Verksamhetsstöd

Styrelsen för Stockholm Vatten AB

Dataskyddsombudets Årsrapport 2024 – 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

Agneta Jönsson
Tf Avdelningschef
Verksamhetsstöd

Bilaga: Dataskyddsombudets Årsrapport år 2024 - Stockholm Vatten och Avfall

Dataskyddsombudets Årsrapport år 2024 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 2024 Stockholm Vatten och Avfall. Stockholm Vatten och Avfall AB.
Diarienummer: Diarienummer
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.

År 2024 var året som AI-verktygen började implementeras i IT-tjänster där man minst kunnat ana det tidigare. Den nya lagen om AI, AI förordningen, antogs i EU under våren och kommer implementeras under de kommande åren i olika faser. Ur ett dataskyddsperspektiv blir frågorna än mer intressanta och komplexa i och med att AI:n skapar nya personuppgiftsbehandlingar och med det nya utmaningar. Det är också uppmärksammat att ett antal incidenter har skett i staden under året då nya AI:n implementerats av misstag i olika digitala verktyg vid uppdateringar. En av de granskningar jag prioriterar under 2025 är just AI och medföljande integritetsproblematik.

Samhället har under 2024 påverkats av flera uppmärksammade personuppgifts- och informationssäkerhetsincidenter, bland annat en större ransomware-attack hos TietoEvry i januari. Incidenten skapade stor oro och informationen var otydlig till en början i stadens verksamheter. Turligt nog klarade sig Stockholm stad i den attacken, men andra kommuner drabbades samtidigt mycket hårt.

Ett steg för att ytterligare släcka revisionskontorets tidigare kritik, att dataskyddsombudet är för operativ, har tagits under året. En dokument controller har fått ansvaret att vara kontaktperson och arbeta med registerförteckningen tillsammans med dataskyddsombudet. Det har lett till att registerförteckningen nu uppdateras att följa processer och informationshanteringsanvisningen. I tidigare dataskyddsrapporter har jag som DSO kritiserat att arbetet med registerförteckningen inte fungerar. Med glädje kan jag säga att den bristen är nästan helt släckt. Med andra ord börjar ryggraden, d.v.s. registerförteckningen, komma på plats och resan mot ett systematiskt dataskyddarbete är startad.

En granskning har skett av följsamheten mot de nya informationssäkerhets- och dataskyddskrav som framkommer från verktyget KLASSA. Verktyget KLASSA bygger på ISO27001:2022, vilket är en internationell standard för informationssäkerhet. Granskningen visar på en del brister men var förväntat då den standard som verktyget bygger på har skärpts till från tidigare versioner och utvecklats med nya krav.

En granskning har skett av Stockholm Vatten och Avfalls kamerabevakningen och dess GDPR-dokumentation och att den fungerar i praktiken. Den fick ingen anmärkning och är fortsatt lätt överskådlig.

Under tidigare år har jag uppmuntrat att stadens förvaltningsmodell PM^3 ska implementeras. Detta för att underlätta arbetet och fördela ansvaret för aktiviteter och åtgärder inom dataskydd. Ett av de granskningsområden jag hade under 2024 var införandet av denna. Detta arbete skjuts fram ett år till 2025 på grund av den omorganisation som initierats av Stockholm Vatten och Avfall under 2024.

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?	125
Har nödvändiga uppdateringar gjorts?	Delvis
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

Ett stort positivt steg framåt har tagits med arbetet med registerförteckningen under hösten 2024. En dokument controller med dataskyddsansvar har utsetts. Kontinuerliga arbetsmöten har skett mellan controller och dataskyddsombudet vilket har utvecklat och förbättrat registerförteckningen. En plan har följts för att prioritera arbetet på ett bra sätt. Dataskyddsombudet har med detta blivit granskande

och rådgivande. Tidigare revisioner har kritiserat Stockholm Vatten och Avfall för just detta att dataskyddsombudet varit för operativt och verksamheten inte engagerad.

De brister som kvarstår är att utse ansvariga för respektive personuppgiftsbehandling och ta fram rutin för registerförteckningen.

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

2.1.4. DSO anger hur allvarliga bristerna är på en skala

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

2.1.5. DSO ger råd och rekommendationer till PUA

Rekommendationen är glädjande att fortsätta med den lilla arbetsgruppen bestående av dokument controller och DSO. Detta i syfte att jobba vidare på samma väg som man slagit in på. Nästa steg blir naturligt att utse ansvariga och utbilda dessa, samt ta fram rutin för hur och när de ska kontrollera och eventuellt uppdatera sina personuppgiftsbehandlingar.

2.2. Styrdokument

2.2.1. Sammanfattning

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?	JA

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

En granskning av styrande dokument har skett under året i samband med att en ny uppdaterad standard (ISO27001:2022 Informationssäkerhet) tillkommit vilket informationssäkeretsverktyget KLASSA bygger på. Ett antal brister har identifierats men var förväntat i och med att standarden skärpts och utvecklats inom informationssäkerhet och dataskydd.

Den lokala tillämpningsanvisningen för informationssäkerhet har fastställts av VD i juni 2024. I den finns roller definierade men är än inte implementerade inom organisationen vilket är nästa steg.

I tjänsten Kompassen saknas processer för dataskydd och de rutiner som borde finnas där har fallit bort.

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

Dataskyddsombudet ger rådet att fortsätta förbättra Kompassen med de rutiner som saknas för att det ska bli lätt att hitta information för medarbetarna. Utifrån de brister som framkommit med GAP-analysen behöver även dokument tas fram och befintliga kompletteras utifrån den uppdaterade ISO-standarden. Detta är en naturlig del av ett systematiskt arbete med dataskydd och informationssäkerhet.

Styrelsen får också rådet att fortsätta på inslagen väg med att implementera riktlinjerna i informationssäkerhet vilket inkluderar även dataskyddet. Om inte dataskyddet inkluderas i nästa version behöver en egen lokal tillämpningsanvisning tas fram av organisationen.

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 41 Förklassning 10 st.
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

Under år 2024 har 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 och av personer med intresse då ansvaret inte är helt tydligt än. Med en mer mogen organisation kommer detta bli mindre personbundet.

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.

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.

Det påbörjade arbetet med kartläggning av informationstillgångar på Avfall har fortsatt under 2024 och har lett till en större förståelse för komplexiteten även för mig som dataskyddsombud. Min möjlighet till att få en överblick har underlättats och granskningar kommer bli betydligt lättare i framtiden.

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

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 Stockholm Vatten och Avfall genomför samma form av kartläggning. Utvecklingen av informationsklassningsarbetet är att lyfta blicken från system och se till flöden och processer vilket ger en än bättre syn på sina informationstillgångar och personuppgiftsbehandlingar.

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 Stockholm Vatten och Avfall. Rutin finns i projekthandboken och på Aquanet. Stockholm Vatten och Avfalls bedömning är **GRÖN**.

Ett område som tidigare belysts i årsrapporterna från dataskyddsombudet, är avsaknaden av en process för när det ska ske gemensamma konsekvensbedömningar i staden. Det kan exempelvis bli aktuellt vid en central upphandling av ett IT-system som ska användas av flera organisationer inom staden. Då ingen tydlig process finns angiven från SLK blir det otydligt vem som ska sköta vad och ha ledartröjan i frågorna som uppstår i konsekvensbedömningarna. I dagsläget löser organisationerna ut det ad hoc med upparbetade inofficiella nätverk, men fastnar ofta i slutfaserna då det inte går att färdigställa dokumentationen då riskåtgärder och kravmassa har svårt att omhändertas centralt. En tydlig process ger effektivare, billigare upphandlingar. Det resulterar i en bättre beställarorganisation där organisationens krav på säkerhetsåtgärder och verksamhetens önskemål och behov omhändertas på ett korrektare sätt. Höga och okontrollerade kvarstående risker utan åtgärder kan leda till sanktioner om en konsekvensbedömning inte omhändertas korrekt. Det är också ibland oklart vem som har mandat att fatta beslut om risker vid sådana här gemensamma upphandlingar vilket är en risk. Detta ger en **GUL** bedömning.

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
X	Inga brister av nämnvärd betydelse identifierade

2.4.5. DSO ger råd och rekommendationer till PUA

Styrelsen behöver fortsatt arbeta för att process för gemensamma konsekvensbedömningar i staden implementeras. Organisationen behöver också tydliggöra hur mandatet är fördelat att äga dataskyddsrisker i centrala/ gemensamma upphandlingar då dessa kan leda till sanktioner om de inte omhändertas korrekt.

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 Integritetsskyddsmyndighetens, 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

Rutinerna som tidigare funnits i Kompassen behöver återskapas då det underlättar för organisationen att omhänderta en registrerads rättigheter. Idag ligger ansvaret på dataskyddsombudet att omhänderta en begäran vilket borde istället ligga på en annan funktion.

Medborgare har blivit bättre på att lämna klagomål om personuppgiftsbehandlingar. Dessa redovisas separat i kapitel 6.

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
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	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 publiceras i Kompassen för att 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?	9
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	0

2.6.2. Syfte

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

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

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

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

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

2.6.3. Resultat

Totalt har 9 st. incidenter med personuppgifter anmälts enligt gällande rutiner under år 2024. Organisationens incidenthantering bedöms vara **GRÖN**.

Under året har en ny typ av incidenter uppmärksammats. Detta genom att AI-funktioner har implementerats vid centrala uppdateringar utan föregående konsekvensbedömningar. Risker som uppstått är t.ex. att mötesprotokoll genereras automatiskt med hjälp av ett AI där nya personuppgiftsbehandlingar skapas omedvetet och lagras utan tillräckligt skydd. AI- genererade sammanfattningar och utan kritisk granskning, kan göra att en tidigare harmlös personuppgiftsbehandling med tydlig rättslig grund plötsligt är känslig och olaglig. Tack vare Stockholm Vatten och Avfalls snabba agerande vid upptäckt kunde en av dessa uppdateringar stoppas fort för resten av staden.

Vid uppkomna incidenter som berör flera verksamheter inom hela Stockholm stad under året, har det varit tydligt att det inte fungerar med den CERT-funktion som startats centralt. Ett exempel på detta var den stora TietoEvry incidenten i januari som uppmärksammades i media. Lärdomen är att det blir snabbt ryktesspridning om inte tydlig kommunikation med korrekt, transparent och trovärdig information kommer ut vid en incident. Detta kan leda till att stadsförvaltningen inte kan göra relevanta bedömningar och åtgärder. Detta ger en **GUL** bedömning utifrån det centrala arbetet där organisationen påverkas negativt pga. andra organisationers brister.

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
X	Inga brister av nämnvärd betydelse identifierade

2.6.5. DSO ger råd och rekommendationer till PUA

Styrelsen ges rådet att fortsätta påverka och uppmuntra det centrala arbetet att utveckla CERT-funktionen vid SLK. Detta för att skapa transparent information och tydliga kontaktvägar vid incidenter.

Kunskap om vad och hur man hanterar personuppgiftsincidenter är en färskvara. Det finns en tydlig korrelation mellan att personalen haft utbildning i Dataskyddsförordningen och en ökad benägenhet att anmäla personuppgiftsincidenter.

Styrelsen rekommenderas att ta fram en organisation att omhänderta lessons learned. Det är en naturlig del av det förbättringsarbete som en mer mogen verksamhet kan ta nästa steg emot.

3. Genomförda granskningar under året

3.1. Sammanfattning

Genomförda granskningar:

- *Dokumentation kopplad till uppdaterade standarden ISO27001:2022*
- *Dataskyddsdokumentation för 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

3.3.1. Dokumentation kopplad till uppdaterade standarden ISO27001:2022

När en ISO-standard uppdateras måste dokumentation såsom rutiner, IT-förvaltning, tillämpningsanvisningar etc. uppdateras och nya skapas. En ISO-standard hjälper till att sätta en bästa praxis för vad som är lämpligt att ha för nivå på informationssäkerheten i en organisation. KLASSA-verktyget kommer från SKR, Sveriges Kommuner och Regioner, och hjälper en organisation utifrån en värdering av nivå av konfidentialitet, riktighet och tillgänglighet, fastställa nivåerna på hur höga eller låga dessa krav ska ställas. En god klassificering och genomarbetad KLASSA, ger en kostnadseffektiv och korrektare bedömning av tekniska och organisatoriska åtgärder.

Dataskyddsförordningen ställer egna krav på att det ska finnas tekniska och organisatoriska åtgärder för att skydda integriteten för de registrerade. Dataskyddsombudet får med hjälp av kraven i KLASSA möjlighet att följa upp att åtgärderna är på plats eller inte och av tillräcklig nivå. Hur dessa ska se ut kan skilja sig mot informationssäkerhetskraven vilka utgår från verksamhetens synvinkel.

De organisatoriska kraven som ska finnas inom en verksamhet kan till exempel vara användarregler. Det innebär att det då ska finnas ett dokument kallat användaravtal som den som ska åtkomst till personuppgifter och andra informationstillgångar, ska ta del av och underteckna. Där förklarar organisationen att vill hen använda IT-utrustning och ha behörighet till IT-tjänster, behöver hen följa reglerna och om man bryter mot dem kan hen få påföljder. Regler kan bestå av att inte låna ut hens inloggning till andra, inte använda IT-utrustning för kriminella handlingar, följa regler för lagring av sekretess osv. Underskriften ger en spårbarhet att visa på att reglerna har meddelats den som ska ha access till den.

Granskningen har syftat till att följa upp vilka luckor som finns i förvaltningsmallar för IT och övriga behov som finns i administrativa dokument. Det var väntat att brister skulle finnas då standarden utvecklats inom informationssäkerhet. Kraven inom dataskydd har också utvecklats och förfinats mot tidigare varianter av verktyget KLASSA. En lista av aktiviteter finns framtagen för vad som behöver förbättras.

	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

3.3.2. Dataskyddsdokumentation för kamerabevakning

Under år 2023 uppdaterades rutiner för kamerabevakning och i dataskyddsombudets årsrapport angavs att detta skulle följas upp att de implementerats och fungerade under år 2024. Det har skett vid ett nytt projekt där kamerabevakning skulle införas. Som dataskyddsombud har jag inget att anmärka på.

	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

Rekommendationen som ges till styrelsen av DSO, är att fortsätta förbättra dokumenten så att de når en bra nivå utifrån kraven i KLASSA. Den lista som finns framtagen med aktiviteter behöver tilldelas resurser och prioriteras. Uppdateras dokumenten efter listan åtgärder kommer arbetet med KLASSA för samtliga ansvariga roller underlättas genom att bli mer ekonomiska och mindre resurskrävande.

4. Risker inom dataskydd

4.1. Sammanfattning

Prioriterade risker inom verksamheten:

- Osäker e-posthantering med personuppgifter (Kvarstår)
- Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)
- Tredjelandsöverföringar (Kvarstår)
- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (bolagets) objektförvaltning (Ny)
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Ny)

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.

Under år 2024 har en riskanalys genomförts tillsammans med informationssäkerhetssamordnaren för att hitta gemensamma åtgärder.

Risk beräknas utifrån RISK= Sannolikhet x Konsekvens

Sannolikhet (1 låg - 5 hög):
Låg risk - Inte trolig att inträffa
Hög risk - Kommer med all sannolikhet att inträffa

Konsekvens (1 liten - 5 stor):
Liten konsekvens - Ingen större påverkan
Stor konsekvens - Omfattande, dyrt kan ändra förutsättningarna dramatiskt

Riskvärde
Låg < 4 (riskerna skall bevakas)

Medel 5-14 (riskerna skall hanteras eller elimineras)

Hög > 15 (riskerna skall elimineras)

4.3. Resultatet av riskkartläggningen

Risk 1 Osäker e-posthantering med personuppgifter

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 in- och utboxen. Det är också inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras på ett tillräckligt bra sätt.

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” eller ”TDialog”. Kvarstående aktivitet för verksamheten, är att se över och bedöma vad tjänsten kan användas till.

Jag som DSO kan inte rekommendera i dagsläget att tjänsten används efter att jag tagit del av analysmaterialet. Samtidigt är behovet kvarstående från verksamheten att möjligheten att e-posta personuppgifter säkert och krypterat.

När årsrapporten skrevs 2023 hade projektet med arbetet av dokumentationen för Säkra meddelanden startat på SLK. Detta för att kunna besvara de risker som framkommit inom de verksamheter som gjort ena konsekvensbedömningar och riskanalyser. Work-shops genomfördes sommaren 2024.

Rekommendationen kvarstår att inte använda tjänsten utan att analysmaterialet finns färdigt. Riskerna har inte besvarats av central förvaltning och informationsmängderna som ska skickas i det är så pass känsligt och skyddsvärt.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

Risk 2 Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)

Vid arbete med KLASSA, vilket har varit fokus för bolagen i år, framkommer det att det saknas dokumentation (både gemensam och lokal). Vid förfrågan kan sällan förvaltningsplan, systemdokumentation etc. tas fram av leverantören eller den egna förvaltningen. Denna brist är allvarlig och gemensamma mallar för hur och vad dessa dokument ska innehålla behöver tas fram centralt. Risken är att man idag förutsätter det finns dokumentation för att det ”borde finnas” eller man ”antar” att det är på plats.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

Risk 3 Tredjelandsöverföringar (Ny)

Vid tidigare årsrapporter har risken med tredjelandsöverföringar lyfts upp. Denna risk uppmärksammas så även i år. Detta beror på att flertalet leverantörer av IT-tjänster numera går över till att endast vara molntjänstbaserade och dessa oftast är kopplade till amerikanska företag. Med den nya presidentens tillträde den 20:e januari finns en farhåga att de nuvarande överföringsmekanismerna ska ryckas upp och att det kan finnas integritetsrisker med att använda dessa tjänster.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

Risk 4 Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (bolagets) objektförvaltning (Ny)

Som tidigare nämnt flera kapitel har det uppstått problem i införande av nya tjänster beroende på resursbrist hos central förvaltning. Detta påverkar implementation av nya gemensamma IT-tjänster och det systematiska arbetet som ska ske löpande i den egna lokala organisationen.

	Hög > 15 (riskerna skall elimineras)
X	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

Risk 5 Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Ny)

Under år 2024 växte efterfrågan på AI och möjligheten att effektivisera arbetet. Då området är nytt och så även lagstiftningen behövs tydlig och transparent dokumentation när en sådan tjänst ska införas. Tyvärr brister ofta dokumentationen från leverantörerna och den som upphandlar verktyget behöver utbilda dem genom kravställning och möten.

Integritetsriskerna är stora då effektiviteten och möjligheten att ta fram ”smarta lösningar” tenderar att gå först i hela samhället. Mitt arbete som dataskyddsombud blir då i dessa införanden än mer viktigt att agera ombud och skydda de registrerades intressen.

En del i denna risk är också att nya funktioner införs i redan befintliga tjänster. Ett exempel på detta är en transkriberingstjänst vid digitala möten. Efter mötet är klart kommer direkt ett AI-genererat protokoll med sammanfattning, beslutspunkter och åtgärder. Det låter bra, men frågorna vi måste ställa oss då är vart sammanställdes informationen? Vem kan ta del av den? Hur känsligt blev materialet i det nya formatet? AI är ett oerhört bra och kraftfullt hjälpmedel som vi måste använda medvetet och till rätt saker.

X	Hög > 15 (riskerna skall elimineras)
	Medel 5-14 (riskerna skall hanteras eller elimineras)
	Låg < 4 (riskerna skall bevakas)

4.4. DSO ger råd och rekommendationer till PUA

1. Dataskyddsombudets rekommendation för att minimera risken att personuppgifter e-postas utan tillräckligt skydd, är att de risker som kommit fram under projektet att införa tjänsten ”Säkra meddelanden” åtgärdas.

2. Genom att ta fram, implementera och kommunicera tillämpningsanvisningarna för informationssäkerhet och dataskydd kommer ansvaret bli tydligare för vem som ska ta fram dokumentationen som i dag saknas.

3. Styrelsen rekommenderas att ta höjd för risken och bestämma aptiten för vad man är villig att riskera när man ingår nya avtal med leverantörer där överföringar till tredjeland sker. Rådet är också att ha en tydlig exitplan och genomlysa marknaden i förstahand inom Sverige och EU/EES. Rutiner för att genomföra TIA, Transfer Impact Assessment, behöver också tas fram.

4. Att ge råd om hur den centrala organisationen ska få mer resurs att utföra sitt arbete är svårt. Men, vi kan belysa utifrån Stadsförvaltningens perspektiv att det blir svårt att arbeta effektivt när den brister och det tenderar att byggas flaskhalsar.

5. Som DSO rekommenderar jag att ni fortsätter vara nyfikna på ny teknik och våga satsa på den. Men, rekommendationen är att göra det med stor medvetenhet och arbeta efter den metod som finns framtagen för informationsklassning, riskanalys och konsekvensbedömning. Genvägar blir kostsamma både utifrån sanktioner (både GDPR och AI-förordningen kan ge sanktioner var för sig) men också individens rättigheter får aldrig förminskas eller glömmas bort.

5. Planerade granskningar under det nya verksamhetsåret

5.1. Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *PM³-modellens implementering*
- *Personuppgiftsbiträdesavtal och rutiner för att teckna dessa*

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

Inom Stockholm stad finns en förvaltningsmodell framtagen för att omhänderta arbetet med ansvar och kontroll av informationstillgångar och IT-tjänster. Den kallas PM³. Stockholm Vatten och Avfall har en anpassad modell framtagen att passa denna organisations egna behov. Efter omorganisationen som ska träda ikraft under början av 2025, kommer jag att följa upp att frågorna om ansvaret för dataskydd omhändertas korrekt. Detta för att organisationen ska kunna mogna i sitt arbete med dataskydd och bli mindre individberoende.

Granskning 2 Personuppgiftsbiträdesavtal

Personuppgiftsbiträden är de leverantörer som på olika sätt förvaltar och utför arbetsuppgifter med personuppgifter på uppdrag år personuppgiftsansvarig, Stockholm Vatten och Avfall. För att reglera vad som får ske med personuppgifter som lånas ut till en leverantör, skrivs ett personuppgiftsbiträdesavtal. Då praxis ändrats under åren sedan GDPR infördes 2018, är det nu tid att se över att avtal finns tecknat när det ska finnas, att instruktioner är korrekta och diarieförda. Rutinen och delegationen för personuppgiftsbiträdesavtal ska också granskas.

6. Övrigt att rapportera

6.1. Klagomål

En av den registrerades rättigheter enligt dataskyddsförordningen är rätten att klaga. Den registrerade kan göra det antingen direkt till personuppgiftsansvarig, Stockholm Vatten och Avfall, alternativt till IMY, Integritetsskyddsmyndigheten. Klagomålen som inkommit till Stockholm Vatten och Avfall bottnar främst i missnöje med att betala avgifter och inte själva personuppgiftsbehandlingen som sådan.

6.2. Intern arbetsgrupp

Under år 2025 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