Dataskyddsombudets Årsrapport år 2022 Stockholm Vatten och Avfall

Tillsammans för världens mest hållbara stad

STOCKHOLM VATTEN OCH AVFALL

Författare: Jessica Hillergård, dataskyddsombud@svoa.se
Rapporten citeras: Hillergård, J (2023). Dataskyddsombudets Årsrapport år 2022 Stockholm Vatten och Avfall. Stockholm Vatten och Avfall AB.
Diarienummer: 22MB1536
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.
Under år 2022 har den nya informationssäkerhetsriktlinjen antagits i Stockholm stad. Den i sin tur ska brytas ner i en tillämpningsanvisning för hur Stockholm Vatten och Avfalls arbete ska genomföras. Ett större arbete med olika parter inom organisationen har därför under året arbetat med dessa frågor, där även jag som dataskyddsombud blivit aktuell för rådgivning. Förvaltningsmodellen och framtagna dokument är dock inte antagna och implementerade vid rapportens författande. Utan förvaltningsmodell med ansvar och roller är det svårt att arbeta systematiskt med dataskydd och är den röda tråden i min rapport för år 2022.

I min rapport från år 2021 skrev jag att en pilotutbildning genomförts med mål att fördjupa kunskapen hos medarbetare i informationshantering, informationssäkerhet och dataskydd. Utbildningen har genomförts under sommaren 2022 och det syns direkt en skillnad i de verksamheter som genomfört den. En indikator är att detektionen av personuppgiftsincidenter ökar och frågeställningarna är flera.

En av de större riskerna som jag vill flagga för är tredjelandsöverföringar och den frustration som finns i organisationen att inte kunna delta i samarbeten p.g.a. det inriktningsbeslut som tagits i staden 2022. Ett sådant fall är när organisationen har uppdrag att arbeta med ny lagstiftning. Samordnande organisation för alla intressenter i Sverige använder Teams. Inriktningsbeslutet innebär att SVOA inte kan delta i arbetsrum för att dela dokument, erfarenheter etc. Exemplet visualiserar risken att det i sådana lägen blir ”work-arounds” på eget bevåg för att bara kunna lösa sin arbetsuppgift.

En risk som jag som dataskyddsombud också vill föra upp är bristen på möjlighet att e-posta personuppgifter säkert.

Under året som gått har också en hel del informationsklassningar genomförts i organisationen och systemförvaltare har utbildats i verktyget KLASSA, metodstöd och förklassningsprotokoll. Som dataskyddsombud ser jag positivt på att detta prioriterats, dock vill jag gärna se mindre fokus på system och mer på informationsmängderna. E personuppgiftsbehandling kan resa genom fler system och verktyg, därför behöver även ex. processer informationsklassas.

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?	78
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 finns i dag dokumenterad i DraftIt Records. Den har vissa behov av uppdatering och komplettering. I registerförteckningen dokumenteras vilka system som finns kopplade till respektive personuppgiftsbehandling, vilka som är biträden, mottagare osv.

Det finns i dagsläget ingen fast struktur och nedtecknad rutin för hur uppdateringar och registerförteckningen ska hanteras systematiskt. I dag sker arbete ad hoc och är i beroende av individens initiativ och kunskap.

Ett arbete med att ta fram en förvaltningsmodell har skett under 2022 med utpekade ansvarsroller. Detta för att systematisera och strukturera arbetet med alla sorters information. Beslut har inte tagits om införande av förvaltningsmodell när rapporten skrivs.

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

Kvarstående rekommendation från 2021- Om registret över behandlingar hanteras som en naturlig del i det löpande dataskyddsarbetet, går det smidigare att se över registret och uppdatera när det sker förändringar eller tillkommer nya behandlingar, utan att det växer till ett onödigt stort arbete och upplevs som ett nödvändigt ont.

I en förvaltningsmodell med tydliga roller och ansvarsområden kommer arbetet bli mer systematiserat än idag. Det behöver finnas en rutin som implementeras och kommuniceras i organisationen.

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 år 2022 har Stockholm stad tagit fram och antagit en ny informationssäkerhetsriktlinje och mall för lokal tillämpningsanvisning. Ett större arbete har också skett utifrån att anpassa förvaltningsmodell från riktlinjen och verksamhetens behov samt skapa mallar utifrån ansvar och rutiner inom SVOA. Dessa är inte antagna eller implementerade av/i organisationen.

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
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

2.2.5. DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation är att anta de framtagna styrdokumenten och implementera dessa i 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 54 I DraftIT 78
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 54 registreringar i verktyget KLASSA. Det som KLASSAS är system där det *kan* förekomma personuppgiftsbehandlingar.

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.

Under år 2022 har också ett arbete skett då förklassningsprotokoll har börjat användas innan en fullständig informationsklassning sker. I det protokollet tas stor hänsyn till personuppgifter och vilken kategori de faller under. En särskild bedömning görs också utifrån hur individen påverkas om konfidentialitet, riktighet eller tillgänglighet brister.

En metod med anvisning för att informationsklassificering finns framtagen men behöver antas och implementeras i organisationen.

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. Det betyder att systemen klassas men inte processer.

Dataskyddsombudets råd är att implementera förvaltningsmodell och anta de dokument som tagits fram, bland annat anvisning för informationsklassificering.

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.

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
	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

Dataskyddsombudets råd är att under året påminna om kraften i det verktyg som konsekvensbedömningen bidrar med. Ett systematiskt arbete med det underlättar upphandling, avtalsskrivning, förvaltning och kravställning.

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

Verksamhetsutvecklingens enhet Informationshantering har arbetat med att uppdatera processen och förbättra rutiner för den registrerades rättigheter under år 2022. Detta var också ett av de områden som dataskyddsombudet granskade under samma år. Förbättringar gjordes genom att ta fram tydligare rutin och mall för registerutdrag. Processbeskrivningen i Kompassen uppdaterades och förtydligades.

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.

2.6. Personuppgiftsincidenter

2.6.1. Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom att en anställd i annan del av Stockholm stad alt. internt uppmärksammar incidenten.
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

Under året som gått kan man se en ökning av personuppgiftsincidenter. Detta är en positiv utveckling mot tidigare år och som pekar på en större medvetenhet. Ett större antal medarbetare har fått fördjupad träning inom informationssäkerhet, dataskydd och informationshantering och ökningen kan

ses korrelera med dessa utbildningstillfällen. Se också granskning i kap. 3 punkten ”*Granska intern kommunikation och utbildning”*.

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
	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

Dataskyddsombudets rekommendation under 2023 är att se över och förbättra efterarbetet med personuppgiftsincidenter. Det vill säga när incidenten är upptäckt och utredd, hur omhändertar man då kunskapen man lärt av den? Syftet med att anmäla en personuppgiftsincident är att förbättra verksamhetens arbete med dataskyddsfrågor och de eventuella risker som finns för den registrerade.

Då de fördjupade utbildningarna har visat sig vara mycket bra för benägenheten att uppmärksamma och anmäla personuppgiftsincidenter, rekommenderas att flera får delta i dessa och repetitionsmöjlighet ges till de som behöver.

3. Genomförda granskningar under året

3.1. Sammanfattning

Genomförda granskningar:

- *Granska intern kommunikation och utbildning*
- *Fungerar processerna för att hantera de registrerades rättigheter*

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 2022. Fokus har lagts på dels den fördjupade utbildning som togs fram och omnämndes i årsrapporten för dataskydd 2021, då kallad pilotutbildning, samt den digitala utbildning som är obligatorisk för alla anställda inom Stockholm stad och som finns på Utbildningsplattformen.

Fördjupad utbildning

Den fördjupade utbildningen har haft uppdelning i flera block med informationssäkerhet, dataskydd och informationshantering. Ett tillfälle har varit uppdelat i flera pass och har avslutats med en övningsdel där frågor har lyfts som berört vanligt uppkommande situationer och diskussion kring dessa. Återkopplingen efter dessa har varit positiva och en ökning av frågor samt anmälda personuppgiftsincidenter kan ses direkt i samband med dem.

Obligatorisk digital utbildning i dataskydd

Dataskyddsombudet har genomfört och granskat utbildningen som är obligatorisk att gå årligen för alla anställda inom Stockholm stad. Den håller en bra kvalitet och är lätt att förstå.

För Stockholm Vatten och Avfall är det endast 17% som genomfört utbildningen.

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

Granskning 2 Fungerar processerna för att hantera de registrerades rättigheter

Verksamhetsutvecklingens enhet Informationshantering har arbetat med att uppdatera processen och förbättra rutiner för den registrerades rättigheter under år 2022. Detta var också ett av de områden som dataskyddsombudet granskade under samma år. Förbättringar gjordes genom att ta fram tydligare rutin och mall för registerutdrag. Processbeskrivningen i Kompassen uppdaterades och förtydligades.

	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

Dataskyddsombudet rekommenderar att en tydlig kompetensplan sätts för området dataskydd. Det finns en tydlig korrelation mellan kunskap och exempelvis att anmäla personuppgiftsincidenter.

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.

4. Risker inom dataskydd

4.1. Sammanfattning

Relevanta risker inom verksamheten:

- Problematik kring tredjelandsöverföringar likt tjänster som Azure m.fl.
- Osäker e-posthantering med personuppgifter

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 Azure m.fl.

Enligt stadens inriktningsbeslut om tredjelandsöverföringar, finns en stor problematik att använda molntjänster då risk för överföringar av personuppgifter utanför EU/EES kan ske. Då flertalet leverantörer idag använder sig av molntjänster är det stor risk att ett sådant informationsutbyte kan ske. En ökad efterfrågan finns också från verksamheten att kunna använda fler molntjänster då den digitala utvecklingen går mot det hållet i samhället.

Stockholm Vatten och avfall har flera samarbetspartners i Sverige. Frågan om att använda Teams har åter väckts upp innan årsskiftet 2022/2023 och var senast aktuell under samma tid två år tidigare. Då beslutade Stadsledningskontoret efter ett samråd med IMY, Integritetsskyddsmyndigheten, att det inte var säkert att använda tjänsten med de tillgängliga skyddsmekanismer som fanns tillgängliga vid dem tidpunkten.

Den risk som jag som dataskyddsombud ser, är att det blir mer och mer svårarbetat för verksamheten att arbeta endast on-prem. Risken är att det blir egna lösningar som går under radarn för att det är för krångligt att efterleva den strikta inriktningen som finns idag. Det är också svårt för samarbeten och den digitala utvecklingen stagnerar.

Ett exempel som är värt är belysa är organisationen Avfall Sverige som är kommunernas branschorganisation inom avfallshantering. De är en organisation som kommuner kan ansluta sig till för att samverka i frågor rörande avfall och återvinning. De skriver *”Regeringen beslutade sommaren 2022 om förändringar i förordningen om producentansvar för förpackningar. Det är en stor reform som innebär att kommunerna står inför ett omfattande förändringsarbete med många viktiga beslut att fatta och det under mycket kort tid. Redan 1:a januari 2024 får kommunerna själva ansvar för insamling av förpackningar från hushåll inom fastighetsnära insamling eller lättillgängliga platser samtidigt som kommunen ska erbjuda separat insamling av matavfall från hushåll. Därefter sker en eskalering av fler åtgärder enligt den nya förordningen fram till 2027. Förordningsförändringen innebär i korthet att kommunerna på mycket kort tid måste bygga upp en infrastruktur för insamling av förpackningsavfall fastighetsnära från hushåll och samlokaliserade verksamheter, tillsammans*

med mat- och restavfall"[1]. Med en sådan stor och snabb förändring behöver Stockholm Vatten och Avfall delta i samarbeten för att kunna hålla jämn takt och dra nytta och dela med sig av egna och andras erfarenheter. Avfall Sverige har det samordnade ansvaret och håller ihop det genom kommunikationsplattformen Teams. Där delas både information, diskussioner osv. Det inriktningsbeslut som nu tagits för staden i januari 2022 innebär att Stockholm Vatten och Avfall inte kan delta i denna samverkan.

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 2 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 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.

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 styrmodell för information

I tidigare kapitel omnämns att det saknas tydlig förvaltning och modell för informationen inom Stockholm Vatten och Avfall. Stockholm stad har antagit modellen PM[3] 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 förvaltningsmodellen 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

[1] https://www.avfallsverige.se/for-medlemmar/forpackningsinsamling/ (2023-01-23)

	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

Som dataskyddsombud lägger jag mycket tid på rådgivning vid skrivande av personuppgiftsbiträdesavtal. Ett återkommande problem är tredjelandsöverföringar hos leverantörer. Detta taktar inte med det inriktningsbeslut om tredjelandsöverföringar som tagits av Stadsledningskontoret i januari 2022. Som dataskyddsombud rekommenderar jag att fastställa bolagets riksaptit i frågan. Det vill säga, vad är man villig att acceptera innan man sätter in en motåtgärd för att reducera risken med tredjelandsöverföring. Som en del av arbetet med att fastställa detta, behöver det säkerställas att rutin finns för att göra TIA- Transfer Impact Assessment när det är aktuellt med molntjänster. Detta för att skapa bättre kravmassor för upphandlingar på leverantörer av tjänster. Det behöver också göras en ny analys vad och vilka personuppgifter som kan acceptareas att de förs över till tredjeland och med vilket skydd.

För att kunna skicka personuppgifter säkert behöver tjänsten ”Säkra meddelanden” eller liknande utvärderas och sedan införas. Innan införande kan ske behöver aktiviteter såsom informationssäkerhetsklassning i verktyget KLASSA, konsekvensbedömning och riskanalys genomföras.

Dataskyddsombudet rekommenderar också att en förvaltningsmodell likt PM[3] implementeras i verksamheten.

5. Planerade granskningar under det nya verksamhetsåret

5.1. Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granska intern kommunikation och utbildning*
- *Dataskyddsförordningen och kamerabevakning*

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 Granska intern kommunikation och utbildning

Det är avgörande att för ett gott dataskydd att det finns en tillräcklig medvetenhet och kunskap inom organisationen om hur personuppgifter får och ska hanteras. Alla personer som hanterar personuppgifter, och de som bestämmer hur de ska hanteras, måste få en adekvat utbildning. Det är viktigt att utbildningen är aktuell och hålls uppdaterad. Förutom de grundläggande kunskaperna om begrepp, principer m.m. som alla behöver, finns det vissa grupper som därutöver kan behöva mer riktade utbildningsinsatser som ger djupare kunskaper.

- Granska rutinerna för grundläggande utbildning till anställda och introduktion till nyanställda
- Granska genomförda gemensamma utbildningsinsatser och sammanställ om möjligt statistik
- Granska grundutbildningens innehåll och säkerställ att den är aktuell

Granskning 2 Dataskyddsförordningen och kamerabevakning

Kamerabevakning är ett område som regleras av dels dataskyddsförordningen, dels den svenska kamerabevakningslagen. Stockholm Vatten och Avfall har flera platser där kamerabevakning används. En granskning kommer genomföras under 2023 för att säkerställa 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.

6. Övrigt att rapportera

6.1. Sammanfattning

Under år 2023 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.

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

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

En del av Stockholms stad