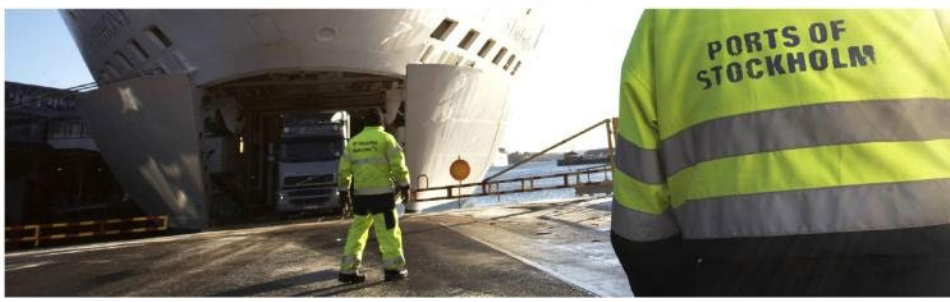
Dataskyddsförordningen, GDPR
Årsrapport 2020



GDPR årsrapport 2020
April 2021

Dnr: SH 2021/307
Utgivningsdatum: 2021-04-14
Kontaktperson: Jessica Hillergård

Bakgrund

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

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att 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”). DSO:n 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 nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt Dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att bolagsstyrelsen ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport för år 2020.

År 2020 har varit ett utmanande år för hela samhället och har inte lämnat Hamnen utan påverkan. På grund av den pågående pandemin fick aktiviteter inom dataskyddsområdet skjutas upp och senareläggas. Men, desto flera har lyckats att genomföras. Några av de milstolpar som nåtts är: konsekvensbedömningar inför upphandlingar, arbete kring Office365 och uppbyggnad samt överföring i det digitala verktyget DraftIT för registerförteckingen.

Hamnen har också beslutat att under 2021 anlita ett externt Dataskyddsombud.

Hamnen som organisation har kommit långt med implementation och har en relativt god mognadsgrad av kunskap, men behöver jobba på att få in det i alla delar av arbetet med personuppgifter.

Därför är nu min rekommendation att:

- prioritera utbildning av personal,
- följa de aktiviteter som årshjulet säger
- uppdatera inventering av registerförteckningen (3 år gammal)
- utse ägare till de olika personuppgiftsbehandlingarna så att dessa hålls uppdaterade systematiskt.

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 DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

Registerförteckning

Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	76
Har nödvändiga uppdateringar gjorts?	NEJ
Bedöms registerförteckningen vara fullständig?	JA
Har verksamheten lämpliga rutiner för registerföring?	NEJ

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 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 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.

Resultat

Totalt har 76 behandlingar registrerats varav 8 anses som högrisk efter granskning av föregående DSO. Det finns aktiviteter upplagda för varje personuppgiftsbehandling. Hamnen har ett högt säkerhetstänkande men efter djupare analys behöver registerförteckningen ses över för att förstå om tillräckliga åtgärder finns för personuppgifternas behandling. Vid en genomgång av registret och inläggning i DraftIT har flera luckor tydliggjorts och konkretiserats då frågeställningar i detta verktyg kräver att man svarar på fler frågor än som var aktuellt 2018 vid införandet av GDPR.

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

DSO:s bedömning av mognadsgraden av registerförteckningen inom Hamnen

Värde	Beskrivning
0	Registerförteckning/ arbetet/ rutin med denna saknas
1	Registerförteckning finns och är beroende av enskilda individers kunskap, ad hoc lösningar är dominerande
2	Registerförteckning finns och är beroende av enskilda individers kunskap, rutin finns men är under implementering.
3	Registerförteckningen och rutin är implementerad med utpekat ansvar för resp personuppgiftsbehandling. Stöd för verksamheten med DraftIT.
4	Registerförteckning och rutin finns och följer årshjulet. Ägare av de olika personuppgiftsbehandlingarna hanterar DraftIT självständigt.

5	Registerförteckningen är fullt implementerad och tillämpas enligt rutin. DSO kan granska efter årshjulet och åtgärder sker systematiskt.

DSO ger råd och rekommendationer till PUA

Då det saknas ansvarig för varje personuppgiftsbehandling som de facto utför dem, behöver en sådan rutin införas hos Hamnen. Detta betyder att utvalda funktioner inom personalgruppen behöver utbildas i verktyget DraftIT alternativt få kunskap om verktyget och förstå det systematiska arbetet med GDPR och kunna rapportera till DSO på excel-formulär. Dessa ska fungera som GDPR-ambassadörer och verka som kontaktpersoner vid de årliga genomgångarna av personuppgiftsbehandlingarna enligt årshjulet och kunna vid behov lägga till nya personuppgiftsbehandlingar, alternativt kontakta DSO för stöd.

Styrdokument

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?	Nej
Är dokumenten uppdaterade?	Nej
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Nej

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.

Resultat

Dokument och information finns att tillgå på intranätet för personalen på Hamnen. Dessa behöver under 2021 ses över och uppdateras.

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

DSO ger råd och rekommendationer till PUA

DSO:s rekommendation är att se över intranätet och tillgängligheten för GDPR-informationen. Detta behöver göras efter att den uppdaterats och kompletterats med ny information som framkommit sedan införandet. Ägare till styrdokumenten behöver utses.

Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	29 i verktyget KLASSA *Samtliga personuppgifts-behandlingar är klassade utifrån GDPR och finns dokumenterade i DraftIT.*
Är klassade personuppgiftsbehandlingar aktuella?	JA (enl. GDPR)

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.

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

Resultat

KLASSA har vidareutvecklats som verktyg av SKR och GDPR har blivit ett obligatoriskt segment med uppmaningen att kontakta DSO om det framkommer att det finns personuppgifter. Detta underlättar också för DSO:s arbete att få löpande information om KLASSA- aktiviteter och eventuella behov om konsekvensbedömning behöver utföras.

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

DSO ger råd och rekommendationer till PUA

När personuppgiftsbehandlingarna inventerats och progressen med ”GDPR-ambassadörer” utsetts är nästa naturliga steg att dessa också kan KLASSA:s för de system som är aktuella för detta. DSO:s rekommendation är att detta följs upp och påbörjas när inventering av personuppgifter är klar.

Konsekvensbedömningar

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

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/skall 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).

Resultat

Hamnen har under 2020 deltagit vid stadsgemensam konsekvensbedömning för elektroniska körjournaler med hastighetsövervakning samt egna för att bedöma möjligheter att arbeta mer molnbaserat.

Hamnen är van som organisation att arbeta med sådana här former av frågor och personalen är engagerad och ambitiös att nå resultat. Dock är detta nu på en ad hoc nivå och nästa steg är att dokumentera processen, finna rutiner och informera om den.

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

DSO ger råd och rekommendationer till PUA

Vidareutveckla konsekvensbedömningsprocessen, dokumentera och informera om rutiner.

Delegation för vem som ska representera PUA och ha mandat att godkänna respektive avslå åtgärder, kvarstående risker och DSO:s råd behöver omhändertas i den nya delegationsordningen.

Individens rättigheter

Sammanfattning

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

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.

Resultat

Rutiner för hur individens rättigheter ska omhändertas har under 2020 arbetats fram tillsammans med registrator. Dessa finns dokumenterade och fungerar.
Viktigt att poängtera är att *inga positiva besked* om radering, begränsning, registerutdrag etc. diarieförs efter Stadsarkivets beslut. Det är *endast nekande besked* som diarieförs. Detta innebär att det behöver föras statistik parallellt för att dessa siffror ska kunna presenteras årligen.

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

DSO ger råd och rekommendationer till PUA

Under 2021 behöver rutinerna ses över och eventuellt uppdateras. En statistik behöver föras för hur många begäran om att utöva rättigheter som inkommer för at kunna möta det önskemål om statistik som inkommit från SLK.

Personuppgiftsincidenter

Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	0
Hur många personuppgiftsincidenter har dokumenterats?	0
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

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 Dataskyddsförordningen 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.

Resultat

Hamnen som organisation har en god förmåga att rapportera *säkerhetsincidenter* i verksamheten och det görs i IA liksom utredningar etc. Inga personuppgiftsincider finns dock anmälda under 2020 och det är en brist.

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

DSO ger råd och rekommendationer till PUA

DSO uppmanar Hamnen att författa en personuppgiftsincidenthanterings rutin som kommuniceras brett samt att information/utbildning på intranätet och av DSO sker löpande.

Genomförda granskningar under året

Sammanfattning

Då jag som DSO är nytillträdd sedan 2021-02-15 ingår inte detta i 2020 års rapport.

Risker inom dataskydd

Sammanfattning

Relevanta risker inom verksamheten:

- *Efterlevnad av SchremsII/ Privacy shield*

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.

Resultatet av riskkartläggningen

Risk 1 Efterlevnad av Schrems II/ Privacy Shield

	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

DSO ger råd och rekommendationer till PUA

I juli 2020 föll en dom i EU-domstolen kallad Schrems II som innebär att tredjelandsöverföringar som hänvisar till Privacy Shield inte längre är möjliga att genomföra. Under 2021 ska detta vara fokusområde för DSO att granska samt informera PUA:s representanter, ledning och personalen inom Hamnen.

Granskningen kommer ske genom att:

- Kartlägga leverantörer, tjänster vid personuppgiftsinventering och inhämta PUB-avtal med instruktioner (Inventeringsprojekt)
- Identifiera genom PUB-avtalens instruktioner vilka som har tredjelandsöverföringar till USA/tredjeland (DSO)

- Frågeställningar om oklarheter om överföringar (Informationsägaren)
- Riskvärdering och Analys (DSO och informationsägaren)

När granskningen är genomförd kan beslut slutligen fattas om eventuella mitigerande åtgärder och/ eller om personuppgiftsbehandlingen kan fortgå med en anmälan till IMY.

Planerade granskningar under det nya verksamhetsåret

Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granskning av personuppgiftsbiträden*
- *Efterlevnad av Schrems II*

Syfte

Avsikten med att välja ut två områden för granskning är för att kunna planera och avsätta tid för detta under det kommande året. Att granska två personuppgiftsbiträden är också e både relevant för granskning, möjligt att mäta och en del av Dataskyddsombudets arbetsuppgift.

Planerade granskningar

Granskning 1

Hamnen har ett flera personuppgiftsbiträden inom verksamhetens olika områden. För att kontrollera att de uppfyller PUB-avtalen väljs 2 st. ut för att granskas med skriftliga frågor under våren 2021. Dessa kommer sedan att redovisas till PUA i separat rapport.

Den metod som ska användas är ett skriftligt formulär med frågor till de personuppgiftsbiträden som valts ut. I personuppgiftsbiträdets avtal ska det finnas inskrivet att de ska underkasta sig en sådan granskning. (Vid behov kan även deras lokaler granskas men pga. pågående pandemi begränsas denna granskning under 2021.)

Granskning 2

Se kapitel ”Risker inom dataskydd”.

Övrigt att rapportera

Övriga observationer

Observation 1 Personuppgiftsbiträdesavtal

Personuppgiftsbiträdesavtal ska vara ordnade vid genomförandet 2018. Det saknas dock som en del i upphandlingsprocessen om hur detta ska omhändertas.

Observation 2 Dataskyddsombudets roll och GDPR-organisation

Enligt Integritetsskyddsmyndighetens vägledning om Dataskyddsombud är det tydligt att denna funktion inte själv ska implementera arbetet utan kontrollera och ge råd likt en revisor. Detta är sällan fullt ut praktiskt då denna funktion oftast har bäst insyn i själva frågeställningarna och sett behoven av en åtgärd. För att få ett bra arbete med GDPR och att det blir en del av det vardagliga arbetet krävs dock att fler blir involverade i hela organisationen.

DSO ger råd och rekommendationer till PUA

Observation 1 Personuppgiftsbiträdesavtal

- Utbildning och lyfta in i upphandlingsprocessen när konsekvensbedömning och instruktion till PUB-avtal som är aktuella.
- Rutiner och kontroller av biträden saknas och ska lyftas in i årshjulet. Utförs av DSO och lämnas i årsrapport.

Observation 2 Dataskyddsombudets roll och GDPR-organisation

1) Inrätta med DSO en mindre styrgrupp som kan leda arbetet framåt med de behov som finns identifierade. Styrgruppen bör bestå av medlemmar med kunskap om organisationen och delegation att fördela arbetsuppgifter.
2) Informera ledning löpande och påvisa behovet och ansvarsfördelning av informationssäkerhets och dataskyddsarbete. GDPR tas med som en punkt i årsrapport och måluppfyllnadsdokument.
3) Inför en grupp med personal från olika verksamheter där man träffas över gränserna och utbyter erfarenhet och kunskap- dessa kan bli GDPR-ambassadörer i sina egna verksamheter. Detta blir i längden en form av egenkontroll och utbildning. På detta sätt kommer också nya rutiner och metoder få lättare spridning och förankring i verksamheten. Denna grupp träffas höst och vår för att sprida erfarenhet och belysa frågor för DSO.