till hanteringsanvisningen finns kopplat till varje personuppgiftsbehandling.*
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		*Registerförteckningar har identifierat de personuppgiftsbehandlingar som finns i organisationen och kopplat dem till hanteringsanvisningen. Dock behöver vissa informationsluckor täppas till. Det kommer med sannolikhet lättare kunna göras i den nya plattformen som är mer användarvänliga och det går att fokusera bättre på obligatoriska frågor.*

2.1.4 DSO ger råd och rekommendationer till PUA

Under år 2026 rekommenderas organisationen att fortsätta arbetet med övergången till den nya förbättrade digitala plattformen och att implementera de uppdateringar som uppmärksammats i samband med kontinuitetsarbetet och inventeringen i hanteringsanvisningen.

Organisationen rekommenderas också att ge de ansvariga (ex. systemägare) en enklare utbildning och information om verktyget för att ett än mer systematiskt arbete ska kunna ske med registerförteckningen.

2.2 Tekniska och organisatoriska åtgärder

2.2.1 Syftet med området

Personuppgiftsansvarig ska tillse att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna, att uppgifterna förloras eller förstörs.
Personuppgiftsansvarig behöver alltid bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, behörighetsbegränsning, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda all information inom verksamheten och ha rätt nivå på skyddsåtgärder, ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA . Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare.

Genom att använda arbetssättet i metodhandboken värderas informationen utifrån konfidentialitet, riktighet och tillgänglighet. Verktyget KLASSA hjälper sedan till att ta fram tekniska och organisatoriska krav att ställa internt och mot leverantörer. Detta innefattar även bedömning och värdering av personuppgifter.
Genom att genomför riskanalyser identifierar informationsägaren risker och väljer åtgärder för att hantera riskerna.

Den personuppgiftsansvariga måste kunna visa hur GDPR efterlevs och att det finns styrdokument och rutiner är en viktig del i detta. Det görs genom att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner så att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd.

Syftet med detta rapporteringsområde är att redogöra för huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser samt att rätt bedömningen för både tekniska och organisatoriska åtgärder är gjorda. Vidare bedömer DSO också huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

2.2.2 Resultat

Verksamheten har gjort de förbättringar som föreslogs i årsrapporten för år 2024 vad gällande länkar etc. på externwebben.

Under år 2025 har förklassningar och klassningar skett i verksamheten och de har sedan stämts av med DSO varannan vecka. Det finns fortfarande ett starkt personberoende att

informationsklassningar sker inom organisationen. När det sker involveras dock DSO på ett bra sätt. Engagemanget att det ska bli rätt tekniska åtgärder finns, och en plan för nya organisatoriska åtgärder inom cybersäkerhetsområdet har prioriterats av ledningen.

Utmaningen framöver kommer vara att fånga upp de AI:n som plötsligt implementeras i IT-tjänster och som skapar nya oväntade personuppgiftsbehandlingar. Det saknas AI-riktlinje och strategi inom Stockholm stad vilket gör det svårt för bolaget att agera och ta höjd för egen AI-användning.

2.2.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		*Verksamheten kan informationsklassa. Dock är det personberoende av nyckelmedarbetare är delaktiga. Men efter förutsättningarna fungerar det bra och fungerande rutin finns för momenten. Minskar nyckelpersonberoendet kommer arbetet bli mer systematiskt och effektivt. Då blir också personuppgifterna bättre klassade.*
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		*Styrande dokument är bra och pedagogiska, men behöver en mindre uppdatering. Bland annat saknas hur AI:n ska behandlas.*
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		*De dokument som finns ligger publicerade delvis på intranätet men också i mappstrukturen. När ändringar görs flaggas det upp som en nyhet om den som ändrar uppmärksammar det.*

2.2.4 DSO ger råd och rekommendationer till PUA

Under 2026 behöver styrande dokument ses över och därefter kommuniceras i till ansvariga i verksamheten så att beroendet av nyckelpersoner minskar för att åtgärder vidtas. Ett förslag är att förtydliga ansvaret och processerna samt uppmärksamma vilka aktiviteter som ska genomföras årligen för de medarbetare som har ansvaret. Med en

tydlig förvaltningsmodell likt PM3 är det också lättare att följa upp att rätt och adekvata skyddsåtgärder är införda och följs upp. Med en förvaltning finns också rutiner med ansvar att systematiskt se över och implementera styrande dokument.

2.3 Konsekvensbedömning avseende dataskydd

2.3.1 Syftet med området

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en s.k. tröskelanalys.
En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utfös för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.
Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas samt korrekta och relevanta skyddsåtgärder identifieras i kravställning på leverantörerna.
Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

2.3.2 Resultat

Under det gånga året har IMY, Integritetsskyddsmyndigheten levererat mer vägledningar än bestraffningar. Det har bland annat syns genom ett mycket bra material innehållande vägledning och mallar för konsekvensbedömningar. Stockholms Hamnar har anpassat sina mallar efter detta.

Ett av de området som fortfarande brister är de stadsgemensamma konsekvensbedömningarna som saknar process. I dagsläget är de dokument som tas fram alldeles för generellt hållna och har inte haft med verksamhetsrepresentanter eller dataskyddsombud. Det leder till att det blir merarbete lokalt och många frågetecken att försöka reda ut. Det förekommer också händelser där personuppgiftsansvarig tvingas använda en tjänst utan att den är färdigdokumenterad.

2.3.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade		*Det finns ett förklassningsprotokoll där bland annat frågan om personuppgifter lyfts och det ska bifogas en bilaga (ny*

personuppgiftsbehandlingar genomföra tröskelanalys?		*2025) som heter tröskelanalys. Bilagan behöver implementeras under 2026.*
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		*En diskussion har tidigare genomförts och dokumentation i handlingsplan och förklassningsprotokoll om frågan om fullständig konsekvensbedömning ska göras. Dokumentationen i det nya protokollet som omnämns ovan behöver implementeras under 2026.*
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		*Lokal nivå- JA*
		Stadsgemensamma konsekvensbedömningar genomförs ad hoc och efter att det är nyckelpersoner som tar initiativ. Det behöver bli tydligare process och rollfördelning för att detta ska bli mer effektivt.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		*Lokal nivå- JA*
		Centrala system delvis
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		*Lokal nivå JA*
		Det finns brister som påtalats av lokala medarbetare till centrala funktioner.

2.3.4 DSO ger råd och rekommendationer till PUA

Det är en kvarstående rekommendation att det tas fram en central process för metod och roller i stadsgemensamma konsekvensbedömningar så att de kan användas mer effektivt lokalt. Den nya bilagan för tröskelanalys behöver implementeras under 2026.

2.4 Den registrerades rättigheter

2.4.1 Syftet med området

Den registrerade har ett antal rättigheter enligt GDPR. Den registrerade kan bland annat begära tillgång (registerutdrag), rättelse eller radering. Den som är personuppgiftsansvarig har att tillmötesgå en begäran enligt de krav som finns i dataskyddsförordningen. (För registerutdrag säger GDPR 30 dagar och för övriga begäran skyndsamt.)
Syftet med detta rapporteringsområde är att kontrollera huruvida det finns ändamålsenliga mallar samt rutiner för besvarande av rättighetsbegäran, huruvida inkomna begäranden har hanterats inom den tidsram som finns att förhålla sig till samt huruvida svaren till de registrerade, baserat på ett antal stickprov, uppfyller lagkraven.

2.4.2 Resultat

Informationen till den registrerade har setts över detta år med. Det har framkommit några förbättringar vid granskningen av cookies vilket framkommer i eget kapitel 3.2.

2.4.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		*Det finns interna instruktioner men är inte publicerade på intranätet.*
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		*Antalet har inte diarieförts då de raderas så fort begäran inkommit och färdigställts. Endast nekande begäran diarieföres enligt hanteringsanvisningen.*
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		*Avvikelser har inte identifierats.*
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		*Ja*

2.4.4 DSO ger råd och rekommendationer till PUA

Arbetet med att omhänderta registrerades begäran om rättigheter är bra och fungerar. Rådet är att se över rutinerna och följa omvärldsbevakningen i eventuella förändringar som kan ske med nya råd från tillsynsmyndigheten. Främst gäller det så kallade cookie-banners vilket EU-kommunionen ser över reglerna för 2026.

2.5 Personuppgiftsincidenter

2.5.1 Syftet med området

Med begreppet personuppgiftsincident avses 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.
Om en inträffad personuppgiftsincident medför en risk/ konsekvens för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskyddsmyndigheten, IMY, inom 72 timmar från att den upptäckts. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste individen informeras utan onödigt dröjsmål.
Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras. Det görs i verktyget IA.
Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

2.5.2 Resultat

Det finns rutiner för hur personuppgiftsincidenter ska hanteras och utredas. Det fungerar bra lokalt, men kan bli svåra att hantera när incidenterna är stadsgemensamma. Främst är kommunikationsvägarna inte alltid tydliga och information kommer sent fram till DSO som får kunskap ofta flera steg från källan. Med det menar jag att en incident upptäcks eller förmedlas från central IT-förvaltning/ IT-leverantör, som i sin tur kontaktar sin kontakt på central förvaltning vid ex. SLK, Stadsledningskontoret. Därefter kontaktar de olika personer i verksamheten vid varje separat tillfälle, likt direktören, HR-chef, ISAM, IT-ansvarig osv. som i sin tur informerar ISAM och/eller DSO. (Ibland informeras ISAM först och därefter DSO vilket lägger till ett steg.) Då det är olika medarbetare som har olika intresseområden som får budskapet, riskerar informationen att bli förändrad av misstag och det blir svårt att ge korrekt råd som dataskyddsombud när delar av pusslet saknas.

2.5.2.1 M365

Under våren 2025 uppdagades det att det fanns M365-liceser och Teamschattar kvar även då det tidigare beslutats att inte gå vidare med pilotprojektet. Det åtgärdades och analysen visade inte på att det fanns känsliga personuppgifter som kan hamnat i obehöriga händer. Lessons learned från detta som IT, ISAM och DSO drog är att det behövs en förvaltning likt PM3 och en bättre livscykelhantering.

Andra incidenter som uppdagats är till följd av att konsulter inte får utbildning i vad Stockholm Hamnars personuppgifts- och informationssäkerhets riktlinje är. Det Hamnarna kan drabbas av då är att information och personuppgifter kan hanteras med tillräckligt skydd.

2.5.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		*Samtliga medarbetare genomgår en digital dataskyddsutbildning varje år. Dataskyddshandläggarna påminns på varje kvartalsträff där ämnet är en stående informations- och diskussionspunkt. Se också granskning 3.3.1*
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		*Lokalt följs de rutiner som finns.*
		*När incidenter sker med personuppgifter i **centrala system** är inte kommunikationsvägarna tydliga och det blir en del förvirring. Det tar lång tid innan DSO och ISAM får information vilket försvårar arbetet. Lessons learned kommuniceras inte från centrala funktioner med DSO:er utan oftast endast med ISAM eller andra medarbetare. Därav blir det svårt att bedöma hur hela staden och också i slutändan verksamheten i stort drar lärdom av incidenter och förbättras.*
Hur många personuppgiftsincidenter har dokumenterats under året?		*5*
Hur många personuppgiftsincidenter har anmälts till IMY under året?		*0*

2.5.4 DSO ger råd och rekommendationer till PUA

Under 2026 rekommenderas personuppgiftsansvarig att öva en incident likt den med Miljödata. Det är inte en fråga om, utan när organisationer utsätts för sådana attacker i dagens läge.

Som dataskyddsombud rekommenderar jag också att alla konsulter informeras om Hamnarnas styrdokument om informationssäkerhet och dataskydd. Se också kapitlet granskning 3.3.1.

2.6 Överföring till tredje land

2.6.1 Syftet med området

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs, får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.
Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelandsöverföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

2.6.2 Resultat

I tidigare rapporter har tredjelandsöverföringar angetts som en risk. Nytt för 2025 årsrapport är att detta är ett separat kapitel.

Stockholms Hamnar har en god insyn i vad tredjelandsöverföringar innebär och det är ett område som ofta diskuteras. Tredjelandsöverföringar är problematiska om de inte analyseras korrekt och att rätt avtal finns för underbiträden som leverantörer använder sig utav. Tredjelandsöverföringar är fortsatt omnämnt som en risk av den anledningen. Hamnarna använder sig av tredjelandsöverföringar, men omhändertas korrekt under 2025 genom analys och medvetenhet.

2.6.3 Sammanfattning

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		*De tredjelandsöverföringar som finns är identifierade i verksamheten.*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		*När tredjelandsöverföringar har varit aktuella finns det omnämnt hur de omhändertagits i personuppgiftsbiträdesavtalets instruktion.*

Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		*När tredjelandsöverföring är aktuell efterfrågas TIA av leverantören/ personuppgiftsbiträdet. Denna bedöms sedan av ISAM och DSO som ger rekommendation om fortsatt progress eller inte med leverantören.*

2.6.4 DSO ger råd och rekommendationer till PUA

Sannolikheten att tredjelandsöverföringar kommer öka, är stor i och med att flera IT-leverantörer flyttar sina tjänster från on-prem (egna servrar) till molntjänster. Under 2026 rekommenderas organisationen att arbeta aktivt med att informera utvalda medarbetare om tredjelandsöverföringar. Det finns också ett behov av att bestämma vilken riskaptit verksamheten har för tredjelandsöverföringar exempelvis genom en molnstrategi.
Det är en utmaning att upphandla tjänster och förvirring finns hos leverantörerna om vad som gäller. Därför är det viktigt att verksamheten fortsätter vara en bra kravställare och kan fånga upp otydligheter med rätt frågeställningar till leverantörer

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskningar:

- Granskning 1 Utbildning i dataskydd och informationssäkerhet
- Granskning 2 Information till den registrerade med fokus på externwebben

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 1 utbildning i dataskydd och informationssäkerhet

En av de brister som identifierats i årsrapporten från 2022-2024 och så även i årets, är behovet av nyckelpersoner för att aktiviteter ska ske med informationssäkerhet och dataskydd. I rapporten från 2024 framkommer att endast 33% av medarbetarna har genomgått den *obligatoriska årliga* utbildningen i dataskydd. För att dataskyddsarbetet ska bli mer systematiskt och mindre personberoende borde nivån vara 80% deltagande. Nyckelvärdet 80% är ett bra riktmärke då ex. föräldralediga och långtidsfrånvarande räknas bort.

2025 har siffran ökat till ca. 42% deltagande. (Då har siffror räknats med för både medarbetare som avslutat utbildningen och som registreras som pågående.)

Utbildning 2025	Anställda	Konsulter
Dataskydd	59%	21%
Informationssäkerhet	66%	19%

I siffran genomgått utbildning räknas även de som är i kategorin pågående.

Utbildning	Grundkurs dataskydd (anställda och konsulter)	Grundkurs informationssäkerhet (anställda och konsulter)
2022	24%	46%
2023	57%	49%
2024	33%	34%
2025	42%	45%

3.3.2 *Granskning 2 Information till den registrerade med fokus på externwebben*

Ett av de områden som visat sig vara mest komplicerade att få kontroll över som personuppgiftsansvarig är informationen till den registrerade och då främst med fokus på cookies och andra typer av digitala spårare på publika hemsidor. Detta är en trend som man kan se hos många personuppgiftsansvariga i hela Sverige och inte endast hos Stockholms Hamnar.

Stockholms Hamnar har bra information till de registrerade genom policys och transparens på sin hemsida. Dock visar granskningen på några mindre förbättringsområden. Detaljerade brister och åtgärder är tidigare presenterat i egen föredragning internt.

3.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation inför 2026 är att prioritera att *minst 80% medarbetare och konsulter* genomför utbildningarna i dataskydd och informationssäkerhet. Kunskap är färskvara och det finns tydliga signaler att det är ett stort förbättringsområde och som gör att organisationen inte är så stark inom området. Det är en risk att så få konsulter som deltar i utbildningen och får kännedom om hur personuppgiftsansvarig förväntar sig att de ska använda och skydda informationen.

I informationen till de registrerade och då främst digitala spårare rekommenderas Stockholms Hamnar att omvärldsbevaka PTS (Post och Telestyrelsen) vägledningar om digitala spårare. Förändringar på området spås komma med den nya uppdaterade dataskyddsförordningen som bearbetas på EU kommissionen och ländernas tillsynsmyndigheter.

4 Risker inom dataskydd

4.1 Sammanfattning

Prioriterade risker inom verksamheten:

- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Stockholms Hamnars) objektförvaltning. (Kvarstår)
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation. (Kvarstår)
- Tredjelandsöverföringar (Kvarstår)
- Osäker e-posthantering med personuppgifter (Kvarstår)
- Lagringsytor utan kontroll (Ny)
- Lågt deltagande i utbildningar (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.

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 (Hamnarnas) 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. Under hösten 2025 har förbättringar skett men som i rapportens framtagande inte har hunnit med att implementeras. Risken fortsätter därmed att bevakas.

	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 startade efterfrågan på AI och möjligheten att effektivisera arbetet. År 2025 har det blivit än mer vardag och efterfrågan ökar konstant. 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.

AI-förordningen har också tillkommit under 2025 vilket ställer högre krav på den som upphandlar tjänster att ha kontroll på sina informationsflöden. Dock kvarstår risken som hög då endast administrativa åtgärder täcker de åtgärder som behövs.

X	Hög > 15 (riskerna skall elimineras)
	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. 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.

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

4.3.4 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.

Rekommendationen kvarstår att inte använda tjänsten utan att analysmaterialet finns färdigt. Riskerna har inte besvarats av central förvaltning, ny tillsattes november 2025, 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)

4.3.5 Lagringsytor utan kontroll

I den nya plattformen Nordic for Zoom (ersätter ZoomX) kommer det finnas möjlighet att dela dokument och skapa egna grupper fritt för samarbete både inom den egna organisationen och med andra. En bra möjlighet, men i en gemensam mapp eller i en samarbetsyta på Sharepoint kan administratörer med särskild behörighet följa upp och gallra information som inte längre är relevant. I Nordic for Zoom finns inte denna administrativa kontroll vilket gör att kraven i dataskyddsförordningen om transparens (registerutdrag) och lagringsminimering inte kan efterlevas.

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

4.3.6 Brist på kunskap/ deltagande i utbildning (organisatorisk åtgärd)

Som tidigare nämnts i granskningen kap 3.3.1 är kunskapsbrist en risk som jag som dataskyddsombud vill lyfta.

	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 Stockholms Hamnars 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 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.
- Under arbetet med införande av Nordic for Zoom behöver risken omhändertas. En rekommendation är att minst skapa en organisatorisk åtgärd med rutiner och förbud, om det inte går att tekniskt stänga av filöverföring, begränsa lagringstiden eller på annat sätt kontrollera ytorna.
- Rekommendationen är densamma som i kapitel 3.4. Deltagandet i de obligatoriska utbildningarna behöver komma upp i minst 80% för att det ska ge en effekt som organisatorisk åtgärd.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granskning 1* Utbildningar i dataskydd
- *Granskning 2* AI (Styrdokument och metod för infoklassning och anpassning mot AI-förordningen och GDPR)

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

Granskning 1 Utbildning i dataskydd

Under 2026 kommer jag att granska att åtgärder för att möta acceptabelt riktvärde på deltagande sker.

Granskning 2 AI (Styrdokument och metod för infoklassning och anpassning mot AI-förordningen och GDPR)

Den nya tekniken är här för att stanna och det saknas styrande dokument för hur området ska omhändertas. Under 2026 kommer jag som DSO att följa upp kvalitet på styrande dokument, hur väl de efterlevs och hur användarvänliga de är.

6 Omvärldsbevakning

6.1 Tillsynsmyndigheten omorganiseras

Den 1:a januari 2026 omorganiserades Integritetskyddsmyndighetens, IMY:s, operativa del. Det har nu inrättats en avdelning för tillsyn och klagomål och en för vägledning, innovation och teknik. Syftet är att:

- stärka myndighetens förmåga att genomföra riskbaserad tillsyn,
- stärka myndighetens förmåga att ge tydlig och effektiv vägledning samt
- effektivisera myndighetens hantering av klagomål

Sannolikt kommer det här leda till fler tillsyner baserade på klagomål och som pressmeddelandet säger, genomföra riskbaserade granskningar av organisationer. Det innebär att organisationen behöver ha god kontroll över sina dataskyddsrisker och arbeta aktivt med dem.

6.2 Kommande förändringar av Dataskyddsförordningen

Ett förslag har lämnats från Europakommissionen i november på förändringar i dataskyddslagstiftningarna inom EU. Förslaget syftar främst till att öka möjligheten för innovation och minska administrativa krav på mindre verksamheter. Förslaget var helt annorlunda än det som levererades som första utkast sex månader tidigare då fokus var att minska kravet på registerförteckning.
Analysen jag som DSO gör är, att områdets fokusområden svänger fort men tydligt är att en organisation fortsatt behöver vara en tydlig beställare till leverantörer av IT-tjänster och ha kontroll på sina legala- och informationssäkerhetskrav. Behovet av att göra riskanalyser och tänka till före och ta medvetna risker är en viktig fortsatt nyckelaktivitet inom dataskyddsarbetet.

6.3 Tillsyn av Miljödata incidenten

Under hösten 2025 skedde en större personuppgiftsincident hos leverantören Miljödata. Den berörde även delar av Stockholm stad då Stadsledningskontorets HR-avdelning hade beslutat att använda plattformen leverantören erbjöd. Stadsdelsförvaltningens medarbetare och tidigare anställda från och med januari 2024 har i och med läckan hamnat på Darknet. Med anledning av IT-angreppet och den efterföljande läckan av personuppgifter har Integritetsskyddsmyndigheten, IMY, beslutat att inleda granskningar mot Miljödata samt två kommuner och en region som har använt företagets tjänster. (Göteborgs stad, Älmhults kommun och Region Västmanland)
Urvalet av de granskade aktörerna har gjorts baserat på typ av verksamhet som bedrivs och indikationer på risker då det var många aktörer berörda. Det finns i nuläget inga planer på ytterligare granskningar från IMY men det är heller inte uteslutet att det kommer att ske. Granskningarna kommer bli vägledande i hur en organisation måste agera innan en personuppgiftsbehandling sker.

6.4 Övrigt

IMY har mer fokus på vägledning än bestraffning sedan ett år tillbaka. Det innebär att en organisation kan söka delaktighet i regulatoriska sandlådor där man testar sig fram till ex. ett nytt AI skulle kunna användas.

Under år 2025 lättades kamerabevakningslagen upp. Ett område som troligen kommer att granskas under 2026 av tillsynsmyndigheten är nog att efterlevnaden av lagen, dokumentationskrav och bedömningar.

7 Övrigt att rapportera

7.1 Interna arbetsgruppen

Den interna arbetsgruppen för GDPR och informationssäkerhet med representanter från verksamheterna har fortsatt arbeta under året som gått. Sammankallande är ISAM och som också håller protokoll och att aktiviteter utförs enligt plan och årshjul.

7.2 Samarbete och kommunikation i dataskydd i staden

Stadsdelsförvaltningarnas DSO:er har ett informellt nätverk kallat ”GUG, GDPR Utan Gränser”. Nätverkets syfte är att användas som bollplank och säkerställa att alla DSO:er inte ska gå på samma frågor som andra DSO:er redan arbetar med och minska belastningen på rådgivande verksamheter likt SLK juridiska avdelning. Nätverket är välfungerande och har även med DSO:er från fackförvaltningar och bolag samt arkivarie och ISAM. Det finns inget formellt nätverk för DSO:er sedan 2020 i Stockholm stad, därför är det här samarbetet än viktigare att vårda. I det nätverket deltar jag som DSO och representerar Stockholms Hamnar.