GDPR, Årsrapport 2020

Dataskyddsombudet

Tillsammans för världens mest hållbara stad

STOCKHOLM VATTEN OCH AVFALL

Författare: Jessica Hillergård, Dataskyddsombud@svoa.se
Rapporten citeras: Hillergård J (2021). GDPR Årsrapport 2020 Stockholm Vatten och Avfall AB.
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 för 2020.

Vid årsskiftet 2019-2020 bestämde SVOA att anlita ett externt Dataskyddsombud. Vid uppstarten av uppdraget som DSO, gjordes en GAP-analys av bolagens mognadsgrad och behov. Ett implementationsprojekt startades parallellt för att uppdatera inventering av personuppgifter. I mars/april 2020 gick SVOA liksom andra bolag in i krisorganisation med fokus mot att upprätthålla de samhällsviktiga tjänster man utför. Delar av det inventeringsarbete och aktiviteter som innefattar fysiska möten har därför skjutits fram till 2021.

År 2020 har varit ett utmanande år för hela samhället och har inte lämnat någon utan påverkan. På grund av den pågående pandemin fick aktiviteter inom dataskyddsområdet skjutas upp. Men, desto flera har lyckats att genomföras. Några av de milstolpar som nåtts är: konsekvensbedömningar inför upphandling, överföring av registerförteckningen till det digitala verktyget DraftIT, samverkan mellan närliggande funktioner inom informationshantering, uppstart av styrgrupp för GDPR är för att nämna några goda framsteg.

SVOA som organisation har kommit en bit på väg med implementationen av GDPR och har en relativt god nivå av kunskap hos vissa nyckelpersoner, men behöver jobba på att få in det i *alla* delar av arbetet med personuppgifter- från ledning och styrelse till kundtjänst och HR.

Därför är nu min rekommendation att:

1. prioritera utbildning av personal,
2. uppdatera inventering av registerförteckningen (3 år gammal)
3. utse ägare till de olika personuppgiftsbehandlingarna så att dessa hålls uppdaterade systematiskt
4. följa de aktiviteter som GDPR-årshjulet anger

Jessica Hillergård
Dataskyddsombud

Innehållsförteckning

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. DSO:n 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 nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt Dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Vid årsskiftet 2019-2020 bestämde SVOA att anlita ett externt Dataskyddsombud. Vid uppstarten av uppdraget som DSO gjordes en GAP-analys av bolagens mognadsgrad och behov. Ett implementationsprojekt startades parallellt för att uppdatera inventering av personuppgifter etc. I mars 2020 gick SVOA liksom andra bolag in i krisorganisation med fokus mot att upprätthålla de samhällsviktiga tjänster man utför. Delar av det inventeringsarbete och aktiviteter som innefattar fysiska möten har därför skjutits fram till 2021.

2. Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig 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 DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

2.1. Registerförteckning

2.1.1. Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	73
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 personuppgiftsansvarig får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

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

Syftet med detta rapporteringsområde är således att rapportera till personuppgiftsansvarig 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 personuppgiftsansvarig behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

2.1.3. Resultat

Registerförteckningen i finns i ett digitalt verktyg kallat DraftIt och består av ett frågeformulär per personuppgiftsbehandling vilket i sin tur blir funktionen av en checklista att alla krav i GDPR dokumenteras korrekt. SLK har beslutat under år 2019 att de tidigare Excel-listor med registerförteckningar som skapades 2018, ska digitaliseras i verktyget DraftIT. När extern DSO utsågs 2020 fördes den befintliga Excel-filen över till DraftIT. Då framkom kunskapsluckor om personuppgiftsbehandlingarna. Detta då den initiala Excel-listan inte var så utförlig jämfört mot de tillkomna krav som vuxit fram på dokumentation sedan GDPR:s införande i maj 2018.

Totalt har 73 behandlingar registrerats i DraftIT. Det finns åtgärder upplagda för delar av de personuppgiftsbehandlingar som behöver kompletteras, kontrolleras eller på annat sätt bearbetas vilket finns dokumenterat i verktygets kommentarsfält. Detta kan bestå i att det saknas information om säkerheten, vem som är ansvarig för personuppgiftsbehandlingen, information till den registrerade, personuppgiftsbiträdesavtal korrekt, tredjelandsöverföringar eller inte osv. Vid den inventering som ska ske 2021 kommer dessa kunskapsluckor att fyllas på enligt plan.

Registerförteckningen är upprättad av en konsult inför GDPR:s införande i maj 2018. Efter detta har registerförteckningen varit ett vilande dokument som återupptogs 2020 i och med överföring från Excel till DraftIT.

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:s bedömning av mognadsgraden av registerförteckningen inom SVOA

Värde	Beskrivning
0	Registerförteckning/ arbetet/ rutin med denna saknas
1	Registerförteckning finns och är beroende av enskilda individers kunskap, ad hoc lösningar är dominerande
2	Registerförteckning finns och är beroende av enskilda individers kunskap, rutin finns men är under implementering.
3	Registerförteckningen och rutin är implementerad med utpekat ansvar för resp personuppgiftsbehandling. Stöd för verksamheten med DraftIT.
4	Registerförteckning och rutin finns och följer årshjulet. Ägare av de olika personuppgiftsbehandlingarna hanterar DraftIT självständigt.
5	Registerförteckningen är fullt implementerad och tillämpas enligt rutin. DSO kan granska efter årshjulet och åtgärder sker systematiskt.

Under 2021 är således målbilden att nå mognadsgrad 3 med ambition att nå 4.

2.1.6. DSO ger råd och rekommendationer till personuppgiftsansvarig

Då det saknas ansvarig person för varje personuppgiftsbehandling som de facto utför dem i organisationen, behöver en sådan rutin och person införas hos SVOA. Idag ligger ansvaret på informationsansvariga vilket inte blir tillräckligt detaljerat då dessa saknar nödvändig kunskap om personuppgiftsbehandlingar på den nivå som behövs. Den person som kan bli aktuell för uppdraget är t.ex. en administratör eller controller som kan beskrivas som ”spindeln i nätet”.

Rådet från DSO betyder att utvalda personer inom SVOA behöver utbildas i verktyget DraftIT för att få förståelse om frågeställningarna i GDPR. Dessa personer ska fungera som GDPR-ambassadörer och verka som kontaktpersoner vid de årliga genomgångarna av personuppgiftsbehandlingarna enligt årshjulet. GDPR-ambassadörerna ska kunna vid behov lägga till nya personuppgiftsbehandlingar, alternativt kontakta DSO för stöd med inläggningen i verktyget DraftIT.

På detta sätt kommer arbetet med Dataskyddsförordningen bli mer systematiserat och framförallt dokumenterat inom organisationen.

2.2. Styrdokument

2.2.1. Sammanfattning

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

2.2.2. Syfte

Området syftar till att personuppgiftsansvarig genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar personuppgiftsansvarig 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 personuppgiftsansvarig. 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 personuppgiftsansvarigs intresse att förstå för att fatta rätt beslut om.

2.2.3. Resultat

Dokument och information finns att tillgå på Aquanet för personalen på SVOA. Dessa behöver under 2021 ses över och uppdateras. DSO har ej haft access till Aquanet under 2020.

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 personuppgiftsansvarig

DSO:s rekommendation är att se över Aquanet och tillgängligheten för GDPR-informationen. Detta behöver göras efter att den uppdaterats och kompletterats med ny information som framkommit sedan införandet 2018.

Eftersom flera av styrdokumenten omfattar både dataskydd och informationssäkerhet bör DSO resonera med informationssäkerhetssamordnare i bedömningar och förslag på åtgärder framåt för nästa verksamhetsår. Detta finns nu inlagt som aktivitet i årshjulet för 2021.

På samarbetsyta finns flera dokument och mallar med instruktioner. Dessa behöver bli antagna, kommunicerade och flyttade till Aquanet för att göras tillgängliga.

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?	36 i KLASSA Samtliga personuppgifts-behandlingar är klassade utifrån GDPR och finns dokumenterade i DraftIT.
Är klassade personuppgiftsbehandlingar aktuella?	NEJ (KLASSA) JA (Enl GDPR)

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 personuppgiftsansvarig 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.

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

SVOA har en tradition att arbeta med KLASSA som verktyg och har utbildningar två gånger/månad med nyanställd personal och konsulter om informationssäkerhet och informationsklassificering utifrån verksamhetens lagstiftningar såsom säkerhetsskyddslagen och OSL. Varje informationsägare är ansvarig för att systemen ska KLASSA:s.

KLASSA har vidareutvecklats som verktyg och GDPR har blivit ett obligatoriskt segment med uppmaningen att kontakta DSO om det framkommer att det finns personuppgifter. Detta underlättar också för DSO:s arbete att få löpande information om KLASSA- aktiviteter och eventuella behov om konsekvensbedömning behöver utföras. Ny process arbetas fram med upphandling genom att det ska lyftas in som en del av deras process vid ny införskaffning av system för att få tydligare krav.

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

2.3.5. DSO ger råd och rekommendationer till personuppgiftsansvarig

När personuppgiftsbehandlingarna inventerats och progressen med ”GDPR-ambassadörer” utsetts är nästa naturliga steg att dessa också kan KLASSA:s för de system som är aktuella för detta. DSO:s rekommendation är att detta följs upp och påbörjas när inventering av personuppgifter är klar.

2.4. Konsekvensbedömningar

2.4.1. Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	NEJ
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Kan ej anges
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

Under 2020 har en rutin för konsekvensbedömningar prövats fram i organisationen och börjar nu bli mogen att definieras i Kompassen som en process. Utav de konsekvensbedömningar som genomförts har en bedömts behöva prövas av IMY Integritetsskyddsmyndigheten i ett så kallat förhandssamråd och berör den Stadsgemensamma upphandlingen av Elektroniska körjournaler med ISA-funktion. Konsekvensbedömning har också gjorts som ett steg i en upphandling för att fånga upp GDPR-krav inför införskaffning av nytt HR-system och i diskussionen kring att kunna använda Teams i O365.

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 personuppgiftsansvarig

Då SVOA har ett pågående arbete med att definiera processer i organisationen som sedan ska publiceras i verktyget Kompassen, är DSO:s råd att koppla in konsekvensbedömning som en stödprocess.

Delegation för vem som ska representera personuppgiftsansvarig och ha mandat att godkänna respektive avslå åtgärder, kvarstående risker och DSO:s råd behöver omhändertas i den nya delegationsordningen.

2.5. Individens rättigheter

2.5.1. Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	N/A

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 personuppgiftsansvarig 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

Under 2020 har inga begäran om registerutdrag skett. I verktyget Kompassen kommer under 2021 en process med stöd visualisera hur individens rättigheter ska omhändertas när den vill utöva den. Idag sker detta ad hoc. En person har begärt att tas bort från register då hen fått felaktig information via SMS. Detta skedde enligt den rutin som finns anslagen på SVOA:s hemsida och fungerade tillfyllest.

Viktigt att poängtera är att *inga positiva besked* om radering, begränsning, registerutdrag etc. diarieförs efter Stadsarkivets beslut. Det är *endast nekande besked* som diarieförs. Detta innebär att det behöver föras statistik parallellt för att dessa siffror ska kunna presenteras årligen.

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 personuppgiftsansvarig

Den process för att individens rättigheter ska kunna nyttjas av den registrerade, behöver när den är färdig, kommuniceras med de avdelningar som kan bli aktuella för detta. Checklistor bör finnas med processen för att ge stöd åt personalen och tas fram i samarbetet för informationshanteringsnätverket.

2.6. Personuppgiftsincidenter

2.6.1. Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	0
Hur många personuppgiftsincidenter har dokumenterats?	0
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 Dataskyddsförordningen 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, Integritetsskyddsmyndigheten, 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

SVOA som organisation har en god förmåga att rapportera *säkerhetsincidenter* i verksamheten som är att förse Stockholmare med vatten och avfallshantering. Inga personuppgiftsincider finns dock anmälda under 2020 och *är en brist.* DSO:s analys är att det troligen saknas förståelse för vad en personuppgiftsincident verkligen är vilket höjer nivån till en allvarlig brist.

2.6.4. DSO anger hur allvarliga bristerna är på en skala

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

2.6.5. DSO ger råd och rekommendationer till personuppgiftsansvarig

DSO uppmanar SVOA att författa en personuppgiftsincidenthanterings rutin som kommuniceras brett omgående samt att information/utbildning på Aquanet sker löpande. Utbildning kan ske av DSO och övriga medlemmar av informationsnätverket inom SVOA. (Se också kapitel 4.)

3. Genomförda granskningar under året

3.1. Sammanfattning

Genomförda granskningar:

- *Dokumentation och skriftliga rutiner*
- *Registerförteckning*
- *GDPR-organisationen*

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 Dokumentation och skriftliga rutiner

Vid den inledande GAP-analysen vid årsskiftet 2019/2020 identifierades ett problem med avsaknad av dokumentation. Det finns information på Aquanet för personal att ta del av men som inte uppdateras löpande. Nya dokument har tagits fram med rutiner. Dessa har dock inte kommunicerats på önskvärt sätt p.g.a. pandemiläget då verksamheten fått prioritera andra samhällskritiska arbetsuppgifter.

DSO har själv upprättat logg för personuppgiftsincidenter och händelser samt för att kunna följa de förbättringar som kan föreslås för organisationen att uppnå en högre mognadsgrad, d.v.s. GDPR ska vara en del av det vardagliga arbetet.

Granskning 2 Registerförteckning

Se kapitel 2.1

Granskning 3 GDPR-organisation

Den inledande GAP-analysen gav vid handen att det saknades en GDPR-organisation inom SVOA, merparten av det arbete som skedde var individers eget initiativ och inte systematiskt. Detta ledde till flera åtgärder av organisationen efter råd av DSO, vilket resulterade i att en styrgrupp för GDPR inrättades med Informationsägarna, Informationssäkerhetssamordnaren, Säkerhetschef och IT-chef. Syftet är att få ut lagstiftningen som en del av de ordinarie arbetsuppgifterna.

3.4. DSO ger råd och rekommendationer till personuppgiftsansvarig

De råd som DSO vill ge personuppgiftsansvarig efter granskningen 2020 är följande:

- Dokumentation och rutiner behöver kommuniceras under 2021 till personalen på en bredare front.
- Fortsätta utveckla GDPR-organisationens arbete. Med endast ett fåtal möten sattes GDPR in i ett större perspektiv och har lyfts in i flera sammanhang än tidigare. En bra vägvisare att det är rätt väg för SVOA att gå.

4. Risker inom dataskydd

4.1. Sammanfattning

Relevant risk inom verksamheten:

- ***Brist på kunskap/ utbildning om Dataskyddsförordningen/ GDPR***

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 Brist på kunskap/ Utbildning om Dataskyddsförordningen/ GDPR

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

4.4. DSO ger råd och rekommendationer till personuppgiftsansvarig

Vid GAP-analysen 2020 framkom att SVOA inte hade fått ut GDPR i hela organisationen. Detta genomsyras i alla granskningsområden där risken blir tydlig och mognadsgraden är låg, d.v.s. det finns inga fasta rutiner men det finns ad hoc lösningar och engagerad personal som kan lösa ut det. Den riskreducerande åtgärden är att utbilda personalen i GDPR och hur efterlevnad ska ske. Finns en medvetenhet om vad en personuppgiftsincident är kommer också sådana att identifieras, förstår man vikten av att göra en konsekvensbedömning och tänka till före blir också detta ett kraftfullt verktyg som sparar tid och pengar.

5. Planerade granskningar under det nya verksamhetsåret

5.1. Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Personuppgiftsbiträden (2 st)*
- *Efterlevnad av Schrems II-domen*

5.2. Syfte

Avsikten med att välja ut två områden för granskning är för att kunna planera och avsätta tid för detta under det kommande året. Att granska två personuppgiftsbiträden är också ett av de mål som tagits fram under 2020 då det är både relevant för granskning, möjligt att mäta och en del av Dataskyddsombudets arbetsuppgift.

5.3. Planerade granskningar

Granskning 1

SVOA har ett flera personuppgiftsbiträden inom verksamhetens olika områden. För att kontrollera att de uppfyller PUB-avtalen väljs 2 st. ut för att granskas med skriftliga frågor under våren 2021. Dessa kommer sedan att redovisas till personuppgiftsansvarig i juni 2021 i separat rapport.

Den metod som ska användas är ett skriftligt formulär med frågor till de personuppgiftsbiträden som valts ut. I personuppgiftsbiträdets avtal ska det finnas inskrivet att de ska underkasta sig en sådan granskning. (Vid behov kan även deras lokaler granskas men pga. pågående pandemi begränsas denna granskning under 2021.)

Granskning 2

I juli 2020 föll en dom i EU-domstolen kallad Schrems II som innebär att tredjelandsöverföringar som hänvisar till Privacy Shield inte längre är möjliga att genomföra. Under 2021 ska detta vara fokusområde för DSO att granska samt informera P personuppgiftsansvarigs representanter, ledning och personalen inom SVOA.

Granskningen kommer ske genom att:

- Kartlägga leverantörer, tjänster vid personuppgiftsinventering och inhämta PUB-avtal med instruktioner (Inventeringsprojekt)
- Identifiera genom PUB-avtalens instruktioner vilka som har tredjelandsöverföringar till USA/tredjeland (DSO)
- Frågeställningar om oklarheter om överföringar (Informationsägaren)
- Riskvärdering och Analys (DSO och informationsägaren)

När granskningen är genomförd kan beslut slutligen fattas om eventuella riskreducerande åtgärder och/ eller om personuppgiftsbehandlingen kan fortgå med en anmälan till IMY Integritetsskyddsmyndigheten.

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