Stockholms stad

Bilaga 7

GDPR Årsrapport

År 2023

Miljöförvaltningen

GDPR årsrapport
Januari 2024

Dnr: 2024-401
Utgivningsdatum: 2024-01-05
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 tidigare tillsynsår involverats i verksamhetens dataskyddsarbete på ett aktivt och löpande sätt. Således har DSO haft insyn i verksamhetens handlingssätt och upplevt att samarbetet mellan verksamheten och DSO 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 säkerställer att rutinen för anmälan av ny personuppgiftsbehandling är förankrad fullt ut i organisationen.
- DSO rekommenderar att verksamheten uppdaterar dokumenten för sociala medier och molntjänster enligt anvisningar nedan och att verksamheten fortsätter arbetet med att implementera styrande dokument.
- DSO rekommenderar att verksamheten säkerställer att samtlig personuppgiftsbehandling informationklassas.
- DSO rekommenderar att arbetet med att lösa den kommuninterna personuppgiftsansvarsfördelningen slutförs.
- DSO rekommenderar att verksamheten gör en mindre justering av strukturen i webbformuläret för registrerades rättigheter.
- DSO rekommenderar att personuppgiftsansvarige lägger särskilt fokus på att sprida kunskap om vad personuppgiftsincidenter är och hur de ska hanteras.
- DSO rekommenderar att verksamhetens anställda får tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och regleringen gällande allmänna handlingar.

- DSO rekommenderar att verksamheten säkerställer att samtliga rekommenderade åtgärder från tidigare årsrapport åtgärdas.

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?	126 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 dataskyddsförordningen 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
126 behandlingar finns registrerade i registerförteckningen 6 december 2023.

DSO kontrollerar om nödvändiga uppdateringar gjorts
DSO konstaterar att den senast uppdaterade versionen av registerförteckningen som tillhandahållits till DSO är daterad 6 december 2023, 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.

I den föregående årsrapporten noterade DSO att det saknades information i ett antal fält i registerförteckningen, framför allt avseende fältet ”*Kategorier av mottagare. (Förutom utlämnande av allmän handling)*”. DSO rekommenderade verksamheten att undvika att lämna fält tomma då det fick registret att framstå som ofullständigt. Detta har åtgärdats i majoriteten av behandlingarna i registerförteckningen.

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. Verksamheten har även ändrat klassificeringsstrukturen vad gäller relationen mellan registerförteckningen och klassificerings-hänvisningar. Så vitt DSO kan bedöma ingår verksamhetens samtliga personuppgiftsbehandlingar 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.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

DSO konstaterar att verksamheten har nedtecknade rutiner för arbetet med registerförteckningen. Verksamheten uppger att rutinen för anmälan av nya personuppgiftsbehandlingar inte är förankrad fullt ut i organisationen. Medarbetarna är dock medvetna om att nya personuppgiftsbehandlingar ska anmälas till respektive chef, som i sin tur har god kännedom om rutinen för anmälan av nya personuppgiftsbehandlingar. Verksamheten arbetar med registerförteckningen som ett levande dokument på ett löpande sätt. DSO bedömer att det är sannolikt att majoriteten av alla nya behandlingar upptäcks och anmäls till ansvarig funktion.

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 arbeta löpande med registerförteckningen utifrån att nya behandlingar införs eller att gällande behandlingar förändras. DSO rekommenderar att verksamheten säkerställer att rutinen för anmälan av nya personuppgiftsbehandlingar är förankrad fullt ut i organisationen.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

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 dataskydds-förordningens 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. DSO har sedan tidigare granskat verksamhetens 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
- Rutin för att hålla artikel 30-registret uppdaterat

DSO har detta tillsynsår granskat verksamhetens följande nedtecknade dokument:

- Policy för Stockholms stads konton i sociala medier
- Riktlinjer för sociala medier – Miljöförvaltningen
- Ansökan för användning av ny molntjänst
- Webbformulär för begäran om rättigheter enligt dataskyddsförordningen

DSO bedömer att den styrande dokumentationen är godtagbart omfattande, men att det finns utrymme för fortsatt arbete med att upprätta än mer styrande dokumentation.

Det saknas till exempel rutindokument som beskriver den interna GDPR-gruppens arbetsuppgifter. För att verksamheten ska uppfylla ansvarsskyldigheten och kunna visa att dataskyddsförordningen efterlevs rekommenderar DSO att verksamheten upprättar ett skriftligt rutindokument där GDPR-gruppens arbetsuppgifter och ansvarsområden framgår.

Föregående tillsynsår utarbetades en rutin för inbyggt dataskydd och dataskydd som standard av Stadsledningskontoret. Miljö- och hälsoskyddsnämnden uppger att rutinen har implementerats i deras arbete och att de genomfört förändringar med anledning av rutinen.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

I dokumentet ”Riktlinjer för sociala medier – Miljöförvaltningen” anges att publicering av bilder och filmer som innehåller personuppgifter oftast kräver samtycke från de berörda personerna. Det anges inte hur samtycke ska inhämtas. Vidare finns ett separat verktyg för inhämtande av samtycke vid publicering på sociala medier som verksamheten ska använda sig av. DSO rekommenderar att verksamheten uppdaterar riktlinjen för sociala medier och inför en hänvisning till verktyget för inhämtande av samtycke.

I dokumentet ”Ansökan användning av ny molntjänst” heter den sista rubriken ”Lista över tredje länder”. Under rubriken finns endast en lista över länder med adekvat skyddsnivå. DSO rekommenderar att verksamheten justerar detta och säkerställer att rubriken speglar innehållet.

DSO bedömer i övrigt att innehållet i de tillhandahållna dokumenten håller god kvalitet. Rutinerna är överskådliga, lättillgängliga, omfattande och är utformade för att kunna användas av samtliga anställda. DSO bedömer att dokumenten är relevanta och 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
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	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. DSO rekommenderar även att verksamheten uppdaterar dokumenten för sociala medier och molntjänster enligt anvisningar ovan.

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?	DSO har inte fått uppgifter om detta
Är klassade personuppgiftsbehandlingar aktuella?	-

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd 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 informations-klassningen 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

I tidigare årsrapport konstaterade DSO att personuppgiftsbehandling som sker i exempelvis MS Outlook och på verksamhetens servrar inte täcktes av de systemövergripande informationsklassningar som gjorts. DSO fick under föregående tillsynsår information om att informationsklassning påbörjats för personuppgiftsbehandlingar som sker på förvaltningens gruppdiskar, normalt i form av MS Office-filer. Verksamheten har hittills genomfört informations-klassning för varje avdelnings gruppdisk. Verksamheten har inte slutfört informationsklassningar för den gemensamma disken, medarbetares personliga diskar eller e-post.

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

3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter med sitt informationsklassningsarbete och att informationsklassningen av verksamhetens diskar och e-post 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 personuppgifts-behandlingar 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?
Miljö- och hälsoskyddsnämnden har efter ett centralt beslut infört ZoomX som videokonferensverktyg. För personuppgifts-behandlingen genomförde verksamheten inte en egen konsekvensbedömning, utan detta genomfördes centralt av staden. Inga konsekvensbedömningar har genomförts av verksamheten under tillsynsåret.

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 konsekvensbedömningar som genomförts tidigare tillsynsår där DSO involverats håller hög kvalitet.

3.4.5 DSO ger råd och rekommendationer till PUA

I årsrapporten från 2021 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 tog del av föregående tillsynsår pågick det ett arbete med att klargöra ansvarsfördelningen. Enligt den information som DSO tagit del av under årets tillsyn har arbetet med att klargöra ansvarsfördelningen avstannat. DSO rekommenderar verksamheten att återuppta och slutföra arbetet. 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?	2 (begäran om registerutdrag)
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	2

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 tagit emot två begäranden om registerutdrag. Samtliga hanterades inom föreskriven tidsfrist på 30 dagar.

DSO konstaterar att verksamheten har goda förutsättningar för att hantera registrerades rättigheter på ett mycket gott sätt. Rutinen för hantering av dessa ärenden tycks vara 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.

Under tidigare tillsynsår noterade DSO att det saknades blanketter för de registrerade som vill utöva sina rättigheter. DSO rekommenderade därför verksamheten att upprätta blanketter att tillhandahålla till registrerade som vill utöva sina rättigheter. Detta har åtgärdats och DSO har tagit del av ett webbformulär där registrerade kan utöva sina rättigheter.

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

Vad gäller webbformuläret avseende de registrerades rättigheter har DSO ett förbättringsförslag avseende strukturen. DSO rekommenderar att rubriken ”Begäran om registerutdrag” ska flyttas ner till en valbar ruta, för att det ska bli tydligt att det är en separat begäran likt en begäran om radering exempelvis. En tydligt

utformad blankett underlättar både för den registrerade som lättare kan 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?	8
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Ingen av incidenterna har rapporterats till IMY eller till berörda personer
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Ej aktuellt

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskydds-förordningen (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 flera 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 det 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 åtta personuppgiftsincidenter som dokumenteras under tillsynsåret har ingen av incidenterna rapporterats till IMY eller till berörda personer.

DSO uppfattar att verksamhetens bedömning av att de inträffade 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 åtta 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 finns ett mörkertal – alltså att det i praktiken sker fler incidenter, men att dessa inte rapporteras eller anmäls till de ansvariga i organisationen. Mörkertalet skulle alltså kunna bero på exempelvis bristande insikt hos tjänstemännen om vad som utgör en personuppgiftsincident och hur en sådan incident ska hanteras när den befaras ha inträffat. DSO 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 – Arbetet med dataskydd vid upphandling*
- *Granskning 3 – De anställdas användning av e-post på arbetet*

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:
- att alla personuppgiftsbehandlingar skulle informationsklassas,
- redigering och komplettering av registerförteckningen,
- upprättande av blanketter till registrerade som vill utöva sina rättigheter, samt
- att problemen kring de kommuninterna personuppgiftsansvaren skulle åtgärdas.

DSO konstaterar att flera av de tidigare 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
- informationsklassning av samtliga personuppgiftsbehandlingar.

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). DSO rekommenderar att Miljönämnden, så långt det går från eget håll, försöker 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 – Arbetet med dataskydd vid upphandling

Dataskyddsförordningen gäller för behandling av personuppgifter i olika it-system som den personuppgiftsansvarige använder. Den personuppgiftsansvarige har ansvar för att säkerställa att all behandling som sker av den personuppgiftsansvarige eller på den personuppgiftsansvariges uppdrag uppfyller kraven på teknisk och organisatorisk säkerhet som uppställs i dataskyddsförordningen. Tekniska och organisatoriska säkerhetsåtgärder kan vara åtgärder som den personuppgiftsansvarige själv vidtar eller kan det vara krav som ställs på en systemleverantör som är personuppgiftsbiträde. För att säkerställa att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas behöver den personuppgiftsansvarige analysera informationen och personuppgiftsbehandlingen. I de flesta fall behöver en riskanalys och informationsklassning göras och i vissa fall behöver en konsekvensbedömning enligt dataskyddsförordningen göras.

Den personuppgiftsansvariges ansvar för att vidta säkerhetsåtgärder för att säkerställa och visa att dataskyddsförordningen följs regleras i artikel 24 och artikel 25 dataskyddsförordningen. Den personuppgiftsansvariges ansvar för personuppgiftsbiträden regleras i artikel 28 dataskyddsförordningen. Den personuppgiftsansvariges och personuppgiftsbiträdens ansvar för att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till risken regleras i artikel 32 dataskyddsförordningen.

DSO konstaterar att verksamhetens visar god kunskap för hur dataskydd ska beaktas vid upphandling och inköp av nya system. Verksamheten använder Stadens mall för PUB-avtal vid upphandling och inköp som omfattar personuppgiftsbehandling av personuppgiftsbiträden. I enlighet med stadens rutin för informationssäkerhet genomför verksamheten en analys av hur personuppgiftsansvaret ska se ut inför nya upphandlingar och inköp av system. Inga nödvändiga åtgärder har identifierats av DSO.

	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 – De anställdas användning av e-post på arbetet

Den behandling av personuppgifter som sker i anställdas e-post på arbetet omfattas av dataskyddsförordningen. Precis som all behandling av personuppgifter behöver den personuppgifts-behandling som sker i e-posten ha en rättslig grund. Behandlingen behöver även vara förenlig med de grundläggande principer som finns i dataskyddsförordningen, såsom att enbart samla in personuppgifter för specifika ändamål, att radera personuppgifterna när de inte längre behövs och att skydda uppgifterna från spridning eller från att obehöriga får tillgång till dem.

För att säkerställa att hanteringen av personuppgifter i e-posten är laglig och sker på ett korrekt sätt måste organisationen ta fram rutiner eller andra riktlinjer som anger hur e-posten ska hanteras.

Därefter behöver informationen spridas till de som berörs inom organisationen.

Skyldigheten att behandla personuppgifter korrekt i e-posten följer av de grundläggande principerna i artikel 5 dataskyddsförordningen. Principerna innebär bland annat att personuppgiftsansvariga

• måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
• bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
• inte ska behandla fler personuppgifter än vad som behövs för ändamålen
• ska säkerställa att personuppgifterna är riktiga
• ska radera personuppgifterna när de inte längre behövs
• ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
• ska kunna visa att dataskyddsförordningen följs och hur det görs.

De grundläggande principerna i artikel 5 ska genomsyra all personuppgiftsbehandling.

DSO konstaterar inledningsvis att verksamheten uppvisar god kunskap avseende hur dataskydd ska beaktas vid användning av e-post. Det finns hos de medarbetare vi talat med en medvenhet om vilka uppgifter som inte ska behandlas i e-post och det finns rutiner för elektronisk kommunikation som även innefattar e-post.

DSO har emellertid fått information om att det förekommer att anställda i viss utsträckning använder e-post för lagring av information istället för att flytta informationen till lämpligt verksamhetssystem. Det är viktigt att lagra information på rätt ställe och att radera e-post som ska raderas enligt dataskydds-förordningen, utan att radera den e-post som utgör allmänna handlingar och därmed ska bevaras. De anställda behöver få tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och allmänna handlingar, vilket kan ske genom exempelvis regelbundna utbildningar till de anställda.

	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 säkerställer att samtliga rekommenderade åtgärder från tidigare årsrapport implementeras. DSO rekommenderar även att de anställda får tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och allmänna handlingar, vilket kan ske genom exempelvis regelbundna utbildningar till de anställda.

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.

Stockholm 2024-01-05

Simon Jernelöv
Externt dataskyddsombud