Stockholms stad

Bilaga 7

GDPR Årsrapport

År 2022

Miljöförvaltningen

GDPR årsrapport
Januari 2022

Dnr: 2023-1086
Utgivningsdatum: 2022-01-17
Kontaktperson: Simon Jernelöv, Dataskyddsombud

1 Bakgrund

EU:s Dataskyddsförordning, GDPR, trädde i kraft 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 hanteringen 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 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 nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

2 Sammanfattning

I egenskap av Dataskyddsombud i Stockholms stads Miljö- och hälsoskyddsnämnd lämnar jag följande årsrapport.

DSO har under tillsynsåret involverats i verksamhetens dataskyddsarbete på ett aktivt och löpande sätt. Således har DSO haft god insyn i verksamhetens handlingssätt och upplever att samarbetet mellan verksamheten och DSO har lett till att verksamheten utför dataskyddsarbete på en god nivå.

DSO konstaterar att verksamhetens dataskyddsarbete håller en förhållandevis hög nivå och att flera av förra tillsynsårets föreslagna åtgärder har åtgärdats på ett lämpligt sätt.

DSO har granskat de sex obligatoriska granskningsområdena samt ett antal områden utöver de obligatoriska. Inledningsvis konstaterar DSO att verksamheten i hög utsträckning uppfyller de krav som ställs enligt dataskyddsförordningen och enligt den aktuella rapporten. DSO återger nedan de områden där vissa brister ändå finns som kan och behöver åtgärdas.

- DSO rekommenderar att verksamheten fortsätter med arbetet att upprätta styrdokument och komplettera de redan upprättade styrdokumenten.
- DSO rekommenderar att verksamheten säkerställer att samtlig personuppgiftsbehandling informationklassas.
- DSO rekommenderar att arbetet med att lösa den kommuninterna personuppgiftsansvarsfördelningen fortsätter.
- DSO rekommenderar att verksamheten upprättar blanketter som kan tillhandahållas till registrerade som vill lämna synpunkter och klagomål eller som vill utöva sina rättigheter enligt dataskyddsförordningen.

3 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 och personuppgiftsincidenter.

Nedan redogörs för nämndens eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	91 stycken
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

I artikel 30, GDPR, anges en skyldighet för varje personuppgiftsansvarig och personuppgiftsbiträde att upprätta ett register över samtliga personuppgiftsbehandlingar som utförs under dess ansvar.

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 som säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

Det är viktigt att personuppgiftsansvarige 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 personuppgiftsansvarige 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 personuppgiftsansvarige behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

91 stycken behandlingar finns registrerade i registerförteckningen 28 november 2022.

DSO kontrollerar om nödvändiga uppdateringar gjorts

DSO konstaterar att den senast uppdaterade versionen av registerförteckningen som tillhandahållits till DSO är daterad 28 november 2022, vilket indikerar att registerförteckningen hålls uppdaterad och levande. Bedömningen att registerförteckningen hålls uppdaterad understöds av uppgifter från den intervju som hållits i samband med tillsynsarbetet.

DSO bedömer hur fullständig registerförteckningen är

DSO bedömer att registerförteckningen är att anse som fullständig. Det framgick under tillsynen att verksamheten har arbetat noggrant med sin registerförteckning och lagt ned ett stort arbete på att säkerställa att verksamhetens samtliga personuppgiftsbehandlingar ingår. DSO konstaterar att verksamhetens samtliga personuppgiftsbehandlingar tycks ingår i registerförteckningen. Det finns definitivt en sådan ambition i verksamheten.

Registreringarna håller i regel en god kvalitet innehållsmässigt och exempelvis är fältet *Laglig grund* ifyllt i samtliga registreringar. I den föregående årsrapporten noterades det att det saknades information i fältet *(Om möjligt) Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder*. Detta har åtgärdats i 90 av

91 behandlingar. Under tillsynen 2021 noterade DSO att registerförteckningen i vissa fall var ifylld utifrån system och inte utifrån behandling. Även detta har åtgärdats i den uppdaterade registerförteckningen.

Den nuvarande registerförteckningen innehåller ett antal tomma fält, framför allt vad avser fältet ”*Kategorier av mottagare. (Förutom utlämnande av allmän handling)*”. DSO rekommenderar verksamheten att undvika att lämna fält tomma då det får registret att framstå som ofullständigt. Fyll därför i alla tomma fält, och skriv exempelvis ”Sker inte”, ”Ej tillämpligt” eller ”Nej” istället för att lämna en fråga obesvarad.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

DSO konstaterar att verksamheten har nedtecknade rutiner för arbetet med registerförteckningen. Det innebär att verksamheten arbetar med registerförteckningen som ett levande dokument på ett löpande sätt.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

3.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter att arbeta löpande med registerförteckningen utifrån att nya behandlingar införs eller att gällande behandlingar förändras. Verksamheten rekommenderas även fylla i alla tomma fält i registerförteckningen. Tomma fält kan få registerförteckningen att framstå som ofullständig.

3.2 Styrdokument

3.2.1 Sammanfattning – svar ifyllt från förra rapport:

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Delvis
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?	Nej

3.2.2 Syfte

Området syftar till att personuppgiftsansvarige genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar personuppgiftsansvarige 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 relevanta 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.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

DSO konstaterar att verksamhetens styrande dokumentation i dagsläget omfattar en stor del av dataskyddsområdet. Verksamheten har följande nedtecknade rutiner:

- Rutin för konsekvensbedömning
- Rutin för tillvaratagande av de registrerades rättigheter
- Rutin för begäran om registerutdrag
- Rutin för hantering av personuppgiftsincident
- Rutin för användning av nya molntjänster
- Rutin för elektronisk kommunikation (berör delvis GDPR, miljö- och hälsoskyddsnämnden uppger att de inväntar rutin från stadsledningskontoret avseende sociala medier)
- Rutin för att hålla artikel 30-registret uppdaterat

DSO bedömer att den styrande dokumentationen är godtagbart omfattande, men att det finns utrymme för fortsatt arbete med att upprätta än mer styrande dokumentation. I föregående årsrapport konstaterade DSO att de tillhandahållna dokumenten saknade en uttryckligen angiven ägare. Verksamheten har nu inkommit med uppdaterade dokument där ägare anges. I föregående årsrapport noterade DSO att det saknades rutin för inbyggt dataskydd och dataskydd som standard. DSO har i år tagit del av en sådan rutin som utarbetats av Stadsledningskontoret centralt och förutsätter att miljöförvaltningen implementerar denna rutin i sitt arbete.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

DSO bedömer att innehållet i de tillhandahållna dokumenten håller god kvalitet. Rutinerna är överskådliga, lättillgängliga, omfattande och är utformade för att kunna användas av samtliga anställda. Även i övrigt bedömer DSO att dokumenten är relevanta och väl uppdaterade.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter arbetet med att implementera styrande dokument.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Ungefär 65 stycken
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stockholms stads riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen saknar verksamheten förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att personuppgiftsansvarige 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 uppdraget, minskar sannolikheten avsevärt att en klassning faktiskt initieras.

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

3.3.3 Resultat

DSO har jämfört systemklassningarna mot de angivna system som anges i registerförteckningens fält ”*Var finns personuppgifterna?*”. DSO konstaterar att de genomförda informationsklassningarna täcker de allra flesta system som används vid de flesta av nämndens personuppgiftsbehandlingar. I föregående årsrapport konstaterade DSO att personuppgiftsbehandling som sker i exempelvis Outlook eller på verksamhetens servrar inte täcktes av de systemövergripande informationsklassningar som gjorts. DSO har nu fått information om att informationsklassning påbörjats för personuppgiftsbehandlingar som sker på förvaltningens gruppdiskar, normalt i form av MS Office-filer. Detta arbete förväntas vara slutfört Q2 2023.

Översyn av klassningarna sker årligen och bedöms vara aktuella. Det innebär att DSO bedömer att lämpliga tekniska och organisatoriska åtgärder är vidtagna för verksamhetens personuppgiftsbehandlingar.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

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

3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter med sitt informationsklassningsarbete i fråga om personuppgiftsbehandlingar som inte sker i de datorsystem som hittills informationsklassats. DSO noterade under tillsynen 2021 att utformningen av SKR:s KLASSA är systemorienterat och att viss personuppgiftsbehandling därför kan vara svår att passa in i den mall som tillhandahålls av KLASSA. DSO rekommenderade därför att informationsklassningsarbetet skulle skiftas från ett systemorienterat till ett behandlingsorienterat arbetssätt. DSO

rekommenderar även att informationsklassningen av verksamhetens gruppdiskar fullföljs enligt plan.

3.4 Konsekvensbedömningar

3.4.1 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

3.4.2 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 uttryckligen angivet i GDPR och ska utföras för alla nya behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). Det är viktigt att personuppgiftsansvarige genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

DSO har inte fått information om att verksamheten har gjort någon retroaktiv inventering av redan pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter och på så sätt föranleda en konsekvensbedömning. Däremot konstaterar DSO att kunskapsläget och medvetenheten kring dataskyddsfrågor bland de anställda är på så pass hög nivå att det enligt vår bedömning inte föreligger någon risk att någon högriskbehandling som inte konsekvensbedömts skulle pågå i dagsläget. Nämndens systemanvändande styrs till övervägande del av Stockholms stads centrala direktiv, vilket minimerar risken att nämnden ensam använder sig av ett system som skulle innebära en hög risk för de registrerades integritet, utan att ha konsekvensbedömts.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Verksamheten har under tillsynsåret genomfört en konsekvensbedömning som DSO varit involverad i. Konsekvensbedömningen gällde en tjänst för säkra meddelanden, *TrustedDialog (TDialog)*. DSO bedömde att det var en väl genomförd konsekvensbedömning och att det inte var nödvändigt för verksamheten att begära förhandssamråd.

Är de genomförda konsekvensbedömningarna aktuella?

DSO konstaterar att de genomförda konsekvensbedömningarna är genomförda i närtid och är aktuella. Personuppgiftsbehandlingarna som konsekvensbedömningarna avser har inte förändrats i någon nämnvärd mån och konsekvensbedömningarna har således inget behov av att uppdateras.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

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

DSO bedömer att verksamhetens regelefterlevnad gällande konsekvensbedömningsarbetet är så gott som fullständig. Kunskapsläget är mycket bra, både hos ledningen och hos berörda anställda i stort. Av den anledningen föreligger en låg risk att verksamheten ägnar sig åt icke konsekvensbedömda personuppgiftsbehandlingar som innebär en hög risk för registrerades fri- och rättigheter.

De genomförda konsekvensbedömningarna där DSO involverats håller hög kvalitet.

3.4.5 DSO ger råd och rekommendationer till PUA

I föregående årsrapport rekommenderade DSO verksamheten att klargöra ansvarsfördelningen mellan Stockholm stad centralt och Miljö- och hälsoskyddsnämnden som personuppgiftsansvarig. Detta gällde framför allt de personuppgiftsbehandlingar som sker i datasystem som upphandlats centralt och där användningen för nämndernas del är påbjuden från Fullmäktige eller Stadsledningskontoret. Enligt den information som DSO tagit del av pågår det nu ett arbete med att klargöra ansvarsfördelningen. Detta kommer sannolikt tydliggöra fördelningen av ansvaret för konsekvensbedömningar av system respektive behandlingar inom staden.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt garanterar 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 personuppgiftsansvarige tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, 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 organ 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 även att det finns undantagssituationer angivna i artikel 12.3, där svarsfristen kan förlängas till mer än en månad.)

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

Om verksamheten inte klarar av att hantera en begäran från registrerade personer i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från IMY:s sida, med sanktioner som följd. Det är därför viktigt att

personuppgiftsansvarige regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Verksamheten har under tillsynsåret inte tagit emot någon begäran från registrerade avseende registerutdrag, begränsning eller radering.

DSO konstaterar att verksamheten har goda förutsättningar för att hantera registrerades rättigheter på ett mycket gott sätt. Rutinen för hantering av dessa ärenden tycks fullt ut förankrad i verksamheten. Det är väl känt för medarbetarna vem de ska kontakta om en begäran från en registrerad inkommer till förvaltningen. DSO bedömer att de rutiner som finns nedtecknade för att tillvarata de registrerades rättigheter är mycket goda.

3.5.4 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

3.5.5 DSO ger råd och rekommendationer till PUA

Under tillsynen 2021 noterade DSO att det saknades blanketter för de registrerade som vill utöva sina rättigheter. DSO har inte fått information om att detta har åtgärdats. DSO rekommenderar därmed att verksamheten upprättar blanketter att tillhandahålla till registrerade som vill utöva sina rättigheter. En sådan blankett underlättar både för den registrerade att lätt kunna ta tillvara sina rättigheter, och för tjänstemännen, som genom en väl ifylld blankett

får den information de behöver för att tillmötesgå begäran redan i ett första skede.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom att medarbetare i verksamheten anmäler till behörig person, eller genom att ledning eller dataskyddssamordnare noterar signaler om incidenter
Hur många personuppgiftsincidenter har dokumenterats?	10
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	2 till IMY, varav 1 även rapporterades till berörda personer
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	1

3.6.2 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 god personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

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, och då inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering även till de berörda personerna.

Om en organisation brister i förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY:s sida. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med Dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för den egna organisationen att förbättra sin personuppgiftshantering genom systematiskt kvalitetsarbete och för tillsynsmyndigheten (IMY) att kontrollera efterlevnaden. Bristande dokumentation är sanktionsgrundande.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

Av de tio personuppgiftsincidenter som dokumenteras under tillsynsåret har två stycken rapporterats till IMY. En av incidenterna rapporterades i tid, det vill säga inom 72 h från upptäckten, medan den andra incidenten inte rapporterades i tid. Den incident som rapporterades för sent bedömdes inledningsvis inte vara av

anmälningspliktig karaktär enligt verksamheten. Incidenten omfattade dock bland annat uppgifter om sjukskrivning. Detta är känsliga personuppgifter och efter rekommendation av DSO anmäldes incidenten till IMY, dock efter utsatt tid. Utöver dessa två incidenter uppfattar DSO att verksamhetens bedömning att de övriga incidenterna varit av ringa betydelse varit korrekt. DSO bedömer även att verksamheten har goda rutiner för att upptäcka och dokumentera incidenter i tid.

3.6.4 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

3.6.5 DSO ger råd och rekommendationer till PUA

DSO noterar att tio stycken personuppgiftsincidenter under ett tillsynsår för en verksamhet av Miljönämndens storlek är ett förhållandevis lågt antal. Det kan finnas två anledningar till ett sådant förhållandevis lågt antal: antingen hanterar verksamheten sina personuppgifter på ett ovanligt tillfredsställande sätt, eller så sker det i praktiken fler incidenter, men som inte rapporteras eller anmäls till de ansvariga i organisationen. Det skulle alltså kunna finnas ett mörkertal, beroende på exempelvis bristande insikt hos tjänstemännen om vad en personuppgiftsincident faktiskt är och hur en sådan incident ska hanteras när den befaras ha inträffat. DSO noterar även att en incident till förstone inte rapporterats till IMY trots att den inkluderat känsliga personuppgifter men ser att verksamheten noggrant har dokumenterat samtliga incidenter och visar mycket goda förutsättningar för att fortsatt förbättra arbetet med hantering av personuppgiftsincidenter samt spridning av kunskap hos personalen. Av den anledningen rekommenderar DSO att personuppgiftsansvarige lägger särskilt fokus på att sprida kunskap om vad personuppgiftsincidenter är och hur de ska hanteras.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Granskning 1 – Implementering av åtgärder från förra årets tillsynsrapport*
- *Granskning 2 – Interkommunala samarbeten (EKR)*
- *Granskning 3 – Agerande med anledning av Schrems II-domen*

4.2 Syfte

En av dataskyddsombudets centrala uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En viktig del av detta arbete är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten behöver fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarige är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under tillsynsåret och vad resultaten av granskningarna är.

4.3 Genomförda granskningar och deras resultat

Granskning 1 - Implementering av åtgärder från förra årets tillsynsrapport

- I föregående årsrapport föreslog DSO ett antal åtgärder, däribland:
- redigering och komplettering av registerförteckningen,
- skifte från ett systemorienterat till ett behandlingsorienterat informationsklassningsarbete,
- upprättande och komplettering av styrdokument,
- upprättande av blanketter till registrerade som vill utöva sina rättigheter,
- rutin och blankett för användning av samtycke som rättslig grund,
- utbildningsinsatser avseende personuppgiftsincidenter, samt

- att problemen kring de kommuninterna personuppgiftsansvaren skulle åtgärdas.

DSO konstaterar att flera av de rekommenderade åtgärderna har implementerats av Miljö- och hälsoskyddsnämnden. De åtgärder som ännu inte implementerats fullt ut enligt den information som tillhandahållits till DSO är:

- placering av personuppgiftsansvar i stadsgemensamma personuppgiftsbehandlingar, samt
- upprättande av blanketter till registrerade som vill utöva sina rättigheter.

Vad gäller placering av personuppgiftsansvar för stadsgemensamma personuppgiftsbehandlingar konstaterar DSO att detta är ett arbete som till sin natur förutsätter ett samarbete mellan flertalet av stadens personuppgiftsansvariga (nämnder och bolag). Nämnden har under året deltagit i ett stadsgemensamt samarbete i avsikt att lösa frågan. DSO bedömer givet detta att Miljönämnden, så långt det går från eget håll, har drivit på för att försöka implementera den rekommenderade åtgärden.

	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

Granskning 2 – Interkommunala samarbeten (EKR)

Under året framkom att personuppgiftshanteringen inom det kommunövergripande samarbete för Energi och klimatrådgivning som bedrivits mellan 26 kommuner i Stockholmsregionen under ett antal år, inte reglerats mellan de deltagande kommunerna.

För att hantera denna brist sattes det igång ett arbete för att i första steget analysera samarbetets förutsättningar utifrån ett GDPR-perspektiv och i nästa steg upprätta en gemensam personuppgiftspolicy och ett datadelningsavtal (artikel 26, GDPR). Dokumenten har under året presenterats för EKR-samverkans

ledningsgrupp och står i begrepp att antas av de medverkande kommunerna, varför problemet får anses åtgärdat.

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

Granskning 3 – Agerande med anledning av Schrems II-domen

Under 2020 kom avgörandet Schrems II från EU-domstolen. Där slog domstolen fast att Privacy Shield-avtalet mellan EU och USA inte gav ett tillräckligt skydd för personuppgifter när dessa förs över till USA. Ogiltigförklarandet innebär att verksamheter inte längre kan stödja sig på Privacy Shield som grund för att överföra personuppgifter till USA. DSO har därför valt att granska verksamhetens agerande med anledning av Schrems II-avgörandet.

DSO konstaterar inledningsvis att verksamheten uppvisar god kunskap om avgörandet och de konsekvenser avgörandet har fått på dataskyddsområdet i stort. Det finns en tydlig förståelse i verksamheten om de problem som tredjelandsöverföring till USA innebär. Som exempel på den goda medvetenheten så ställer verksamheten numera krav i nya upphandlingar av data- och molntjänster så att inga otillåtna tredjelandsöverföringar av personuppgifter ska ske. Vissa stadsgemensamma system kan innebära tredjelandsöverföringar och i dessa fall har verksamheten valt att använda andra system eller att inte använda systemet fullt ut för att i den mån det är möjligt kunna undvika tredjelandsöverföringar.

DSO noterar däremot att kommunikationsavdelningen i verksamheten använder sig av ett flertal olika sociala medier, exempelvis Instagram, Facebook och LinkedIn. Där publicerar verksamheten exempelvis bilder på politiker eller information som har med verksamheten att göra. Verksamheten uppger att de publicerar personuppgifter på sociala medier i så låg utsträckning som möjligt, vilket DSO rekommenderar att de fortsätter med. I

dagsläget finns en stadövergripande policy för sociala medier som endast berör dataskydd generellt. Verksamheten uppger att arbetet med en rutin avseende sociala medier som berör dataskydd specifikt har påbörjats och att de inväntar denna.

	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

DSO rekommenderar att verksamheten implementerar och använder sig av en blankett för inhämtning av samtycke vid publicering av personuppgifter på sociala medier, samt upprättar nedtecknade rutiner för användning av samtycke. DSO uppmuntrar att arbetet med en policy för sociala medier och dataskydd har påbörjats och rekommenderar verksamheten att implementera denna i organisationen när den är färdigställd.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *DSO har inte identifierat eller blivit uppmärksammad på några risker i verksamheten som inte redan är hanterade i riskanalyser och konsekvensbedömningar.*

5.2 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. DSO behöver som underlag för sin planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, gällande 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.

5.3 Resultatet av riskkartläggningen

	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

5.4 DSO ger råd och rekommendationer till PUA

En Miljöförvaltning tillhör inte typiskt sett den del av en kommuns verksamhet där det hanteras stora mängder känsliga personuppgifter eller vars personuppgiftsrisker på annat sätt kan förväntas vara framträdande.

Givet detta och att DSO i dagsläget inte har kännedom om några nämnvärda risker i nämndens verksamhet, lämnas inga rekommendationer på detta område.