Dataskyddsombudets årsrapport för 2023

Stadsbyggnadsnämnden

Dataskyddsombudets årsrapport
Januari 2024

Dnr: 2024-00526
Utgivningsdatum: 2024-01-24
Kontaktperson: Frida Sjökvist

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 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 är skyldig att ge till personuppgiftsansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:s granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Rapporten är ett redskap för nämnd/bolagsstyrelse för att kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur 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 *dokumenteringsskyldighet*. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

Min sammanfattande bedömning utifrån granskningen är att SBK till stor del har en tillfredsställande organisation för att bedriva ett systematiskt dataskyddsarbete.

Vid 2022 års (fjolårets) granskning har det identifierats ett par brister kopplade till kontorets registerförteckning samt konsekvensbedömningar. Arbetet med ***registerförteckningen*** har fortlöpt väl under 2023 och SBK är på god väg mot ett fullgott register. I årets granskningsrapport ges rekommendationer för att uppdatera registerförteckningen rutinmässigt. Vad gäller ***konsekvensbedömningar*** har kontoret tagit till sig av rekommendationer i 2022 års granskningsrapport och genomfört riskanalys för konsekvensbedömningar i samband med informationsklassningar, samt upprättat konsekvensbedömningar i erforderliga fall.

Det föreligger fortsatt brister i kontorets ***styrdokument***. SBK har bra och upplysande information på intranätet men det bör göras en översyn av behov av styrande dokument och innehållet i dessa.

Vad gäller ***tekniska och organisatoriska åtgärder*** för personuppgiftsbehandlingar har det under året genomförts ett antal informationsklassningar där personuppgifter har beaktats. SBK är på god väg med informationsklassningsarbetet i verksamheten och det rekommenderas att dataskydd fortsatt blir en naturlig del av det.

I granskningen har det inte identifierats några brister vad gäller granskningsområdet ***individens rättigheter***. Det har heller inte identifierats några större brister vad gäller hanteringen av ***personuppgiftsincidenter*** men undertecknad har gett ett par rekommendationer i fråga om styrande dokument och hanteringsprocess.

DSO har också identifierat ett par brister vad gäller information till anställda vad gäller behandling av deras personuppgifter.

Medvetenhet om dataskydd hos medarbetare har framhållits som en rekommendation vid ett flertal tillfällen i granskningsrapporten. Medvetenhet och utbildning kring dataskydd är ofta en framgångsfaktor för ett långsiktigt välfungerande dataskyddsarbete i en organisation.

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 eller bolagets 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?	45
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Delvis
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

Stadsbyggnadskontoret har för närvarande 45 registrerade behandlingar varav merparten är under behandling. Det har således lagts till 5 st. behandlingar i registret sedan fjolårets granskning. I 2022 års granskning noterades att registret inte var komplett då det fortfarande finns behandlingar som saknar obligatoriska registreringsuppgifter. I årets granskning har undertecknad gjort 15 st. stickprov på angivna behandlingar i behandlingsregistret. De registrerade behandlingarna som granskats har registrerats vid olika tidpunkter. Av de 15 granskade behandlingar föreligger brister i 7 st. (se nedan). Bristerna består i att det exempelvis saknas motivering kring valet av laglig grund, rutiner för uppföljning av pu-biträde när det finns och/eller beskrivning av vidtagna säkerhetsåtgärder.

Brister föreligger, enligt stickprov, i följande registrerade behandlingar:

- Årets stockholmsbyggnad – behöver kompletteras.
- Telefoni (text, bild och röstmeddelanden) – ej fullständigt.
- LISA självservice
- Testverktyg för jobbsökande
- Individuell flexmall
- First card (innehavare)
- WinLas (anställningsfrågor)

Det har skett en viss uppdatering av behandlingsregistret, vilket bedöms som positivt, men det kvarstår vissa brister vad gäller obligatoriska registreringsuppgifter.

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

3.1.5 DSO ger råd och rekommendationer till PUA

Vad gäller registrering av nya och/eller förändrade behandlingar som förekommer inom SBK krävs att samtliga medarbetare som hanterar nya processer har kunskap dels om *vad som utgör en personuppgiftsbehandling*, dels *att detta ska kommuniceras till dataskyddssamordnare för registrering.*

Nya personuppgiftsbehandlingar sker ofta i samband med att ett nytt avtal tecknas eller att ett beslut tas. Vad gäller nya ingångna avtal eller förändringar i verksamheten bör det införas en typ av rutin som styr godkännandeprocessen, exempelvis att i avtalsdatabasen/avtalssystemet ange om personuppgifter behandlas inom ramen för avtalet. På så sätt blir frågan om personuppgiftsbehandling en naturlig del vid ett nytt avtal.

SBK bör tydliggöra för medarbetare att nya och förändrade personuppgiftsbehandlingar ska meddelas till dataskyddssamordnaren, exempelvis via information på intern hemsida samt information på månadsmöte/APT eller liknande.

Att utbilda medarbetare kring vad som är en personuppgiftsbehandling är en förutsättning för att en medarbetare ska kunna förstå att en personuppgiftsbehandling är aktuell.

SBK bör vidare uppdatera behandlingsregistret med ny DSO.

3.2 Styrdokument

3.2.1 Sammanfattning

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

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.

3.2.3 Resultat

Följande styrdokument har granskats:

- Integritetspolicy / Dataskyddspolicy SBK
- Lathund för hantering av personuppgifter inom SBK – intern information
- Vägledning för personuppgiftsincidenthantering
- Lokal rutin incidenthantering (beslutad men ej kommunicerad till medarbetare)

Styrdokument är värdefulla verktyg för alla organisationer. Ett styrdokument såsom en policy eller en lathund ger inte endast vägledning i specifika situationer i den dagliga verksamheten utan säkerställer också att lagar, föreskrifter och andra regelverk efterlevs. Styrdokument som hanteras rätt kan skapa förutsebarhet och effektivisera processer, inte minst på dataskyddsområdet.

Integritetspolicy / Dataskyddspolicy uppdaterades senast 2023-02-14. Policyn är av mer generell karaktär och riktas främst till den registrerade. Det bör klarläggas vilket syfte policyn har och hur informationen kommuniceras till den registrerade. Eftersom informationen till registrerade ges även på extern hemsida bör det säkerställas att ev. uppdateringar sker i både policy och på hemsidan.

SBK har också en lathund för hantering av personuppgifter som uppdaterades i december 2019. Lathunden innehåller relevant information till SBK:s medarbetare men saknar struktur med bl.a. rubriker och tydlig avsnittsindelning.

SBK har mycket information om personuppgiftsbehandling på intranätet. På intranätet finns information om exempelvis inbyggt dataskydd, tekniska och organisatoriska skyddsåtgärder och ”tips” om hur övrig styrande information kan implementeras.

Informationen om personuppgiftsbehandling på intranätet bör hållas lättförståelig och relevant för medarbetarna. Information på intranätet bör istället utformas så att det underlättar arbetsprocesser, kommunikation och kunskapsdelning. Intranätet behöver därför inte innehålla information om exempelvis inbyggt dataskydd eller tekniska och organisatoriska skyddsåtgärder då det inte påverkar medarbetare i deras dagliga arbete. Sådan information kan istället, med fördel, finnas i en dataskyddspolicy för att säkerställa att beslut om principer och åtgärder tas på ledningsnivå.

Vägledningen för personuppgiftsincidenthantering innehåller bra och relevant information vid en personuppgiftsincident. Terminologin Datainspektionen används istället för IMY. Vägledningen finns publicerad på intranätet under Personuppgiftsincident, vilket bedöms som positivt. Ett par rutiner som anges i vägledningen är dock inte längre aktuella, eftersom IMY numera har en e-tjänst för rapportering av incidenter.

SBK har beslutat om en ny lokalrutin för incidenthantering, som också innehåller ett särskilt avsnitt om personuppgiftsincidenter. Rutinen innehåller bra, tydlig och viktig information avseende personuppgiftsincidenter, exempelvis om dokumentation av incidenter som inte varit tydligt i övriga styrdokument.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

3.2.5 DSO ger råd och rekommendationer till PUA

SBK bör gå igenom vilken information som gör sig mest lämplig på intranätet respektive i styrdokument, såsom lathund och dataskyddspolicy. Information avseende exempelvis tredjelandsöverföringar, inbyggt dataskydd eller tekniska och

organisatoriska skyddsåtgärder kan med fördel finnas tillgängligt i en dataskyddspolicy.

Informationen i styrdokument bör anpassas dels efter krav i GDPR, dels efter verksamhetens behov och förutsättningar. SBK bör gå igenom om vissa avdelningar behöver specifika styrande dokument och rutiner, såsom ekonomi och HR.

Ett styrdokument inom dataskydd bör också kompletteras med åtminstone följande:

- Tydligt angivet syfte, målgrupp, ansvar (befogenheter och ansvarsområden)
- Behandling av känsliga och extra skyddsvärda personuppgifter
- Information när personuppgifter samlas in från den registrerade (artikel 13 GDPR)
- Information när personuppgifter samlas in från annan än den registrerade (artikel 14 GDPR)
- Rutiner kring registerutdrag
- Information till anställda (som registrerade) om personuppgiftsbehandling

SBK bör också säkerställa att beslutade styrdokument revideras minst en gång varje år.

SBK rekommenderas att uppdatera terminologin ”Datainspektionen” till ”IMY” samt uppdatera kontaktuppgifter till DSO i styrdokumenten.

Vad gäller vägledningen för anmälan av personuppgiftsincidenter bör SBK se till att den stämmer överens med aktuella rutiner och information hos IMY och att den synkas med den lokala rutinen för incidenthantering.

SBK bör säkerställa att samtliga styrdokument synkas och att hänvisningar till övriga styrdokument är korrekta.

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?	8 (under 2023)
Är klassade personuppgiftsbehandlingar aktuella?	Delvis

3.3.2 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 faktiskt 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.

3.3.3 Resultat

Under 2023 har sju stycken informationsklassningar genomförts (Bluebeam, Zoom X, Klara arkivförteckningssystem, Grannehörande, Säkra digitala möten, Trusted Dialog, Geodatabutiken och Stadsbyggnadsbenchen).

I denna granskning granskas informationsklassningarna endast utifrån ett dataskyddsperspektiv.

I ovanstående klassningar har personuppgifter varit en del i informationsklassningen. Det har identifierats vilka personuppgifter som behandlas och om de utgör integritetskänsliga eller känsliga personuppgifter. Syftet är att få en indikation på känsligheten i uppgifterna som behandlas. I bedömningen beaktas även art, omfattning, sammanhang och ändamål med personuppgiftsbehandlingen. Enligt undertecknad föreligger det inga brister ur ett dataskyddsperspektiv i informationsklassningarna. I samband med informationsklassningarna har det också utförts en riskanalys för huruvida en konsekvensbedömning behöver utföras.

I 2022 års granskning observerades att kommande informationsklassningar kommer planeras in för en tidsperiod om 3-5 år. Enligt SBK kommer en ny person tillträda som informationssäkerhetssamordnare i början av 2024 och fortsätta arbetet med informationsklassningar. SBK är på god väg med att informationsklassa information, inkl. personuppgifter, i verksamheten. Nedanstående angivelse av risk är främst kopplad till att det finns ytterligare information att klassa, och som även inkluderar 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
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.3.5 DSO ger råd och rekommendationer till PUA

SBK är som ovan sagts på god väg med informationsklassningen av informationstillgångar. Det bedöms som positivt att en ny medarbetare tillträder inom kort för att kunna prioritera informationsklassningsarbetet.

Denna granskning fokuserar endast på dataskyddsperspektivet i informationsklassningarna och utifrån den granskning som har gjorts av genomförda klassningar under 2023 har dessa en bra struktur vad gäller dataskydd. Väsentliga delar kring känsligheten på informationen har beaktats och det har utförts tillfredsställande riskanalyser för konsekvensbedömningar.

Personen som tillträder bör säkerställa att kvaliteten på klassningarna upprätthålls. Det bör säkerställas att SBK:s registerförteckning i Draftit uppdateras i samband med klassningarna.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Delvis
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Delvis
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/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). Notera att IMY på sin webbplats har publicerat en förtydligande förteckning över när personuppgiftsbehandlingar kräver en konsekvensbedömning. Det är viktigt att PUA genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

I SBK:s ”Lathund för hantering av personuppgifter” anges att nya system som ska tas i bruk också ska anmälas till kontorets Dataskyddsombud. I lathunden nämns inget om när eller huruvida en konsekvensbedömning ska upprättas. Som ovan sagts (under avsnittet styrdokument) finns det andra situationer än vid nya system som konsekvensbedömning kan behöva upprättas. Nya eller förändrade personuppgiftsbehandlingar kan exempelvis förekomma när SBK ingår avtal om en ny tjänst eller beslutar om nya/förändrade rutiner.

På SBK:s intranät finns information om konsekvensbedömningar och exempel på situationer då en sådan ska genomföras. Det anges också att Dataskyddsombudet ska involveras. Det finns även en mall för konsekvensbedömning publicerad på intranätet.

Under 2023 har konsekvensbedömning gjorts för Bostadsanpassningen och Zoom X. Dataskyddsombudet har varit involverad vid båda bedömningarna.

Bedömningen är att SBK vid sitt fortsatta informationsklassningsarbete kommer att kunna identifiera informationstillgångar / system / situationer där konsekvensbedömning kan komma att behöva upprättas. Som noterats ovan under avsnitt 3.3.5 är det viktigt att det implementeras en skriftlig rutin som säkerställer att det görs en riskanalys avseende konsekvensbedömning vid informationsklassningar.

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

3.4.5 DSO ger råd och rekommendationer till PUA

SBK bör se över informationen som finns på intranätet vad gäller konsekvensbedömningar och se till att den samstämmer med information i skriftliga styrdokument. Det bör som sagt säkerställas i en skriftlig rutin när riskanalys avseende konsekvensbedömningar ska upprättas, exempelvis vid informationsklassningar och vid upphandlingar. Rutinerna bör kommuniceras till berörda medarbetare.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

3.5.2 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 dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från

Integritetsskyddsmyndighetens (”IMY”) 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

Under året har SBK endast haft en begäran om registerutdrag och det har inte varit något problem för kontoret att göra denna sammanställning. Ingen anmärkning har framförts över hanteringen.

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

Det registerutdrag som begärts under året har varit relativt enkelt att besvara, men för att ta höjd för mer komplicerade förfrågningar behöver kontoret ha en komplett registerförteckning (se ovan, punkt 3.1) så att vi vet vilka informationsmängder som måste genomsökas för att alltid kunna sammanställa registerutdragen.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Meddelande från SLK Informationssäkerhet; Incidentrapporteringssystemet IA; Meddelande från medarbetare
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?	-

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.”

I en verksamhet kan förekomma många andra typer av incidenter, som inte involverar personuppgifter. Det är viktigt att hålla den saken i åtanke, så att årsrapporteringen inte omfattar annat än just personuppgiftsincidenter. Vidare är det en grundförutsättning för hanteringen av personuppgifter att incidenter över huvud taget upptäcks, samt att verksamheten förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som dataskyddsförordningen kräver.

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. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

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 konstaterat att det handlar om en personuppgiftsincident. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. 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:s sida. DSO:s årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering 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 dokumentering är sanktionsgrundande.

3.6.3 Resultat

Under 2023 har nio stycken personuppgiftsincidenter registrerats i IA. Ingen av incidenterna har rapporterats till IMY.

På SBK:s intranät finns information om personuppgiftsincidenter samt rutiner för hur dessa ska hanteras. De rutiner som det hänvisas till på intranätet som rör personuppgiftsincidenter innehåller en

gammal terminologi avseende tillsynsmyndigheten (som numera kallas IMY).

SBK har också en lokal rutin för incidenthantering som i skrivande stund är beslutad men inte kommunicerad till medarbetare. Rutinen innehåller ett specifikt avsnitt om personuppgiftsincidenter med relevant och tydlig information.

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

3.6.5 DSO ger råd och rekommendationer till PUA

SBK rekommenderas att se över rutinbeskrivningarna avseende personuppgiftsincidenter och säkerställa att hanteringsprocessen är tydlig för samtliga medarbetare. Informationen på intranätet bör synkas med informationen i den nya rutinen för incidenthantering.

Ett förslag är att ange Dataskyddsombudets kontaktuppgifter under avsnittet Personuppgiftsincidenter på intranätet för att medarbetare ska kunna diskutera det inträffade och få stöttning kring hur incidenten ska hanteras och om anmälan till IMY bör ske.

SBK bör uppdatera informationen på intranätet efter senaste terminologin för tillsynsmyndigheten (IMY).

Många personuppgiftsincidenter orsakas av den s.k. mänskliga faktorn varför det är naturligt att personuppgifter inträffar i en större organisation med många medarbetare. För att organisationen ska kunna arbeta proaktivt vad gäller incidenter samt kunna anmäla incidenter inom utsatt tid är det viktigt att medarbetare är medvetna om vad som utgör en personuppgiftsincident. Det finns fördelar med att diskutera incidenthantering med medarbetare även muntligen för att lyfta vissa specifika frågeställningar och tydliggöra det väsentliga i att incidenter rapporteras till rätt person

och i rätt tid. SBK kan därför med fördel kommunicera ny rutin kring incidenthantering till medarbetare även *muntligen*, på exempelvis APT, månadsmöte eller liknande.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Granskning av information till registrerade

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

	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

GDPR ställer krav på att den registrerade ska få information när dennes personuppgifter behandlas. Sådan information ska lämnas av den personuppgiftsansvarige när uppgifterna samlas in, men även när den registrerade begär det.

Vad gäller information till medborgare (en kategori av registrerade) har SBK bra information vad gäller personuppgiftsbehandling inom SBK med vidare hänvisning till Stockholms stads information vad gäller personuppgifter och dataskydd. Informationen till

medborgare på extern hemsida bedöms som tillräcklig. Informationen på extern hemsida bör dock uppdateras med kontaktuppgifter till ny DSO.

En annan kategori av registrerade som SBK behandlar personuppgifter om är *anställda*. SBK har som arbetsgivare en långtgående skyldighet enligt GDPR att informera anställda om behandlingen av deras personuppgifter. Det innebär att det ska vara klart och tydligt för de anställda hur arbetsgivaren behandlar deras personuppgifter. De anställda ska få information om att arbetsgivaren samlar in personuppgifter, varför de samlas in och hur de används. De anställda ska vidare få information om vilka ytterligare rättigheter de har enligt GDPR, exempelvis rätten att begära registerutdrag. Skyldigheten att informera de anställda gäller i princip vid all behandling av uppgifter om anställda.

SBK ger anställda information om personuppgiftsbehandling i ett s.k. ”användarkontrakt” som en anställd godkänner i samband med nyanställning. Användarkontraktet är främst kopplat till arbetsplatssystem såsom dator och programvaror. Informationen om behandling av personuppgifter rör därför också behandlingen inom ramen för *datoradministrationen*.

SBK rekommenderas att kartlägga vilka personuppgiftsbehandlingar som sker inom kontoret som helhet vad gäller anställda, samt vilken laglig grund och ändamål som ska anges för behandlingarna. SBK rekommenderas även att uppdatera behandlingsregistret i Draftit med samtliga behandlingar som rör anställda, men även tidigare anställda och personer under rekrytering.

Anställda bör få information om *samtliga* personuppgiftsbehandlingar som sker om dem, vilken laglig grund kontoret stödjer sig på samt vilket ändamål SBK har för behandlingarna. Det bör också anges hur länge informationen sparas, om information inhämtas från andra källor, om personuppgifter lämnas till tredje man, om överföring av personuppgifter sker till tredje land samt vilka rättigheter den anställde (som registrerad) har såsom rätt till registerutdrag och begäran om rättning/radering.

5 Risker inom dataskydd

5.1 Sammanfattning

DSO har tillsammans med dataskyddssamordnare och enhetschef för kontoret genomfört en riskbedömning under oktober 2023. Riskanalysen baseras på relevanta artiklar i GDPR och DSO liksom verksamheten har fått möjlighet att identifiera var brister inom dataskydd finns inom verksamheten.

5.2 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.

5.3 Resultatet av riskkartläggningen

DSO har som sagt tillsammans med verksamheten genomfört en riskanalys avseende dataskydd under 2023.

Ett flertal risker som identifierats i riskbedömningen är kopplade till ett ofullständigt behandlingsregister, exempelvis vad gäller principer för personuppgiftsbehandling.

Vissa frågor kopplade till informationssäkerhet har också varit svåra för verksamheten att svara på.

DSO ansvarar för att uppdatera riskbedömningen vid behov och minst årligen.

5.4 DSO ger råd och rekommendationer till PUA

Som ovan sagts bör SBK fortsatt arbeta med uppdatering av behandlingsregistret och främja rutiner för uppdatering vid nya och förändrade behandlingar. DSO kan involveras vid behov av råd och stöd.

Risker kopplade till dataskydd har inte sällan ett starkt samband med risker inom informationssäkerhet. Som ovan sagts bör SBK säkerställa att dataskydd är en naturlig del av informationssäkerhetsarbetet, och vice versa.

6 Planerade granskningar under det nya verksamhetsåret

Vid kommande verksamhetsårs granskning kommer minst de brister som identifierats under årets granskning att följas upp.

7 Övrigt att rapportera

7.1 Sammanfattning

Det är kommunens medarbetare som behandlar personuppgifter dagligen och som ställs inför utmaningar kring personuppgiftsbehandling. Vad gäller exempelvis personuppgiftsincidenter visar statistik på att en stor del av incidenterna orsakas av den s.k. mänskliga faktorn.[1]

Utbildning och medvetenhet är en viktig parameter i det proaktiva arbetet kring både personuppgiftsincidenter och för att hålla sig uppdaterad om eventuella förändringar och nyheter inom dataskyddsområdet. Att diskutera potentiella incidenter och frågeställningar inom dataskydd som medarbetarna kan ställas inför håller medvetenheten ”a jour”.

SBK erbjuder medarbetare årlig e-grundutbildning inom dataskydd, vilket är positivt. Kontoret har också en dataskyddssamordnare som bidrar till ett välfungerande dataskyddsarbete.

[1] https://www.verizon.com/business/en-sg/resources/reports/dbir/2022/summary-of-findings.

Det finns dock ett värde i att medarbetare mer regelbundet diskuterar dataskyddsfrågor.

7.2 Syfte

Avsikten med denna punkt i årsrapportmallen är att ge möjlighet att komplettera bilden av statusen i dataskyddsarbetet. Under denna rubrik kan anges sådant som inte på ett naturligt sätt tas upp under någon av punkterna i rapporteringsstrukturen ovan, eller som inte heller ryms i den inledande sammanfattningen (som ju enbart bör innehålla de två-tre allra mest centrala observationerna eller händelserna från det gångna året).

7.3 Övriga observationer

Samtliga medarbetare inom SBK erbjuds en grundutbildning i dataskydd samt informationssäkerhet. Utbildningarna ska genomföras årligen.

Kontoret bör säkerställa att medarbetare i förekommande fall erbjuds mer riktad utbildning samt kompetensutveckling inom dataskydd som är anpassad efter deras behov och ansvarsroll. Dataskydd bör diskuteras vid exempelvis månadsmöten och APT för att bli en naturlig del av medarbetares arbetssätt.

7.4 DSO ger råd och rekommendationer till PUA

PUA bör tillse att kontoret har resurser för att erbjuda erforderlig utbildning och kompetensutveckling inom dataskydd till medarbetare.