Verksamhetsutveckling
Johanna Munther

Styrelsen för Stockholm Vatten och Avfall AB
Styrelsen för Stockholm Avfall AB

Dataskyddsombudets Årsrapport 2023 – Stockholm Vatten och Avfall

FÖRSLAG TILL BESLUT

Styrelsen föreslås besluta

att anta årsrapporten ifrån bolagets dataskyddsombud

att ge bolaget i uppdrag att vidta åtgärder i enlighet med rekommendationerna

Christian Rockberger
Verkställande direktör

Johanna Munther
Avdelningschef
Verksamhetsutveckling

Bilaga: Dataskyddsombudets Årsrapport år 2023 Stockholm Vatten och Avfall

Dataskyddsombudets Årsrapport år 2023 Stockholm Vatten och Avfall

Tillsammans för världens mest hållbara stad

STOCKHOLM VATTEN OCH AVFALL

Författare: Jessica Hillergård, Dataskyddsombud@svoa.se
Rapporten citeras: Hillergård, J (2024). Dataskyddsombudets Årsrapport år 2023 Stockholm Vatten och Avfall. Stockholm Vatten och Avfall AB.
Diarienummer: 24SVOA64, 24SVOA73 och 24SVOA74
Kontaktuppgifter: Stockholm Vatten och Avfall AB, 106 36 Stockholm
Telefon: 08-522 120 00
Webb: www.svoa.se

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.
Dataskyddsåret har varit fullt av både upp och nergångar. Den 25:e maj firade GDPR 5 år sedan införandet och mycket har hänt och kommer hända. En snabb omvärldsbevakning pekar på att GDPR och det kommande NIS2-direktivet[1] kommer att ligga till grund för flera kommande förordningar inom EU. Bland annat kan det omnämnas att regleringar kommer ske inom områdena AI (Artificiell intelligens), IoT (Internet of Things) och DMA (Förordningen om digitala marknader)[2] vilket alla påverkar SVOA:s dagliga arbete. År 2023 var också året då terrorhotsnivån i Sverige höjdes och flertalet uppmärksammade incidenter med attacker mot myndigheter och organisationer skedde. Det i sin tur har också lett till en ny syn på behov av säkerhetskontroller och krisorganisationer.

Tidigare år har revisionskontoret anmärkt på att Dataskyddsombudet inte ska vara operativt i dataskyddsarbetet utan vara granskande, utbildande och rådgivande. Organisationen ska själv efter råd, stöd och rekommendation ta fram stöddokument, annars riskerar dataskyddsombudet att granska sig själv[3]. Tanken med dataskyddsförordningen är att det ska var som vilken annan lagstiftning som helst och arbetas med systematiskt där personuppgifter behandlas. Stadsledningskontoret, SLK, har tagit fram en förvaltningsmodell för information kallad PM[3] i syfte att besätta roller med ansvar för informationshantering. Organisationen har anpassat PM[3]-modellen under en tid och nu finns en remiss för hur roller och ansvar ska fördelas. Detta kommer underlätta arbetet med dataskyddsfrågor då dataskyddsombudets roll blir som lagen säger, strikt rådgivande, och arbetsuppgifterna att ta fram en rutin hamnar ur verksamhetens eget perspektiv. Rutinen ska spegla verkligheten och omhändertar de administrativa risker analyserna säger de ska åtgärda vilket kommer fram ur PM[3]-arbetet. När ansvarsfördelningen är gjord i hela PM[3]- organisation kommer också arbetet med registerförteckning, styrdokument och analyser göras mer systematiskt. Som granskning kommer jag som DSO att följa upp implementeringen av den framtagna modellen under 2024 då det är av vikt att aktiviteter inom dataskyddsområdet startar så snart som möjligt. Idag sker aktiviteter personberoende och situationsanpassat, vilket jag önskar vi förbättrar under år 2024.

Som Dataskyddsombud, DSO, för SVOA, har jag främst arbetat med frågan om ZoomX under år 2023. Kraven på digital kommunikation har varit stora sedan första dagarna av pandemin år 2020. Det befintliga verktyget Skype har börjat bli föråldrat och uppdateras inte av leverantören i den takt som behövs. Stockholm stad har nu implementerat en europeisk variant av Zoom kallad ZoomX som är baserad i Tyskland. Verktyget har nu börjat rullas ut i vissa delar av staden under hösten 2023.

En av de risker som uppdagades för år 2022 är delvis släckt under år 2023. Den identidierande risken innebar tidigare att SVOA inte kunde använda digitala tjänster p.g.a stadens inriktningsbeslut om tredjelandsöverföringar. Ett förnyat inriktningsbeslut (KS 2023/241) kom hösten 2023 angående användande av tredjelandsöverföringar. Detta har öppnat upp för att bolaget självt kan fatta beslut i frågorna men med förbehållet att exit-plan behöver finnas på plats. Anledningen till detta är överenskommelsen mellan USA och EU/EES bygger på en så kallad ”President order” och kan rivas upp av en ny amerikansk president efter valet 2024 eller vid en rättslig prövning. Detta ställer i sin

[1] NIS2; Syftet med NIS2-direktivet är att harmonisera de olika medlemsländernas cybersäkerhetskrav och tillämpning av säkerhetsåtgärder samt stärka medlemsländernas samarbete för samhällsviktiga tjänster. NIS2-direktivet fastställer miniminivåer för regelverket och mekanismer för ett effektivt samarbete mellan tillsynsmyndigheterna i varje medlemsland.
[2] Förordningen om digitala marknader; Syftet är att hindra så kallade grindvakter från att bland annat ställa oskäliga villkor för företag och slutanvändare och att säkerställa öppenhet när det gäller viktiga digitala tjänster. EU-kommissionen utsåg i september 2023 för första gången sex grindvakter: Alphabet, Amazon, Apple, ByteDance, Meta och Microsoft. Detta gjorde de med stöd av olika kriterier i DMA som avgör om ett företag är en grindvakt. Efter att ha betecknats som grindvakter har företagen sex månader på sig att följa listan över vad de får göra och inte får göra enligt DMA, så att slutanvändare och företagsanvändare av grindvakternas tjänster får mer valmöjligheter och större frihet.
[3] Dataskyddsförordningen artikel 39.1 a-e

tur höga krav på förvaltningen av informationstillgångar och systemförvaltarna vilket avspeglar sig i de frågor jag får mest av organisationen.

Två planerade granskningar har genomförts av DSO under 2023. Den ena var organisationens dataskydd- och informationssäkerhets- utbildning och kommunikation. Där kan en mycket stor förbättring i antalet deltagare ses under det gågna året. Från 17% till 86% delaktighet. Statistik för dataskyddsutbildningen kan ej inhämtas p.g.a tekniska problem med att ta ut rapporter från utbildningsplattformen. Den andra granskningen var kamerabevakning vilket redovisas i kapitel 3 och som redovisas med inga akuta brister att åtgärda.

Jessica Hillergård
Dataskyddsombud

Innehåll

1. Inledning

1.1. 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. Dataskyddsombudet har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för styrelsen att ta emot de råd och rekommendationer som Dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen. I rapporten får styrelsen insyn i vad Dataskyddsombudets granskningar visat av verksamheten och status avseende integritet och dataskydd. Årsrapporten syftar till att styrelsen ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig styrelsen att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

2. Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som personuppgiftsansvarig, PUA, som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är**:**

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter
- personuppgiftsincidenter

Nedan redogörs för bolagets status och Dataskyddsombudets slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter Dataskyddsombudets genomförda uppföljning och granskning.

2.1. Registerförteckning

2.1.1. Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	123
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nej

2.1.2. Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister eller register av register).

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att PUA får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna om individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete. Man kan styra insatserna där de gör störst nytta.

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamhetens har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

2.1.3. Resultat

Registerförteckningen har under 2023 uppdaterats delvis med de processer som definierats i informationshanteringsplanen men saknar fortfarande systematiskt arbete i form av skrivna rutiner från organisationen och sker helt ad hoc, det vill säga sporadiskt och beroende av en individs egen kunskap och intresse. Målsättningen är att informationsansvarig ska i sin organisation, peka ut

ansvarig medarbetare att hålla personuppgiftsbehandlingen uppdaterad i registerförteckningen, informationssäkerhetsklassa och göra administrativa åtgärder likt se över behörigheter.

Ett arbete med att ta fram en förvaltningsmodell, PM[3], har skett under 2022 och 2023 med utpekade ansvarsroller. Detta för att systematisera och strukturera arbetet med alla sorters information. Därefter kan organisationen påbörja ett mer systematiskt arbete.

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

2.1.4. DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
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

2.1.5. DSO ger råd och rekommendationer till PUA

Rekommendationen kvarstår från tidigare rapporter. När förvaltningsorganisationen är satt behöver respektive informationsägare ombesörja att personuppgiftsbehandlingarna uppdateras. Detta måste ske systematiskt och efter årliga rutiner och bli mindre personberoende vilket det är i dagsläget.

2.2. Styrdokument

2.2.1. Sammanfattning

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

2.2.2. Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

En brist inom detta område bör förstås ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör lyftas fram till PUA. Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till bristande kvalitet i hur verksamheten utför aktiviteterna, men även till att verksamheten slösar värdefulla resurser när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

2.2.3. Resultat

Under 2023 har tillämpningsanvisningen för informationssäkerhet arbetats fram av SVOA och på intranätet Aquanet har instruktioner för ex. hur en medarbetare ska agera vid en personuppgiftsincident. På externwebben har cookie-policyn setts över och uppdaterats.

Tillämpningsanvisningen är inte omhändertagen i rutiner och PM[3]-organisationen saknas vilket leder till ansvarig för uppdateringar inte sker systematiskt.

2.2.4. DSO anger hur allvarliga bristerna är på en skala

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

2.2.5. DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation är att fortsätta arbetet med tillämpningsanvisningen för informationssäkerhet. Nästa steg är att implementera dem i verksamhetens rutiner, bland annat för dataskyddsfrågor. Rutinerna kommer bli tydligare att ta fram när PM[3]-modellen är implementerad.

Under år 2024 behöver kontinuitetsplanerna ses över och vid behov uppdateras. Detta då det från centrala funktioner inom staden identifierats vara en brist i hela staden.

2.3. Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

2.3.1. Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	I verktyget KLASSA 17 I DraftIT 123
Är klassade personuppgiftsbehandlingar aktuella?	JA

2.3.2. Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att en klassning faktisk initieras.

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

Viktigt är också att notera att Dataskyddsombudet omhändertar den registrerades intresse och informationssäkerhetssamordnaren har fokus på verksamhetens krav på informationen i form av tillgänglighet, riktighet och konfidentialitet. Verktyget för DSO är i första hand registerförteckningen och dokumentationen där. Informationssäkerhetssamordnaren har KLASSA som verktyg för att se till att verksamhetens krav efterlevs i form av dokumentation i förvaltningsplaner, systembeskrivningar etc.

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare.

Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll.

2.3.3. Resultat

Det finns 17 registreringar i verktyget KLASSA. Det som KLASSAS är system där det *kan* förekomma personuppgiftsbehandlingar. En minskning mot 2022 då 54 klassningar genomförts. Att färre finns inlagda i KLASSA beror på de låga skyddsvärden som kommit fram under förklassningen.

Under år 2023 har fortsatt arbete skett med förklassningsprotokoll och då i tre steg vilka är: A-klassning i designfasen, B-klassning vid införandet och C-klassning vid årlig uppföljning. Protokollet från dessa ska signeras av informationsägaren och har konkretiserat skyddsvärdet för informationen och då även personuppgifterna som kan ingå i dessa. Dataskyddsombudet har blivit inbjuden till sådana vid flertalet tillfällen och metoden börjar sätta sig i organisationen men sker ad hoc då PM[3] inte är implementerad.

Samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Detta kan vara behörighetsbegränsning, skydd av lösenord på dokument osv. Detta dokumenteras i DraftIT. En klassificeringsstruktur med märkning av dokument finns inte.

2.3.4. DSO anger hur allvarliga bristerna är på en skala

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

2.3.5. DSO ger råd och rekommendationer till PUA

Arbetet med att informationsklassa sker idag efter instruktioner och rutiner men med ett personberoende av systemförvaltare vilka ser till systemet/informationsbäraren och inte informationstillgången som kan flöda genom flera system. Det betyder att systemen klassas var för sig men inte processer vilket ger vita fläckar på kartan över flöden och informationstillgångars skyddsåtgärder.

Det påbörjade informationskartläggningsarbetet inom Avfall som startade under hösten 2023, är en mycket bra strategi för att synliggöra flöden inom hela organisationen. Rekommendationen är att samtliga delar av SVOA genomför samma kartläggning.

2.4. Konsekvensbedömningar

2.4.1. Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	JA
Har alla potentiella högriskbehandlingar konsekvensbedömts?	JA
Är de genomförda bedömningarna aktuella?	JA

2.4.2. Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

2.4.3. Resultat

Organisationen arbetar med konsekvensbedömningar, bland annat som ett verktyg för att få fram krav innan upphandling sker. Arbetet sker gemensamt med andra organisationer i staden men också endast inom SVOA. Rutin finns i projekthandboken.

Under år 2023 har också ett mer gemensamt arbetssätt med andra bolag inom staden genomförts i syfte att konsekvensbedöma kommunikationstjänsten ZoomX. Metoden att arbeta gemensamt förespråkas av tillsynsmyndigheterna inom EU och har lett till tidsvinster och ett mer helhetssynsätt när fler ögon är inblandade och frågeställningar till leverantören blir gemensamma istället för enskilda om samma sak.

Metoden med gemensamma konsekvensbedömningar inom staden har framförts av DSO:er som behov av införande till SLK de senaste åren och förtydligades än mer under 2023. Problematiken är i dagsläget att en tjänst tas fram centralt och därefter lämnas det till varje separat förvaltning och bolag att ta fram en egen konsekvensbedömning och informationsklassning. Detta leder till att alla respektive organisationer har behov att ställa liknande frågor under en längre tid till ex. SLK IKT. Med införandet av ZoomX togs istället en normerande klassning och konsekvensbedömnings-underlag fram centralt av SLK, som sedan endast kompletterades av de enskilda organisationerna utifrån sina respektive uppsättningar av tjänsten och behov.

2.4.4. DSO anger hur allvarliga bristerna är på en skala

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

2.4.5. DSO ger råd och rekommendationer till PUA

Som Dataskyddsombud ger jag rådet att fortsätta det goda arbetet med gemensamma konsekvensbedömningar samt få metoden för gemensamma bedömningar antagen av staden då det sker ad hoc idag, det vill säga det är den enskildes intresse att det görs i enskilda fall utan en fastställd process. Rekommendationen är också att använda verktyget frekvent vid upphandlingar och utbilda/ informera organisationen under 2024 när PM[3] är antaget och rutiner kan tas fram i organisationen.

2.5. Individens rättigheter

2.5.1. Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Kan ej anges då endast nekande registreras enligt Stadsarkivariens gallringsregler.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Inga avvikelser har framkommit

2.5.2. Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

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

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningen krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Intetgritetsskyddsmyndighetens, IMY:s sida, med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

2.5.3. Resultat

Inget att anmärka på då behov av rättning, radering osv. sker direkt enligt rutin i kundtjänst. Inga förfrågningar om registerutdrag har inkommit under året. Det har dock framkommit klagomål vilket redovisas i kapitel 6.1.

2.5.4. DSO anger hur allvarliga bristerna är på en skala

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

2.5.5. DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation är att se över och ytterligare eventuellt vid behov optimera process och rutin för registerutdrag. Samma rekommendation gäller för övriga rättigheter som den registrerade kan vilja utöva. Rutiner och processer behöver sedan kommuniceras med verksamheten för att kunna implementeras om igen.

2.6. Personuppgiftsincidenter

2.6.1. Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom anställda och biträden.
Hur många personuppgiftsincidenter har dokumenterats?	5
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	1

2.6.2. Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter ska de berörda registrerade personerna, utan dröjsmål underrättas.

Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad osv.

2.6.3. Resultat

Under första halvan av år 2023 skedde samtliga identifierade incidenter. Det som är positivt är att trenden med uppmärksam SVOA-personal som också sett andra organisationers incidenter och hjälpt dem se sina brister så att de har kunnat åtgärdas.

En incident anmäldes till IMY, Integritetsskyddsmyndigheten. Den berörde den större incident som rekryteringsföretaget Visma Recryts underleverantör drabbades av under våren. Incidenten uppmärksammades stort i media då flertalet myndigheter och privata bolag drabbades.

2.6.4. DSO anger hur allvarliga bristerna är på en skala

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

2.6.5. DSO ger råd och rekommendationer till PUA

Organisationen är fortsatt bra på att arbeta med incidenter när de sker, men metoden lessons learned är fortfarande inte helt implementerat då arbetet idag inte utgår från processer och flöden utan mer från system. Med PM^3 kommer detta bli tydligare och förbättringsarbetet kommer att bli bättre. Rekommendationen är att ha samverkansgrupp mellan IT, informationssäkerhet, informationsägare och säkerhetsenheten en gång i kvartalet för att följa upp incidenter och se förbättringar. Metoden med en sådan tvärgrupp har visat sig vara av stor nytta i andra organisationer och gemensamma beröringsområden har blivit lättare att samarbeta i.

3. Genomförda granskningar under året

3.1. Sammanfattning

Genomförda granskningar:

- *Granska intern kommunikation och utbildning*
- *Kamerabevakning*

3.2. Syfte

En av Dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

3.3. Genomförda granskningar och deras resultat

Granskning 1 Granska intern kommunikation och utbildning

Granskningen som genomförts är hur utbildning och information om dataskydd skett i organisationen under 2023. En genomgång av utbildningarna har också gjorts och där finns inget att anmärka på faktainnehåll.

Staden har tagit fram flera utbildningar inom informationssäkerhet och dataskydd. Ett av de problem som flaggats av Dataskyddsombuden i staden är brist på möjlighet till uppföljning och att Dataskyddsombudet får ”tjata” på medarbetarna att gå de årliga obligatoriska utbildningarna. Som ett led av ett förbättringsarbete har staden tagit fram en årlig certifiering. Det innebär att det automatiskt sker ett utskick till medarbetarnas mail att de ska genomgå en obligatorisk utbildning. Strax innan sommaren 2023 startade certifieringarna av informationssäkerhet och under hösten certifiering i dataskydd. Dataskyddsombudet har uppmärksammats på att certifieringsutbildningarna infördes utan att HR informerades. Detta är beklagligt och berodde på att inte heller DSO eller Informationssäkerhetssamordnare fick information om införandet. Önskvärt är att det informeras tydligare från centrala funktioner i staden när en sådan förändring sker.

Under år 2022 var siffran på individer som genomgått utbildningen i informationssäkerhet 17 % av medarbetarna. Under 2023 har det ökat till 337 medarbetare av 392 st. möjliga d.v.s. 86 % deltagande. En mycket bra siffra vilket visar på att certifieringen fungerar för denna utbildning. Utbildningen i dataskydd har inte fungerat att ta ut statistikrapporter ifrån.

	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 2 Kamerabevakning

Kamerabevakning är ett område som regleras delvis av dataskyddsförordningen men också kamerabevakningslagen. Stockholm Vatten och Avfall har flera platser där kamerabevakning används. En granskning planerades i rapporten för år 2022. Syftet med granskningen var att:

- Granska om den kamerabevakning som idag genomförs omhändertar dataskyddsförordningen när det behövs.
- Granska att rutinerna för kamerabevakning innefattar dataskyddsförordningen.
- Granska att den information som ges på skyltar och webb ger korrekt information om personuppgiftsansvar etc.

Under 2023 har en ingående översyn av kamerabevakningen inom SVOA skett utifrån Dataskyddsförordningen och de rutiner som berör området. Inget att anmärka framkom vid granskningen och som en del av det systematiska arbetet förbättrades de skriftliga rutinerna.

	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

3.4. DSO ger råd och rekommendationer till PUA

DSO:s råd till personuppgiftsansvarig är att fortsätta uppmuntra utbildning och informationsinsatser. Fördjupade informationsmöten under åren har skett till en väsentlig bättre kunskap som visar sig vid uppmärksammande av fel och brister, incidenter osv.

Under år 2024 ska de uppdaterade rutinerna inom området kamerabevakning följas upp och se om dessa implementerats och om de fungerar som tänkt.

4. Risker inom dataskydd

4.1. Sammanfattning

Relevanta risker inom verksamheten:

- Problematik kring tredjelandsöverföringar likt tjänster som Azure m.fl. (Kvarstående)
- Osäker e-posthantering med personuppgifter (Kvarstående)
- Brist på förvaltningsmodell för information, PM[3] (Kvarstående)

4.2. Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som Dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

4.3. Resultatet av riskkartläggningen

Risk 1 Problematik kring tredjelandsöverföringar likt tjänster som Microsoft Azure m.fl. (Kvarstående)

I Dataskyddsombudets årsrapport för 2022 beskrevs denna risk som större och allvarligare. Förutsättningen för Stadsledningskontorets inriktningsbeslut angående tredjelandsöverföringar innebar att inga överföringar fick ske av personuppgifter till bland annat USA. Detta ledde till inlåsningseffekter och svårigheter för SVOA att delta i flera projekt och samverkansgrupper. Denna risk har nu sänkts då ett nytt inriktningsbeslut togs under hösten 2023. Men, som Dataskyddsombud väljer jag att ha kvar denna risk även i rapporten för 2023.

Bakgrunden till att det i första hand blev olagligt att överföra uppgifter till tredjeland var den ogiltigförklaring av certifieringsmekanismen Privacy Shield som skedde sommaren 2020. Detta gav en inlåsningseffekt som hindrade flertalet digitala tjänster SVOA behövde använda i det dagliga arbetet då leverantörer idag använder sig av molntjänster som finns baserade i USA. Sommaren 2023 kom EU/EES överens med USA om en certifieringsmekanism kallad DPF, Data Privacy Framework, vilket öppnade upp för nya överföringar igen. Men, DPF är inte prövat rättsligt och bygger på en så kallad ”president order”. Det betyder att om DPF prövas i rätten kan det ogiltigförklaras likt som skedde år 2020. Det kan också bli problem vid ett presidentval, vilket sker 2024, då en ny president i USA kan välja att riva upp föregående presidents beslut.

Risken har nu utvecklats till att SVOA kan göra överföringar till tredjeland, men inte utan att ta höjd för att tjänsten inte kan användas med kort varsel pga. att överföringen är olaglig likt år 2020.

	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

Risk 2 Osäker e-posthantering med personuppgifter (Kvarstående)

Varje personuppgift som ska hanteras måste behandlas säkert. När en personuppgift e-postas med någon av stadens leveranser sker själva överföringen krypterat, men är okrypterad i inboxen. Det är också inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras på ett tillräckligt bra sätt. En krypteringstjänst saknas idag.

En gemensam konsekvensbedömning, riskanalys och klassning ska genomföras under 2024 för tjänsten ”Säkra meddelanden” som staden tagit fram. Risken kvarstår då tjänsten inte kunnat implementeras under 2023.

X	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
	Inga brister av nämnvärd betydelse identifierade

Risk 3 Brist på förvaltningsmodell för information, PM³ (Kvarstående)

I tidigare kapitel omnämns att det saknas tydlig förvaltning och modell för informationen inom Stockholm Vatten och Avfall. Stockholm stad har antagit modellen PM³ för detta. Det innebär att det finns tydliga roller fördelade i organisationen med ansvar för att tex. att en kontroll utförs att behörigheter har tagits bort eller tilldelats som de ska. I modellen tar man också höjd för att förutom att riskanalyser och informationsklassningar genomförs systematiskt, omhändertas också ansvaret för vem som ska ombesörja att personuppgiftsbehandlingen är uppdaterad årligen, att Dataskyddsombudet kontaktas vid förändringar osv.

	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

4.4. DSO ger råd och rekommendationer till PUA

I årsrapporten för år 2022 rekommenderade jag styrelsen[4], att diskutera riskaptiten för organisationen vad gäller tredjelandsöverföringar. SVOA behöver digitalisera och utnyttja molntjänster där detta går då det är effektivt och minskar kostnader. För år 2023-års rapports rekommendation vill jag som DSO utveckla mitt råd att driva frågan inom PM³ och utnyttja möjligheten att förhandssamråda med Integritetsskyddsmyndigheten oftare än vad som görs idag.

För risken med brist på säker e-posthantering ger jag rådet att fortsätta invänta de gemensamma aktiviteterna som ska ske i staden. Testning har skett under hösten av SLK och visst grundmaterial

[4] Styrelsen är personuppgiftsansvarig, PUA

finns framtaget. Vid Denna rapports författande kompletteras med tekniska beskrivningar av tjänsten och SKL behöver besätta roller för systemförvaltarorganisationen.

För risken om brist på förvaltningsmodell, PM[3], kan jag som DSO inte annat än fortsatt rekommendera att implementera en sådan. Idag sker arbetet ad hoc då medarbetarna är engagerade, men det är personberoende att aktiviteter sker. Detta blir också tydligt när förändringar behöver ske och kedjan för vem som har ansvar för aktiviteter är otydligt och leder till osäkerheter.

5. Planerade granskningar under det nya verksamhetsåret

5.1. Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *PM³-modellens implementering*
- *Kontinuitetshantering*

5.2. Syfte

Som nämnts tidigare är det granskande arbetet en av Dataskyddsombudets viktigaste uppgifter. Eftersom Dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

5.1. Planerade granskningar

Granskning 1 Förvaltningsmodellen, PM³:s implementering

Syftet med PM³ är att ha utpekade roller och ansvarsfördelning. SVOA har tagit fram en modell som var på remiss under 2023 men ej antagits vid rapportens framtagning. Under implementeringen har jag som DSO för avsikt att granska att dataskyddsfrågan omhändertas korrekt.

Granskning 2 Kontinuitetshantering

I händelse av avbrott i tjänster ska en kontinuitetsplan finnas för att tjänsterna ska kunna återupptas så snart som möjligt, om än eventuellt i begränsad funktion. Den ska innehålla en enkel plan och checklistor med:

- Reservrutin – Hur arbetar vi på alternativa sätt under en störning? Inklusive roller och ansvar.
- Återställningsrutin – Hur återställer vi den kritiska aktiviteten eller resursen efter en störning? Inklusive roller och ansvar.
- Återgångsrutin – Hur återgår vi till ordinarie arbetssätt när den kritiska aktiviteten eller resursen fungerar igen? Inklusive roller och ansvar.
- Nödvändiga kontaktuppgifter – Vilka kontaktuppgifter behövs för att kunna utföra uppgifterna? Vilka behöver informeras om läget, internt och externt?[5]

Ändamålet att granska kontinuitetsplanerna är att ombesörja att dataskyddets krav på säkerhetsåtgärder och de registrerades intressen omhändertas även i kriser.

[5] https://www.msb.se/contentassets/6e1e4b913e734c7eb914374fae577416/fordjupning-om-kontinuitetsplan.pdf (2024-01-04)

6. Övrigt att rapportera

6.1. Klagomål

Ett registrerat klagomål angående dataskydd inkom under mars månad till SVOA. Det berörde samtycke om hanteringen av kakor på extern-webben. Detta eskalerades till systemförvaltningsledare som i sin tur utredde detta skyndsamt med berörd leverantör samt svarade kund.

6.2. Intern arbetsgrupp

Under år 2024 behöver den arbetsgrupp som jobbade internt med dataskyddsfrågor under 2021, startas upp igen. Representanter i denna behöver vara utsedda utifrån förvaltningen av informationsmängderna. Syftet med en sådan grupp är att verksamheten kommer närmare Dataskyddsombudet och informationssäkerhetssamordnaren och ett utbyte av kunskap och behov flödar lättare. Arbetssättet har visat sig vara lyckat i andra verksamheter. Frekvens av möten är minst en gång per kvartal och deltagare bör vara medarbetare med intresse och som har förmåga att informera och utbilda sina kollegor samt fånga upp behov och frågor.

Stockholm Vatten och Avfall är en samhällsbyggare i framkant som driver och utvecklar vatten- och med miljöfokus. Varje dag, året runt förser vi 1,4 miljoner stockholmare med rent och gott kranvatten, renar avloppsvatten och ser till att avfallet tas om hand. Tillsammans med invånare, företag och andra intressenter arbetar vi för att Stockholm ska bli världens mest hållbara stad.

Stockholm Vatten och Avfall
Tel 08-522 120 00
kund@svoa.se
www.svoa.se

En del av Stockholms stad