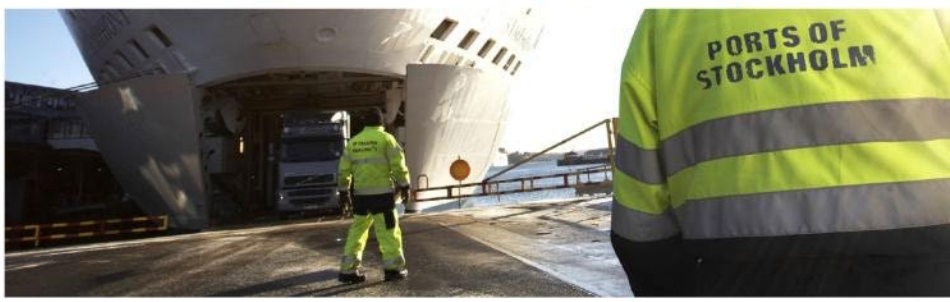
Dataskyddsombudets Årsrapport år 2021 för Stockholms Hamnar



Sammanfattning

I egenskap av ert dataskyddsombud lämnar jag följande årsrapport.
Stockholm Hamnar har under år 2021 genomgått en hel del förändringar inom området säkerhet och informationssäkerhet. Med detta har också området som inkluderar dataskydd fått en nystart. En tydlig förändring är att flera arbetsgrupper startats där även nu dataskyddsombudet och informationssäkerhetssamordnaren deltar som rådgivande funktioner. Området har synliggjorts och är en positiv utveckling. En intern arbetsgrupp för dataskyddsfrågan har införts under året.

Stockholm Hamnar har under året haft fyra personuppgiftsincidenter. Detta är en positiv utveckling från att det aldrig rapporterats tidigare år. Detta indikerar att kunskapen om dataskyddsförordningen börjat spridas och viljan att prata om brister har ökat. När en personuppgiftsincident har skett finns också en tydlig vilja att hitta åtgärder och agera på händelsen. Under år 2022 behöver vi fortsätta den här utvecklingen och sprida kunskaperna ytterligare lite till.

Under det gångna året har ett nätverk byggts upp av dataskyddsombud i de tekniska förvaltningarna/bolagen. Detta har resulterat i att gemensamma problem har kunnat lösas enklare och kunskaper överföras på ett naturligare sätt.

Året har fortfarande påverkats av pandemin med rekommendationer av hemarbete och digitala möten. En gemensam arbetsgrupp där bland annat Stockholms Hamnar deltagit, har arbetat med att kunna gå över till M365 Teams i staden. Beslut har fattats av SLK att inte gå in i Teams efter samråd med IMY, Integritetsskyddsmyndigheten. Beslutet är baserat på att säkerheten inte är tillräckligt tillfredsställande. Detta har också lett till att Hamnarens egna M365 projekt avslutas.

Revisionskontoret har haft i uppdrag att revidera bolagens följsamhet gentemot dataskyddsförordningen. Revisionen lyfter fram främst problemet med en allt för operativt dataskyddsombud då denna ska ha en ren granskande roll. Detta är en fråga som jag tar med mig in i 2022, men som är problematisk då lagstiftningen fortfarande är ung och personalen behöver stöd.

Organisationen har en utmaning att vara både framåtblickande och teknikdrivna, samtidigt som styrdokument är omoderna. I dagsläget är ett av det absolut viktigaste styrdokumentet, Stockholm stads IT-säkerhets- och informationssäkerhetsriktlinjen för området från 2014. Förhoppningen är dock att den nya riktlinjen som varit på remiss, antas av Kommunfullmäktige i januari 2022.

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?	76
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nej

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 finns i dag dokumenterad i DraftIt Records. Registerförteckningen består av 76 st. aktiva och 13 st. inaktiva registreringar. Det betyder att efter uppdatering har 13 st. av de tidigare personuppgiftsbehandlingarna arkiverats då de inte längre utförs inom organisationen. De aktiva registreringarna är riskbedömda och har antingen godkänts av DSO efter granskning, alternativt att det begärts någon form av komplettering ska genomföras. I registerförteckningen dokumenteras vilka system som finns kopplade till respektive personuppgiftsbehandling, vilka som är biträden, mottagare osv.

Det finns i dagsläget ingen fast struktur och nedtecknad rutin för hur uppdateringar och registerförteckningen ska hanteras systematiskt. I dag sker arbete ad hoc och är i beroende av individens initiativ och kunskap.

På begäran kan den befintliga registerförteckningen tas fram och distribueras till tillsynsmyndigheten IMY, Integritetsskyddsmyndigheten.

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

Om registret över behandlingar hanteras som en naturlig del i det löpande dataskyddsarbetet går det smidigare att se över registret och uppdatera när det sker förändringar eller tillkommer nya behandlingar, utan att det växer till ett onödigt stort arbete och upplevs som ett nödvändigt ont.

Det behöver skapas en rutin som implementeras och kommuniceras till personalen.

Det behöver frigöras tid och resurs för att registerförteckningen ska uppdateras.

2.2 Styrdokument

2.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	NEJ
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?	Till viss del

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

Bristerna som är identifierade är avsaknaden av uppdaterad informations- och it-säkerhetsriktlinje. Den befintliga är från 2014. En ny riktlinje har tagits fram och ska förhoppningsvis antas av Kommunalfullmäktige i januari 2022.

Organisationen har tagit fram rutiner för personuppgiftsincidenter, registerutdrag etc. och innefattar sådant de själva kan styra över.

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
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

Den stora bristen består i den förlegade informationssäkerhets- och itsäkerhetsriktlinjen som är från 2014.

2.2.5 DSO ger råd och rekommendationer till PUA

I artikel 24 GDPR finns en allmän regel om att de personuppgiftsansvariga ska kunna visa att lämpliga tekniska och organisatoriska åtgärder genomförts för att säkerställa att personuppgiftsbehandlingen utförs i enlighet med säkerhetskraven (ansvarsskyldighet). Ett sätt att visa detta är genom en informationssäkerhetspolicy som sätter upp ramar för arbetet med säkerhet, och som alla anställda känner till.

Det är viktigt att organisationens IT-utrustning inte används för otillbörliga ändamål, så som nedladdning av upphovsrättsskyddade verk, surfande på olämpliga hemsidor och så vidare. Arbetsgivaren ska kunna kontrollera, övervaka och följa upp hur datorerna används, men för att kunna göra det kräver Integritetsskyddsmyndigheten att det finns tydliga och väl kända regler dels om vad som är tillåtet/otillåtet när de anställda använder

IT-utrustningen, dels om hur arbetsgivaren kommer att kontrollera efterlevnaden av dessa regler, till exempel genom stickprovskontroller. I en IT-policy kan man inkludera exempelvis riktlinjer för anställdas internetanvändning.

När informationssäkerhets och itsäkerhetsriktlinjen är antagen av KF, Kommunalfullmäktige, behöver denna anpassas mot organisationens egna förutsättningar.

En granskning av befintliga rutiner behöver ske under 2022.

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?	I verktyget KLASSA 33 I DraftIT 76
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

Det finns 33 registreringar i verktyget KLASSA. Det som KLASSAS är system där det *kan* förekomma personuppgiftsbehandlingar. En personuppgiftsbehandling kan också innefatta flera system än ett.

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.

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

Behovet av tekniska och organisatoriska säkerhetsåtgärder ska bedömas bland annat utifrån uppgifternas känslighetsgrad och de hot, den sårbarhet och de risker som kan uppkomma i samband med behandlingen. Om det sker förändringar så kan det finnas skäl att se över befintliga säkerhetsåtgärder och kanske omvärdera och förändra.

Inbyggt dataskydd och dataskydd som standard enligt artikel 25 i GDPR ska genomsyra hela utvecklingsprocessen och varje IT-systems hela livscykel, överallt där personuppgifter förekommer. Hur pass komplext arbetet i praktiken blir med att

implementera detta beror helt på sammanhanget och behandlingarna. Det finns alltså ingen universallösning, utan inbyggt dataskydd och dataskydd som standard är något som varje organisation måste förhålla sig till på en principiell, strategisk nivå och sedan arbeta med utifrån de egna förutsättningarna. Med en klar och tydlig struktur och väl anpassade rutiner i säkerhetsarbetet uppnår ni förutsägbarhet. Om ni har tydliga, interna rutiner eller följer en standard minskar ni riskerna för att ni missar något viktig eller att ni gör misstag som kan leda till kostsamma säkerhetsincidenter.

Dataskyddsombudets råd är att fortsätta arbetet med informationssäkerhetsklassning i både DraftIt och KLASSA.

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 aktivt och sker i samverkan mellan flera nyckelroller. Rutiner finns på plats, men behöver kommuniceras till personalen då aktiviteten idag sker individberoende, d.v.s. individer har kunskapen men inte bredden vilket kan försvåra processen.

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
	Inga brister av nämnvärd betydelse identifierade

2.4.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets råd är att 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.

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

Under nästkommande år, 2022, behöver rutinerna ses över att de fortfarande är aktuella och fungerar.

2.6 Personuppgiftsincidenter

2.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom att egen personal uppmärksammar incidenter
Hur många personuppgiftsincidenter har dokumenterats?	3
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

Organisationen har under året blivit mer uppmärksamma på personuppgiftsincidenter. Värt att notera är att Hamnaren hade ingen personuppgiftsincident alls innan 2021. Det ansågs i rapporten 2020 att detta var en allvarlig brist. Med utbildning och kunskapsspridning har således en del av organisationen börjat se incidenter och förstår bättre vinsten av att lyfta dem som en del av ett förbättringsarbete. Efter personuppgiftsincidenterna har personalen direkt engagerat sig och försökt att se åtgärder.

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

Dataskyddsombudet har under årets andra halva engagerats mer i operativa möten där olika frågor diskuteras. Detta i syfte att utbilda nyckelfunktioner och fånga upp behov samt ge råd. Detta är en väg framåt i kunskapsspridningen och indikerar att öppet diskussionsklimat leder till fler rapporter om personuppgiftsincidenter.

Rekommendationen är att fortsätta arbetet med kunskapsspridning.

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskningar:

- *”GDPR-Information” till den anställde*

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 ”GDPR-Information” till den anställde

När dataskyddsombudet deltagit vid klassningar i verktyget KLASSA under 2021 har detta varit ett område som kommit upp som en varningsflagga. Det har funnits oklarhet om det finns information till den registrerade anställda och vad som meddelas och när.

Stockholm Hamnar har påbörjat en granskning av detta område och har identifierat uppdateringsbehov under hösten 2021.

	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

3.4 DSO ger råd och rekommendationer till PUA

Stockholm Hamnar har påbörjat en genomgång av detta område under hösten 2021 och rådet är att fortsätta detta arbete under 2022. Hamnaren har ett dokument för den nyanställde hur personuppgifter behandlas och till vad. Vid nyanställning alternativt inhyrning av konsult, ska personalen gå utbildningen ”Säker i Hamnar” som bland annat

innefattar informationssäkerhet. Till denna borde också GDPR-utbildningen på Stockholm stads utbildningsplattform läggas till.

Önskvärt är också att både Säker i Hamnar och GDPR-utbildning har genomgåtts innan tjänstekort och behörigheter lämnas. Detta behöver kontrolleras att det är genomfört och att identiteten kontrollerad och dokumenterad.

4 Risker inom dataskydd

4.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Brist på kunskap om dataskyddsförordningen*
- *Inbyggt dataskydd och dataskydd som standard*

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

4.3.1 Risk 1 Brist på kunskap om dataskyddsförordningen

En konsekvensbedömning avseende dataskydd enligt artikel 35 i GDPR ska alltid göras om en planerad personuppgiftsbehandling kan medföra en hög risk för de registrerade individerna. Detta förutsätter att det finns en allmän förståelse i organisationen för att dataskyddsansvariga kan behöva bli inblandade i en mängd olika sammanhang i verksamheten när personuppgifter förekommer, och
i synnerhet innan personuppgifter börjar behandlas i stor skala eller med hjälp av ny teknik.

I dagsläget har flera medarbetare goda kunskaper och arbetar systematiskt med dataskyddsfrågorna. Dock sker det inte i hela organisationen, en tydlig indikator på detta är att det finns kunskapsöar som är bra inom vissa specifika områden vilket beskrivs i den här rapporten. Risken är också att brist på förståelse skapar frustration och man ser det som ett hinder och inte en möjlighet att lagstiftningen finns.

	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

4.3.2 Risk 2 Inbyggt dataskydd och dataskydd som standard

Tanken är att inbyggt dataskydd och dataskydd som standard enligt artikel 25 i GDPR ska genomsyra hela utvecklingsprocessen och varje IT-systems hela livscykel, överallt där personuppgifter förekommer. Hur pass komplext arbetet i praktiken blir med att implementera detta beror helt på sammanhanget och behandlingarna. Det finns alltså ingen universallösning, utan inbyggt
dataskydd och dataskydd som standard är något som varje organisation måste förhålla sig till på en principiell, strategisk nivå och sedan arbeta med utifrån de egna förutsättningarna.

Under år 2021 har arbetet med dataskydd och informationssäkerhet aktualiserats och fått större plats inom området. Vinsten att göra det lätt att göra rätt har fått ta plats när man gör upphandlingar och tittar på nya IT-system.

	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

4.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att de befintliga digitala utbildningarna som finns på Stockholm stads intranät i dataskyddsförordningen blir obligatoriskt att genomgå årligen för samtliga anställda. Detta bör finnas med i ett årshjul som en fast aktivitet.

Förutsättningen att detta sker är att ledningen och styrelsen också har förståelse för vad riskerna är och betyder för organisationen. Därför rekommenderas ledningsgruppen att genomgå den specifika digitala utbildning för chefer som finns framtagna inom området och som är publicerat på Stockholm stads utbildningsplattform.

Under arbetet med registerförteckningen kan man med fördel se över om det finns system att bygga in mer dataskydd som standard. Ett exempel kan vara automatisk gallring av papperskorgen efter ex en månad osv.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granska intern kommunikation och utbildning*
- *Fungerar processerna för att hantera de registrerades rättigheter*

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 Granska intern kommunikation och utbildning

Det är avgörande att för ett gott dataskydd att det finns en tillräcklig medvetenhet och kunskap inom organisationen om hur personuppgifter får och ska hanteras. Alla personer som hanterar personuppgifter, och de som bestämmer hur de ska hanteras, måste få en adekvat utbildning. Det är viktigt att utbildningen är aktuell och hålls uppdaterad. Förutom de grundläggande kunskaperna om begrepp, principer m.m. som alla behöver, finns det vissa grupper som därutöver kan behöva mer riktade utbildningsinsatser som ger djupare kunskaper.

- Granska rutinerna för grundläggande utbildning till anställda och introduktion till nyanställda
- Granska genomförda utbildningsinsatser och sammanställ om möjligt statistik
- Granska grundutbildningens innehåll och säkerställ att den är aktuell

5.3.2 Granskning 2 Fungerar processerna för att hantera de registrerades rättigheter?

Ett av huvudsyftena med dataskyddsförordningen är att värna om enskilda individers rättigheter i sammanhang där deras personuppgifter behandlas och registreras. Därför måste alla organisationer vara medvetna om att man endast kan behandla personuppgifter om man respekterar individens fri- och rättigheter, och har rutiner för att bemöta och uppfylla dessa rättigheter när det blir aktuellt. Bestämmelserna om rättigheterna finns i

artiklarna 12-21 i GDPR. Det handlar bland annat, men inte enbart, om rätten till registerutdrag och rätten till radering. Under 2022 kommer följande att granskas:

- Granska om organisationen har klart för sig när de olika rättigheterna gäller
- Granska organisationens rutiner för att hantera förfrågningar från de registrerade om att utöva sina rättigheter enligt artiklarna 12-21 i GDPR
- Granska hur organisationen i praktiken hanterat begäran om registerutdrag.
- Granska hur organisationen i praktiken hanterat begäran om radering.
- Granska om organisationen svarar i tid på förfrågningar från de registrerade
- Granska hur organisationen dokumenterar (och gallrar) i samband med hantering av förfrågningar från registrerade

6 Övrigt att rapportera

6.1 Sammanfattning

Det behövs oftast en arbetsgrupp som tar det praktiska ansvaret för dataskyddsarbetet, både att identifiera vad som behöver göras och att genomföra det. Det räcker sällan med ett ensamt dataskyddsombud eller en ensam ansvarig person, utan det krävs en laginsats. Dataskyddsombudet ska också ha en granskande roll vilket försvårar att också vara en projektledare för implementation och framtagande av styrdokument vilket också framkommer av revision genomförd av revisionskontoret 2021.

Under 2021 har en intern arbetsgrupp införts för GDPR-arbetet och är i uppstartsutförande. Där ingår flera nyckelroller såsom registrator, kommunikatör, IT-avdelning osv.

6.2 DSO ger råd och rekommendationer till PUA

- Säkerställ att personerna i arbetsgruppen får adekvat utbildning
- Granska att organisationen har en fungerande dataskyddsorganisation med definierade roller. Säkerställ att rollerna är tillsatta så att det finns någon som innehar dem i praktiken och inte bara "på pappret".