Stockholms stad

Bilaga 10

Årsrapport GDPR

2022

Skärholmens stadsdelsnämnd

GDPR årsrapport
Januari 2023

Dnr: SKHLM 2023/42
Utgivningsdatum: 2023-01-24
Kontaktperson: Maria Nilsson

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.

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Vid årsskiftet 2021/2022 lämnade dåvarande DSO Sabina Toromanovic sitt uppdrag. Hon ersattes av Maria Nilsson, som också är författaren till denna årsrapport.

För Skärholmens del har året dominerats av arbetet med att kartlägga och komplettera förteckningar över informationstillgångar samt arbetet med att uppdatera registerförteckningen och delegationsordningen.

Under året som gått har Skärholmens stadsdelsförvaltning arbetat mycket aktivt med frågorna inom dataskydd och informationssäkerhet. Rollen informationssäkerhetssamordnare, ISAM, har reviderats och flyttats till enheten för HR och internt skydd.

Skärholmens stadsdelsförvaltning har haft 14 st. personuppgiftsincidenter under året, dock har ingen bedömts vara så allvarlig att den anmälts till IMY, Integritetsskyddsmyndigheten.

Som DSO är mina huvudsakliga rekommendationer inför 2023 följande:

- Bli bättre på att involvera förvaltningens DSO och informationssäkerhetssamordnare i samband med upphandling av tjänster och system.

- Förstå vikten av konsekvensbedömning av personuppgiftsbehandlingar samt utse vem som ska hålla i konsekvensbedömningar.

- Fortsätt arbetet med registerförteckningen.

- En uppföljning av kunskapsläget inom dataskydd och informationssäkerhet behöver göras, samt repetition av de digitala utbildningarna på utbildningsplattformen.

- Nästa år planerar de europeiska dataskyddsmyndigheterna att granska dataskyddsombudens roll och ställning. Ett mycket välkommet initiativ som förhoppningsvis kommer att underlätta såväl för den som innehar rollen som DSO

som den verksamhet DSO är satt att granska. Följ det arbetet noggrant!

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som Dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens status och DSO:s slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:s genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	707
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Delvis

3.1.2 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).

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 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.

3.1.3 Resultat

Registerförteckningen finns i ett digitalt verktyg kallat DraftIt och består av ett frågeformulär per personuppgiftsbehandling vilket i sin tur blir en checklista för att stämma av att alla krav i GDPR hanteras och dokumenteras korrekt. I föregående års årsrapport för Skärholmens stadsdelsnämnd uppgavs att det fanns 1980 behandlingar registrerade i DraftIt. Under året har fokus i arbetet med dataskydd framför allt varit att uppdatera och bygga om modulen för Skärholmen i syfte att förenkla det dagliga arbetet med dataskyddsfrågor. I syfte att skapa en lättare överblick byggdes formulären om och är nu enbart ett per avdelning. Under arbetet med översynen av behandlingarna i DraftIt framkom även att många registreringar låg dubbelt, ibland tredubbelt. Avdelningarna har under året aktivt sett över sina registreringar och raderat inaktuella och/eller dubbletter. Nu finns 707 registreringar i systemet. DSO bedömer att de som finns nu är aktuella. Under 2023 kommer fokus vad gäller registerförteckningen vara att kontrollera att alla behandlingar finns i DraftIt och att göra riskbedömningar.

DSO kontrollerar hur många behandlingar som registrerats

Det finns 707 registreringar i systemet DraftIt. DSO bedömer att de som finns nu är aktuella.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Under året har fokus i arbetet med dataskydd framför allt varit att uppdatera och bygga om modulen för Skärholmen i syfte att förenkla det dagliga arbetet med dataskyddsfrågor. Avdelningarna har gått igenom de registreringar som var inlagda i systemet och plockat bort dubbletter.

DSO bedömer hur fullständig registerförteckningen är

Arbetet med att rensa i DraftIt har varit ett första nödvändigt steg i arbetet med att ha en uppdaterad och fullständig registerförteckning. DSO bedömer att ett stort arbete kvarstår: att under 2023 lägga in de

behandlingar som i dagsläget inte ligger i systemet. Detta kommer att behöva takta med den kartläggning av informationssäkerhetstillgångar som pågår på förvaltningen.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Avdelningarna har utsedda ansvariga, men listan över dessa är gammal och delvis inaktuell. DSO bedömer att verksamheten under 2023 behöver uppdatera listan över ansvariga för att säkerställa att det löpande arbetet med registerföring fortgår.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

3.1.5 DSO ger råd och rekommendationer till PUA

Verksamhetsansvariga för respektive avdelning bör gå igenom personuppgiftsbehandlingarna och göra uppdateringar på behandlingar som tillkommit. Detta behöver ske i takt med den kartläggning av informationssäkerhetstillgångar som pågår på förvaltningen.

3.2 Styrdokument

3.2.1 Sammanfattning

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

3.2.2 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.

Eftersom flera av styrdokumenten omfattar både dataskydd och informationssäkerhet bör DSO resonera med informationssäkerhetssamordnare i bedömningar och förslag på åtgärder framåt för nästa verksamhetsår.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?
Den enskilt största förbättringen på området är att Stockholms stad under året beslutat att anta ny riktlinje för informationssäkerhet i Stockholms stad (beslutad av kommunfullmäktige 2022-02-21). Den förra var från 2014.

Under år 2022 har en ökad aktivitet inom informationssäkerhet på förvaltningen lett till att flera dokument tagits fram. Bland dessa kan GAP-analys informationssäkerhet Skärholmen som tagits fram av två konsulter främst lyftas fram som ett gott exempel. Under 2023 kommer arbetet med informationssäkerhet fortsätta utifrån konsulternas rekommendationer.

Skärholmens stadsdelsförvaltning har en mängd handböcker och rutiner på plats, bland annat ”Handbok för hantering av personuppgifter enligt GDPR”, ”Information om hantering av personuppgifter” och ”Rutin för konsekvensbedömning”.

Samtliga rutiner/grundläggande styrdokument är uppdaterade i november 2021.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet
DSO bedömer att innehållet i existerande dokument håller lämplig kvalitet, men att de behöver gås igenom under 2023 för att se om de behöver uppdateras.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

3.2.5 DSO ger råd och rekommendationer till PUA

Stockholms stad har en stadsövergripande sida på intranätet med information om dataskyddsfrågor. Förvaltningens rutiner är ett komplement till de stadsövergripande. Under 2023 bör de lokala rutinerna gås igenom för att se om de behöver uppdateras utifrån nya stadsövergripande rutiner och/eller rekommendationer.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Inga personuppgiftsbehandlingar har informationsklassats.
Är klassade personuppgiftsbehandlingar aktuella?	Se svar ovan.

3.3.2 Syfte

För att kunna skydda information med rätt slags skydd 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 årligen av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. Enbart sådan informationsklassning som avser behandling av personuppgifter är av intresse för DSO:s årsrapportering.

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

3.3.3 Resultat

Enligt stadsdelsförvaltningens informationssäkerhetssamordnare har det inte genomförts några informationssäkerhetsklassningar av personuppgiftsbehandlingar. Dock har en konsekvensbedömning alltid gjorts vid informationssäkerhetsklassning av nya system som innefattar behandling av personuppgifter.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

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

3.3.5 DSO ger råd och rekommendationer till PUA

När personuppgiftsbehandlingarna inventerats och uppdaterats, är nästa steg att dessa också ska KLASSA:s för de system som är aktuella för detta. DSO:s rekommendation är att görs under 2023.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

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

3.4.2 Syfte

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

3.4.3 Resultat

Organisationen arbetar med konsekvensbedömningar, men främst kopplat till informationsklassning av nya system. Då registerförteckningen inte är helt uppdaterad är det oklart om alla personuppgiftsbehandlingar som behöver konsekvensbedömas har identifierats.

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?
Nej. Arbete pågår med att uppdatera DraftIt och när verksamheterna slutfört uppdateringen kommer de att, med stöd av DSO, påbörja arbetet med att bedöma vilka behandlingar som bör konsekvensbedömas.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?
Förvaltningen har till exempel identifierat Nyckelfri hemtjänst som en potentiell högriskbehandling och konsekvensbedömt den. DSO:s bedömning är att de flesta högriskbehandlingar är konsekvensbedömda, men eftersom registerförteckningen inte är komplett går frågan inte att besvara med hundra procents säkerhet.

Är de genomförda konsekvensbedömningarna aktuella?
DSO bedömer att de genomförda konsekvensbedömningarna är aktuella.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

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

3.4.5 DSO ger råd och rekommendationer till PUA
Oftast är det stadsdelens DSO och informationssäkerhetssamordnare som har identifierat nya behandlingar som verksamheterna ska införa. Ansvaret för att konsekvensbedömning och informationsklassning genomförs ligger på verksamheterna. Under 2023 är det viktigt att verksamheterna medvetandegörs om det egna ansvaret för utförandet av konsekvensbedömningar.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	2
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	2

3.5.2 Syfte

Registrerade personer har enligt Dataskyddsförordningen 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.

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.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?
Stadsdelsförvaltningen har en intranätssida med GDPR-information. Den har samtliga områden omhändertagna som berör den registrerades intressen. Stadsdelens delegationsordning är tydlig vad gäller vilken funktion som har rätt att fatta beslut angående begäran från de registrerade.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

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

3.5.5 DSO ger råd och rekommendationer till PUA

DSO anser att de rutiner som finns följs. Rådet blir därför att fortsätta arbeta strukturerat med hanteringen och att inte glömma att meddela DSO när en begäran inkommer, så att DSO kan föra statistik över antal inkomna begäran.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom att personalen uppmärksammar dem alternativt meddelas av personuppgiftsbiträden.
Hur många personuppgiftsincidenter har dokumenterats?	14 st. har dokumenterats i stadens incidentrapporteringssystem, IA.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Inga har ansetts behöva rapporteras till IMY.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	-

3.6.2 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.”

Enligt Dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, även i de fall incidenten inte ska rapporteras till IMY. Bristande dokumentation står i strid med Dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentation är sanktionsgrundande.

3.6.3 Resultat

De incidenter med personuppgifter som skett hos Skärholmens stadsdelsförvaltning under 2022 är av olika art, men framför allt rör det sig om information som kommit fel vid utskick eller obehörig åtkomst.

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

Eftersom inga allvarliga incidenter inträffat under 2022 har ingen kontroll utförts av verksamhetens förmåga att rapportera incidenter i tid till IMY. Noteras kan att ett antal stadsövergripande incidenter inträffat under 2022. Ansvaret för att rapportera till IMY har då i samtliga fall ansetts åligga annan än Skärholmens stadsdelsnämnd.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

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

3.6.5 DSO ger råd och rekommendationer till PUA

PUA har ett väl inarbetat system för incidentrapportering, som bedöms vara känt inom verksamheten. Under 2023 rekommenderas att ansvariga chefer ges stöd i att prioritera hantering av inkomna rapporter i IA, så att dessa utreds skyndsamt.

4 Genomförda granskningar under året

4.1 Sammanfattning

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.

Genomförda granskningar 2022:

- kontroll av genomförda obligatoriska webbutbildningar i dataskydd och informationssäkerhet
- genomföra kartläggning av mognadsgrad i dataskyddsfrågor på alla nivåer i organisationer
- hantering av informationssäkerhet- och dataskyddsfrågan vid upphandling.

4.2 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 PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

4.3 Genomförda granskningar och deras resultat

Granskning 1

- kontroll av genomförda obligatoriska webbutbildningar i dataskydd och informationssäkerhet

För att effektivt kunna arbeta med dataskyddsfrågan är det av vikt att samtliga medarbetare har en grundförståelse för vad det innebär att hantera personuppgifter i sin dagliga verksamhet. Stockholms stads utbildningsplattform har grundutbildningar i dataskydd och informationssäkerhet som utgör en bra introduktion till arbetet och är dessutom obligatorisk för alla medarbetare. I Skärholmen ser statistik över genomgångna kurser ut så här:

- 28,2% har genomfört e-utbildningen ”Informationssäkerhet för medarbetare i staden”

- 45,5% har genomfört e-utbildningen ”Grundkurs i dataskydd”

DSO rekommenderar att PUA under nästa år genomför en informationskampanj till samtliga medarbetare om vikten av att genomföra dessa utbildningar.

	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

- delegationsordningen gällande GDPR och kännedom om ansvarsfördelning i organisationen (genomföra kartläggning av mognadsgrad i dataskyddsfrågor på alla nivåer i organisationer)

Meningen som står inom parentes ovan lyftes av förutvarande DSO som en granskning som skulle genomföras under 2022. Den är dock mycket omfattande, varför en avgränsning har behövt göras. Avgränsningen syftar till att granska hur delegationsordningen ser ut gällande dataskydd, samt hur väl den är känd i organisationen.

Delegationsordningen uppdaterades under 2022 vad gäller GDPR. Beslutsfattandet ligger på chefsnivå i alla typer av ärenden förutom det löpande dataskyddsarbetet (till exempel att föra register) som ligger på lokal dataskyddsorganisation. Den lokala dataskyddsorganisationen fastställdes redan när GDPR trädde ikraft, men skulle behöva utvärderas och uppdateras under 2023.

	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 3

- hantering av informationssäkerhet och dataskydd vid upphandling

Det senaste året har en upphandling om trygghetslarm (”Trygghetsskapande teknik”) genomförts tillsammans med en annan stadsdel. DSO har därför valt att granska underlaget till den upphandlingen. I upphandlingsunderlaget finns skrivningar, bl.a. om personuppgiftsansvar och att leverantören vid behov ska teckna PuB-avtal. Stadens PuB-avtalsmall finns med som en egen bilaga..

DSO:s samlade bedömning vad gäller upphandling som genomförs med hjälp av nämndens upphandlingsstrateg är att de steg och moment som behövs för att säkerställa korrekt hantering av personuppgifter utförs. Det finns också en klar rutin för hantering av dataskyddsfrågor vid offentlig upphandling, den finns publicerad på förvaltningens intranätsida för dataskydd.

	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

4.4 DSO ger råd och rekommendationer till PUA

Vad gäller de obligatoriska utbildningarna bör de ingå i introduktion till nyanställda. Om de redan gör det bör PUA informera ytterligare om vikten av att gå utbildningarna.

Vad gäller upphandlingar så fungerar det i dagsläget finns det på förvaltningen väl upparbetade arbetssätt. Det finns en klar och tydlig rutin för upphandlingsprocessen, som stadsledningskontoret tagit fram. Den finns tillgänglig på stadens intranät, via inköp och upphandling.

DSO rekommenderar att tillse att dataskyddsfrågan finns med i samtliga rutiner som förvaltningen tar fram. DSO rekommenderar även att processen för avrop från ramavtal skrivs ned och att förvaltningen där tillser att dataskyddsfrågan tas om hand särskilt.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Brist på kunskap om Dataskyddsförordningen
- Finns rutin för avrop från ramavtal som staden tecknat?

5.2 Resultatet av riskkartläggningen

Brist på kunskap om Dataskyddsförordningen

Det här är en risk som togs upp i årsrapporten för 2021 och det är en risk som flera andra Dataskyddsombud också tagit upp. Det är en ständigt relevant risk i och med att dataskyddsfrågor till sin natur är komplexa. Det är inte ens hälften av förvaltningens anställda som slutfört stadens obligatoriska utbildning, vilket kan ses som en indikation på att området inte känns relevant på individnivå. Det är också tydligt att ansvarsfördelningen mellan verksamheterna och DSO inte är klar. Det är verksamheten som ska initiera konsekvensbedömningar, men idag sker de ofta på initiativ av DSO eller informationssäkerhetssamordnare. Vad gäller DraftIt är det verksamheterna som ska hålla den uppdaterad, inte DSO.

	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

Finns rutin för avrop från ramavtal som staden tecknat?

Vid avrop från ramavtal som staden tecknat är det upp till den som gör avropet att tillse att personuppgifter tas om hand. DSO har inte sett någon rutin för detta, men även om det inte finns en rutin så kan det vara så att kunskapen ändå finns i verksamheterna. DSO bedömer dock detta som ett riskområde som behöver undersökas närmare under 2023.

	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

5.3 DSO ger råd och rekommendationer till PUA

Verksamheterna behöver fortsätta utveckla arbetssätt för att få in dataskyddsfrågorna i sitt löpande arbete. Rutiner för avrop från ramavtal behöver tas fram och/eller ses över samt göras kända i alla verksamheter.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Registerförteckningen (Draftit)
- Behörighetstilldelning, främst för system som innehåller känsliga personuppgifter

6.2 Syfte

Det granskande arbetet är en av dataskyddsarbetets viktigaste delar. Eftersom dataskyddsombudet ofta har begränsat med tid, bör granskningsområdena väljas med eftertanke. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt.

6.3 Planerade granskningar

Registerförteckningen (DraftIt)

Under 2022 har DraftIt byggts om för att underlätta arbetet med registreringar. Vidare har ett antal dubbletter plockats bort från systemet. Verksamheterna planerar att granska och riskbedöma de registreringar som finns i systemet och även gå igenom och uppdatera med nya behandlingar. DSO kommer att följa detta mycket noga och genomföra löpande kontroller under året för att säkerställa att arbetet fortlöper enligt plan.

Direktupphandlingar och avrop

Vid avrop från ramavtal som staden tecknat är det upp till den som gör avropet att tillse att personuppgifter tas om hand. DSO har inte sett någon rutin för detta, men även om det inte finns en rutin så kan det vara så att kunskapen ändå finns i verksamheterna. DSO bedömer dock detta som ett riskområde som behöver undersökas närmare under 2023.

7 Övrigt att rapportera

7.1 Sammanfattning

Flera av IMYs beslut som överklagats ligger hos Högsta Förvaltningsdomstolen för slutligt avgörande, vilket kommer att ge ytterligare praxis.

PUA bör hålla sig uppdaterad om utgången av EU-kommissionens arbete med att skapa en ny process för överföring av personuppgifter eftersom säker överföring av personuppgifter utanför EES skulle minska den administrativa bördan som omger delar av personuppgiftsarbetet på förvaltningen just nu.

7.2 Syfte

I detta kapitel lyfter DSO fram de viktigaste slutsatserna från årets omvärldsbevakning.

7.3 Övriga observationer

IMYs roll börjar formaliseras

Flera av IMYs beslut som överklagats ligger hos Högsta Förvaltningsdomstolen för slutligt avgörande, vilket kommer att ge ytterligare praxis.

Schrems II-domen

Enligt Schrems -domen får personuppgifter inte överföras utanför EES om inte exportören använder en godkänd mekanism som gör överföringen laglig, till exempel det s.k. Privacy Shield. Efter Schrems II anses inte Privacy Shield längre tillräckligt säkert att använda.

För närvarande förbereder EU-kommissionen ett så kallat adekvansbeslut, som är den rättsliga process som ger en generell möjlighet till överföring utanför EES. Ett beslut om detta förväntas fattas tidigast under våren 2023.

7.4 DSO ger råd och rekommendationer till PUA

PUA bör hålla sig uppdaterad om utgången av EU-kommissionens arbete med att skapa en ny process för överföring av personuppgifter eftersom säker överföring av personuppgifter utanför EES skulle minska den administrativa bördan som omger delar av personuppgiftsarbetet på förvaltningen just nu.

Nästa år ska de europeiska dataskyddsmyndigheterna granska dataskyddsombudens roll och ställning. En återkommande fråga inom förvaltningen är vad DSO kan, får och ska hjälpa till med. Rollen som DSO är ju också den relativt ny och har formats olika beroende på vem som haft rollen som DSO. En tydligare rollbeskrivning kommer att underlätta såväl för den som innehar rollen som DSO som den verksamhet DSO är satt att granska.