Stockholms stad

Dataskyddsombudets årsrapport för 2024

Stadsbyggnadsnämnden

Dataskyddsombudets årsrapport
Januari 2025

Dnr: 2024-18866
Utgivningsdatum: 2024-12-12
Kontaktperson: Frida Sjökvist, Johanna Ljungmark

1 Bakgrund

EU:s Dataskyddsförordning[1] (GDPR) 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. GDPR syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt GDPR är varje nämnd inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnden behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd i Stockholms stad har i enlighet med GDPR 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 nämnden att ta emot de råd och rekommendationer som DSO är skyldig att ge till personuppgiftsansvarig enligt GDPR samt för att få insyn i vad DSO:s granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Rapporten är ett redskap för nämnden för att kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur personuppgiftsansvarig efterlever dataskyddslagstiftningen.

GDPR bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnden ska kunna *visa* att verksamheten efterlever GDPR. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighet*. Årsrapporten är även ett medel för nämnden uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Innehåll

2 Sammanfattning

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

Verksamheten har påbörjat arbetet med att flytta över ***registerförteckningen*** från Draftit till Klara Dialog. Granskningen har visat att registret i dagsläget inte uppfyller kraven enligt GDPR. Verksamheten bör säkerställa att samtliga processer och behandlingar som SBK är personuppgiftsansvarig respektive personuppgiftsbiträde för förs in i registret samt att de uppgifter som är obligatoriska enligt GDPR tillförs registret.

Vad gäller ***konsekvensbedömningar*** så rekommenderas PUA att i samband med informationsklassning bedöma om en konsekvensbedömning erfordras, samt dokumentera den bedömning som görs.

Det föreligger fortsatt brister gällande ***styrdokument.*** Innehållet i den information som finns tillgänglig bedöms vara tillräcklig. Dock bör personuppgiftsansvarig säkerställa att PUA har kontroll över innehållet och ev. ändringar som görs i ”Handbok för informationshantering” eftersom något formellt beslut av innehållet inte tas av PUA själv.

När det gäller ***tekniska och organisatoriska säkerhetsåtgärder*** för personuppgiftsbehandlingar har det under året genomförts ett antal informationsklassningar där personuppgifter har beaktats. Endast mindre brister har identifierats i hanteringen. PUA rekommenderas införa rutiner för att säkerställa att de personuppgiftsbehandlingar som identifieras i samband med klassningarna tillförs verksamhetens behandlingsregister.

I granskningen har det inte identifierats några brister vad gäller granskningsområdet ***individens rättigheter,*** då det inte har inkommit några begäranden under 2024.

Avseende ***personuppgiftsincidenter*** bör PUA se till att det vid varje misstanke om en personuppgiftsincident görs en bedömning om det inträffade utgör en incident, om incidenten ska anmälas till IMY samt om den registrerade ska informeras.

Gällande ***personuppgiftsbiträdesavtal*** rekommenderas PUA säkerställa att PUB-avtalen kompletteras med en instruktion för personuppgiftsbehandlingen, förtydliga behovet av PUB-avtal i inköpsprocessen samt överväga att skapa en tydligare översikt över tecknade PUB-avtal.

DSO har också identifierat mindre brister vad gäller dataskydd vid inköpsprocessen. Granskningen har visat att det finns ett antal dokument som är en bra grund för att dataskydd ska beaktas vid upphandling, bland annat den s.k. checklistan. PUA rekommenderas komplettera checklistan med åtgärder för att säkerställa att dataskyddsperspektivet beaktas i inköpsprocessen.

Vidare har DSO identifierat brister vad gäller personuppgiftsbehandling i ostrukturerad data. PUA rekommenderas att regelbundet rensa personuppgifter i e-post och gemensamma mappar samt informera medarbetare hur och var personuppgifter får behandlas.

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 som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som GDPR 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?	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 artikel 30 i GDPR 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

Verksamheten planerar att gå över från att ha sin registerförteckning i verktyget Draftit till Klara dialog. Klara dialog är ett verktyg för att redovisa, presentera och styra verksamhetsinformation.

Formkravet som GDPR ställer på registerförteckningen är att den ska vara skriftlig i elektronisk form (artikel 30.3). Hur informationen ska organiserat är inte definierat. Artikel 30 uppställer vidare ett antal krav på vad en registerförteckning ska innehålla:

- Namn och kontaktuppgifter till organisationen
- Namn och kontaktuppgifter till eventuella gemensamt personuppgiftsansvariga samt, i tillämpliga fall, dataskyddsombud
- Ändamålen med personuppgiftsbehandlingen
- Kategorier av registrerade
- Kategorier av personuppgifter
- Eventuella mottagare som personuppgifterna lämnas till
- Hur länge uppgifterna sparas (om möjligt)
- Beskrivning av tekniska och organisatoriska säkerhetsåtgärder (om möjligt)

Verksamheten har slutfört arbetet med att strukturera processer utifrån olika verksamhetsområden i Klara dialog. Arbete med att koppla processerna till personuppgiftsbehandlingar pågår. För vissa processer är rättslig grund och ändamål enligt GDPR angivet. Mot bakgrund av kraven ovan uppfyller registret i Klara dialog i dagsläget *inte* kraven enligt GDPR. Verksamheten bör komplettera registret med de (ifyllbara) fält som är obligatoriska enligt dataskyddsförorddingen. Verksamheten bör också säkerställa att registret innehåller samtliga behandlingar som SBK är

personuppgiftsansvarig respektive personuppgiftsbiträde för. Det blir en strukturell fördel för verksamheten om samtliga behandlingar redovisas på samma ställe.

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

PUA bör säkerställa att registerförteckningen i Klara dialog uppfyller kraven i GDPR och att registret blir uppdaterat med samtliga behandlingar som SBK är PUA resp. PUB för.

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 GDPR är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna *visa* att GDPR:s 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

Vid fjolårets granskning noterades ett antal brister i SBK:s styrdokument. Verksamheten har enligt uppgift inte gjort några ändringar i befintliga styrdokument sedan fjolårets granskning. Verksamheten har istället framfört att information och rutiner som finns på samarbetsytan ”Informationshantering” ska tolkas som styrande dokument (”handbok för informationshantering”). På samarbetsytan finns grundläggande information till medarbetare vad gäller personuppgiftsbehandling, registerförteckning, begäran om registerutdrag, personuppgiftsbiträdesavtal, konsekvensbedömningar och särskilt om hantering av skyddsvärda uppgifter. Vad gäller identifiering och hantering av personuppgiftsincidenter finns det en länk till sidan om Informationssäkerhet på samarbetsytan. Det finns även länkar till Stockholms stads intranät avseende personuppgifter men denna länk fungerar ej.

Mot bakgrund av det syfte som finns med styrande dokument, dvs. att PUA ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att medarbetare får information om vad som gäller och förväntas av dem, bedöms innehållet i den information som finns tillgänglig på samarbetsytan som tillräcklig.

Enligt artikel 5 GDPR ska SBK som PUA också kunna visa att de grundläggande dataskyddsprinciperna i GDPR efterlevs (ansvarsskyldighet), exempelvis genom att upprätta interna riktlinjer för dataskydd och utbilda personal. GDPR ställer inget explicit krav på att riktlinjer måste beslutas av ett visst organ hos PUA (t ex personuppgiftsansvarig nämnd). PUA rekommenderas dock säkerställa att PUA har kontroll över innehållet och ev. ändringar eftersom något formellt beslut av innehållet inte tas av PUA själv. Sådant säkerställande kan ske genom exempelvis någon form av delegation eller liknande.

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

PUA bör säkerställa att PUA har kontroll över innehållet och ev. ändringar som görs i ”Handbok för informationshantering” eftersom något formellt beslut av innehållet inte tas av PUA själv. Sådant säkerställande kan ske genom exempelvis någon form av delegation eller liknande.

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 2024)
Är klassade personuppgiftsbehandlingar aktuella?	Ja

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 2024 har följande informationsklassningar genomförts:

- Hantera digitala stöd och funktioner
- Hantera it-säkerhet
- Hantera informationssäkerhet
- Redovisa och förvalta information
- Hantera bostadsanpassningsbidrag
- Hantera återställningsbidrag
- Hantera geografisk information och visualiseringar

I samtliga klassningar har det angetts vilka personuppgifter som behandlas samt rättslig grund för behandlingen. Undertecknad har inga kommentarer på angivelse av rättslig grund.

Personuppgiftsbehandlingarna som identifierats i samband med klassningarna har dock inte lagts till i SBK:s behandlingsregister.

I klassningarna ”hantera reparationsbidrag”, ” hantera bostadsanpassningsbidrag”, ”hantera återställningsbidrag” framgår att känsliga personuppgifter behandlas, vilket kan vara en indikation på att konsekvensbedömning erfordras. I samtliga klassningsprotokoll anges att konsekvensbedömning är genomförd. För övriga klassningar som innebär en personuppgiftsbehandling (dock inte av känsliga sådana) framgår dock inte huruvida konsekvensbedömning erfordras.

I ”Handbok för informationsklassning” anges att i de fall en personuppgiftsbehandling med höga risker identifieras i samband med riskanalys vid informationsklassning, ska en konsekvensbedömning göras.

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

Den bedömning som sker i samband med informationsklassningar avseende behov av konsekvensbedömning bör dokumenteras. Detta även i de fall bedömningen är att det inte finns behov av att ta fram en konsekvensbedömning. Beakta att konsekvensbedömning kan behövas även då inte känsliga personuppgifter behandlas.

SBK kan med fördel också se till att de personuppgiftsbehandlingar som identifieras i samband med klassningarna också läggs till i processer i verksamhetens behandlingsregister. Rutinen bör formaliseras.

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?	-

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 GDPR, 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

SBK har inte genomfört några konsekvensbedömningar under 2024.

Vad gäller identifiering och hantering av konsekvensbedömningar har SBK information om vad en konsekvensbedömning är och när det behövs göras en sådan, i sin ”Handbok för informationshantering” på samarbetsytan. På samma yta finns en hänvisning till SBK:s mall för konsekvensbedömning.

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

Som sagts ovan i avsnitt 3.3.5, rekommenderas SBK bedöma om en konsekvensbedömning behövs i samband med informationsklassning, även om inte känsliga personuppgifter behandlas. Bedömningen bör dokumenteras.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0 (under året)
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	-

3.5.2 Syfte

Registrerade personer har enligt GDPR (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 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 GDPR 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 kraven i GDPR, 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

Det har inte inkommit några begäran från registrerade under 2024. Undertecknad kan därför inte notera några brister eller utge några rekommendationer.

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

-

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?	10 st.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1 st.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	1 st.

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt GDPR (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 GDPR kräver.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland GDPRs 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. GDPR 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 GDPR 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 GDPR 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 året (2024) har totalt tio personuppgiftsincidenter rapporterats i verksamhetens IA-system. Undertecknad har gått igenom dokumentationen av incidenterna.

I en av de dokumenterade incidenterna framgår det av dokumentationen att det inte är aktuellt att anmäla incidenten till IMY. Det saknas dock motivering till varför någon anmälan inte är aktuell.

I en annan dokumenterad incident framgår det av dokumentationen att anmälan har skett till IMY och att registrerad är informerad. Det

saknas dock motivering till varför det inträffade ska anmälas och varför den registrerade ska informeras.

I en annan dokumenterad incident framgår att det inträffade inte har anmälts till IMY med en kort motivering till varför.

Tröskeln för att anmäla en personuppgiftsincident till IMY är låg. Det är endast vid fall då det är osannolikt att incidenten innebär någon risk för den registrerades fri- och rättigheter som anmälan inte behövs, vilket talar för att det finns en slags presumtion för att anmälan ska ske. SBK bör därför vid varje inträffad incident bedöma varför det inträffade är en personuppgiftsincident, varför incidenten ska/inte ska anmälas till IMY samt varför/varför inte den registrerade ska informeras, mot bakgrund av kriterierna i GDPR samt dokumentera bedömningen. Sådan dokumentation ska kunna uppvisas till IMY på förfrågan.

Av SBK:s interna rutin för hantering av personuppgiftsincidenter (i handboken för informationshantering) framgår att bedömningen om incidenten ska anmälas till IMY ska göras i samråd med dataskydds- och informationssäkerhetssamordnare och dataskyddsombud. Av de tio inträffade incidenterna under året har dataskyddsombudet endast konsulterats vid en av incidenterna.

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 bör tillse att det vid varje inträffad incident görs en bedömning av om:

- det inträffade utgör en personuppgiftsincident samt varför/varför inte

- personuppgiftsincidenten ska anmälas till IMY samt varför/varför inte
- den registrerade ska informeras om det inträffade samt varför/varför inte

Bedömningen bör utgå från GDPR och främst artikel 12 4 p., 33 och 34.

Verksamheten bör också säkerställa att dataskyddsombudet medverkar vid bedömningen om personuppgiftsincidenten ska anmälas till IMY. Det finns inget krav på att dataskyddsombudet ska medverka vid bedömningen enligt GDPR. Om verksamheten upplever att dataskyddsombudet inte behöver konsulteras vid bedömningen kan det uttryckas i de interna rutinerna (i handboken för informationshantering) att konsultation kan ske i förekommande fall.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Granskning av personuppgiftsbiträdesavtal
- Granskning av dataskydd vid inköpsprocessen
- Granskning av ostrukturerad data

4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av GDPR. En central del av det arbetet är att göra återkommande granskningar av hur väl GDPR 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 Granskning av personuppgiftsbiträdesavtal

4.3.1 Syfte

Som personuppgiftsansvarig anlitar SBK i vissa fall ett s.k. personuppgiftsbiträde som utför hela eller delar av en personuppgiftsbehandling. Enligt artikel 28 GDPR ska en sådan behandling regleras genom avtal, eller annan rättsakt. Avtalet ska säkerställa att:

- Båda parter följer GDPR
- Båda parter är medvetna om sina åtaganden och skyldigheter mot varandra och de registrerade
- Båda parter skyddar de registrerades personuppgifter
- Båda parter dokumenterar och kan visa att de följer reglerna (ansvarsskyldighet)

GDPR ställer upp ett antal minimikrav för vad ett personuppgiftsbiträdesavtal ska innehålla (artikel 28.3):

- Att behandling endast får ske enligt dokumenterade instruktioner från den personuppgiftsansvarige

- Försäkran om konfidentialitet och lagstadgad tystnadsplikt
- Lämpliga säkerhetsåtgärder
- Villkor för anlitande av underbiträden
- Skyldighet att vidta åtgärder för att uppfylla de registrerades rättigheter
- Bistå den personuppgiftsansvariga i fråga om dennes skyldigheter enligt artikel 32–36 GDPR
- Hur personuppgifter ska hanteras när avtalet upphör
- Skyldighet att gå med på och bistå vid granskning och inspektioner.

Personuppgiftsbiträdesavtalet fyller således en viktig funktion för PUA för att säkerställa att behandlingen hos personuppgiftsbiträdet sker i enlighet med GDPR.

Syftet med granskningen är att bedöma huruvida pub-avtal har tecknats i tillämpliga situationer och om avtalet uppfyller de krav som GDPR ställer på utformningen.

SBK tillhör Stadsbyggnadsnämnden, som är en nämnd inom Stockholms stad. Det är också Stadsbyggnadsnämnden som är personuppgiftsansvarig för personuppgiftsbehandling inom nämndens verksamhet. För det fall en nämnd behandlar personuppgifter för en annan nämnds räkning är den nämnden att betrakta som personuppgiftsbiträde i förhållande till den andre nämnden. Enligt GDPR ska varje personuppgiftsbiträdes hantering av personuppgifter regleras genom avtal eller annan rättsakt. Nämnderna inom Stockholms stad är självständiga juridiska personer och kan därför inte civilrättsligt teckna interna personuppgiftsbiträdesavtal, varför förhållandet bör regleras genom någon annan s.k. rättsakt.

Syftet med granskningen är därför vidare att granska huruvida en sådan tillämplig rättsakt finns.

4.3.2 Resultat

I granskningen har det gjorts stickprov på tre stycken personuppgiftsbiträdesavtal som SBK tecknat med olika personuppgiftsbiträden. Följande avtal har granskats:

- Personuppgiftsbiträdesavtal mellan SBK och Firma Thomas Henriksson, per den 3 mars 2022.
- Personuppgiftsbiträdesavtal mellan SBK och 3 Step IT Trading AB, per den 1 februari 2023.

- Personuppgiftsbiträdesavtal mellan SBK och Phenox Group AB, 2022 (datum framgår ej).

Personuppgiftsbiträdesavtal mellan SBK och Firma Thomas Henriksson
PUB-avtalet är tecknat i enlighet med SBK:s mall för PUB-avtal. Det saknas dock en instruktion till PUB-avtalet, som normalt sett ska läggas som en bilaga till PUB-avtalet, vilket bedöms som en brist. Att ge instruktioner om vilka personuppgifter som får behandlas, hur behandlingen ska gå till samt ange ändamålet med behandlingen är en viktig del i regleringen av förhållandet mellan PUA och personuppgiftsbiträde. Utan närmare instruktioner från PUA kan SBK inte säkerställa att behandlingen sker i enlighet med GDPR. Har inga instruktioner givits för personuppgiftsbehandlingen riskerar ansvaret för felaktiga behandlingar hamna hos SBK i egenskap av PUA.

Personuppgiftsbiträdesavtal mellan SBK och 3 Step IT Trading AB
PUB-avtalet är tecknat i enlighet med SBK:s mall för PUB-avtal. Inga brister notifierade.

Personuppgiftsbiträdesavtal mellan SBK och Phenox Group AB
PUB-avtalet är tecknat i enlighet med SBK:s mall för PUB-avtal. Saknas angivelse vad gäller datum för undertecknande. I övrigt bedöms inte pub-avtalet innehålla några brister.

Rutiner för identifiering och upprättande av PUB-avtal
SBK har bra information om när personuppgiftsbiträdesavtal behövs i handboken för informationshantering. SBK rekommenderas förtydliga behovet av pub-avtal i inköpsprocessen, se avsnitt 4.4.

Översikt av PUB-avtal
SBK:s PUB-avtal finns, likt övriga avtal, i ärendehanteringssystemet Public. SBK saknar en tydlig översikt över vilka PUB-avtal som finns samt vid vilka personuppgiftsbehandlingar som personuppgiftsbiträde anlitas. Sådan angivelse kan exempelvis ske i någon form av avtalsdatabas / lista och i registerförteckningen. Fördelen med en tydlig översikt är att SBK enklare och mer effektivt kan följa upp avtal, notera och hantera löptider samt förenkla sökbarheten. Vid eventuella personuppgiftsincidenter är det också en förutsättning att SBK som PUA har kännedom om ett personuppgiftsbiträde anlitas för den behandling som incidenten berör, inte minst för att klargöra

ansvarsfrågan för incidenten. I motsatt situation, då ett personuppgiftsbiträde drabbas av en incident, bör SBK enkelt kunna söka fram om biträdet anlitas av SBK.

Nackdelen med att ha PUB-avtalen i ett ärendehanteringssystem är också att det finns en risk att avtalet och dess innehåll är felstavat och att det därför inte går att söka fram avtalet över huvud taget. Risken finns också att SBK tappar den interna kontrollen över vilka avtal som är förenade med PUB-avtal och hur många/vilka personuppgiftsbiträden som anlitas.

I ett PUB-avtal framgår också om eventuell tredjelandsöverföring sker hos personuppgiftsbiträdet eller eventuella underbiträden. Ytterligare en risk med att inte ha PUB-avtalen i en tydlig och sökbar översikt är att det blir svårt för SBK att, vid eventuella upphävda adekvansbeslut från EU-kommissionen, bedöma vilka tredjelandsöverföringar som är otillåtna.

Efter samtal med verksamheten framgår att alla PUB-avtal planeras sorteras under en specifik kod i systemet Klara Dialog. Det blir då lättare att söka efter och hitta avtalet. Detta kan dock endast göras med kommande PUB-avtal och ej med befintliga. Det har också påbörjats ett arbete med sammanställning av PUB-avtal i systemkatalogen.

Reglemente för nämnder

Stockholms stad har ett s.k. Reglemente med allmänna bestämmelser för Stockholms stads nämnder (KFS 2020:07). Av reglementet framgår att när en nämnd agerar som personuppgiftsbiträde åt en annan nämnd ska den personuppgiftsansvariga nämnden ge instruktioner om behandlingen till den personuppgiftsbiträdande nämnden. SBK har däremot ingen översikt över i vilka situationer och vid vilka personuppgiftsbehandling som annan nämnd inom Stockholms stad anlitas, vilket bedöms som en brist.

4.3.3 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

4.3.4 DSO ger råd och rekommendationer till PUA

SBK bör tillse att PUB-avtal kompletteras med instruktion enligt ovanstående brist.

SBK rekommenderas förtydliga behovet av PUB-avtal i inköpsprocessen, se avsnitt 4.4.

SBK kan vidare överväga att skapa en tydligare översikt över tecknade PUB-avtal.

4.4 Granskning av dataskydd vid inköpsprocessen

4.4.1 Syfte

Upphandlingar kan i flera fall innebära att leverantören behöver behandla personuppgifter för SBK:s räkning.

GDPR påverkar alla faser i en inköpsprocess, från att upphandlingen förbereds till uppföljning av avtalet.

I förberedelsefasen bör det inventeras vilka personuppgifter som kommer behandlas inom ramen för upphandlingen och om dessa är känsliga, vilken rättslig grund som finns för behandlingen samt hur behandlingen av personuppgifter ska gå till.

Vid upphandling bör ansvar, roller och villkor för personuppgiftsbehandlingen framgå redan av upphandlingsdokumenten, bland annat genom krav på

anbudsgivarna, krav på varan eller tjänsten och genom särskilda kontraktsvillkor.

I själva upphandlingsdokumenten har SBK sedan att säkerställa att GDPR:s krav om att endast anlita s.k. ”tillförlitliga biträden” uppfylls. SBK måste säkerställa att leverantören har relevant kompentens, organisation, rutiner och tekniska möjligheter att skydda personuppgifterna. Vilka krav som behöver ställas beror på vilka personuppgifter som behandlas, om de är känsliga och vilken typ av produkt eller tjänst som ska upphandlas. En eventuell genomförd konsekvensbedömning utgör också ett viktigt underlag för hur krav kan utformas mot bakgrund av identifierade risker. Kraven kan normalt sett säkerställas genom att ett personuppgiftsbiträdesavtal (PUB-avtal) tas med i upphandlingsdokumenten.

Syftet med granskningen av dataskydd i upphandlingsprocessen är att granska huruvida relevanta aspekter enligt ovan beaktas i processen.

4.4.2 Resultat

Granskningen av själva inköpsprocessen är avgränsad till de s.k. lokala upphandlingarna som SBK själva har kontroll över. Centrala och gemensamma upphandlingar ägs av Stadsledningskontoret.

Vad gäller lokala upphandlingar finns information / processkarta för inköp och upphandlingar på intern hemsida. På hemsidan finns också olika dokument samt checklista för att genomföra upphandlingen. Som en aktivitet i checklistan för upphandling finns angivet att ta fram förlaga till pub-avtal. SBK har också en mall för upphandlingsstrategi för att uppdragsgivare/beställare av upphandlingen ska veta vem denne ska vända sig till vad gäller informationssäkerhet för upphandlingen. I mallen finns en hänvisning till SBK:s handbok för informationshantering (som innehåller information om personuppgiftsbehandling) samt en skrivelse/punkt som benämns ”PUB-avtal”.

Vid en upphandling görs också en s.k. upphandlingsstrategi som syftar till att sätta ramarna för hur upphandlingen ska genomföras. Målet är att på bästa sätt tillgodose verksamhetens behov.

SBK har ingen metodik för dokumentation av bedömning som gjorts inför upphandlingen kring frågor såsom om och vilka personuppgifter som behandlas samt om konsekvensbedömning och

PUB-avtal behövs. Någon dokumentation har därför inte genomgåtts inom ramen för granskningen och det kan därför inte bedömas huruvida relevanta frågor kring dataskydd *faktiskt* har beaktats i upphandlingarna.

Det finns även en text i Kommers som är riktad till leverantörer om hur personuppgifter behandlas i samband med själva upphandlingen. I texten framgår att beställaren är personuppgiftsansvarig, vilka personuppgifter som normalt behandlas, ändamål med behandling, rättslig grund, registrerades rättigheter etc. Informationen avseende behandling av personuppgifter i samband med upphandlingen bedöms som tillfredsställande.

4.4.3 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

4.4.4 DSO ger råd och rekommendationer till PUA

SBK har som ovan beskrivits ett antal dokument som är en bra grund för att dataskydd ska beaktas i upphandlingarna, bland annat den s.k. checklistan. Det finns som sagt en hänvisning till handbok för informationshantering som innehåller information om både vad personuppgifter (även känsliga sådana) är för något, när personuppgifter behandlas, när konsekvensbedömning behöver genomföras samt när PUB-avtal behövs. SBK kan med fördel ta fram en form av åtgärder i punktform (i checklistan) som ansvarig beställare ska ”bocka av”, för att inte riskera att frågeställningarna ”faller mellan stolarna”. I dagsläget bedöms det nämligen oklart om det är upphandlingsenheten eller beställaren som ansvarar för att gå igenom exempelvis relevant information i handbok för informationshantering (som inkluderar PUB-avtal och konsekvensbedömning) och då finns det en risk att frågeställningarna inte beaktas alls.

Frågor som med fördel kan finnas med i checklistan och som beställaren ska ”bocka av” är följande:

- Vilka personuppgifter behandlas inom ramen för den upphandlade tjänsten/produkten? Behandlas känsliga personuppgifter?
- Anlitas något personuppgiftsbiträde? Om ja, tillse att pub-avtal tecknas.
- Tillse att kraven i ev. PUB-avtal överensstämmer med de krav som ställs inom ramen för informationsklassningen
- Behövs konsekvensbedömning göras innan personuppgiftsbehandlingen påbörjas?

I checklistan kan framgå att dataskyddssamordnare och/eller DSO alltid kan konsulteras för frågor.

Upphandlingsenheten kan med fördel också ha som ”kontrollfråga” att ovanstående frågor har beaktats i upphandlingen.

Om förändringar sker enligt ovan bör också medarbetare som kan agera beställare samt upphandlingsenheten informeras om innebörden av informationen och dokumenten.

4.5 Granskning av ostrukturerad data

4.5.1 Syfte

Data, inklusive personuppgifter, brukar delas in i strukturerad vs. ostrukturerad data. Strukturerad data är sökbar och finns i en databas, och är på så sätt lättare att ha kontroll över och därmed skydda. Ostrukturerad data är inte sökbart i ett system och är inte del av någon databas. Det kan exempelvis vara personuppgifter som förekommer i bilder, ljudinspelningar, PDF-filer, e-postmeddelanden eller i dokument/mappar där det inte finns en tydlig struktur eller kontroll över innehållet. Både strukturerad och ostrukturerad data omfattas av GDPR. Det innebär att de grundläggande principerna såsom uppgiftsminimering, lagringsminimering och konfidentialitet även ska appliceras på ostrukturerad data. Det är inte förbjudet att behandla personuppgifter i ostrukturerad data utan är tvärtom nödvändigt i en verksamhet, men det kan medföra en risk att verksamheten inte har kontroll över personuppgifterna som medför större risk för att de grundläggande principerna i GDPR inte uppfylls.

Syftet med granskningen är att granska huruvida personuppgifter i ostrukturerad följer GDPR:s krav. Notera att kontaktlistor och

personuppgifter i e-post inte omfattas av granskningen av integritetsskäl (vad gäller anställda).

4.5.2 Resultat

Hanteringen av ostrukturerad data har framförts som ett problem i verksamheten.

Gemensam mapp

På den gemensamma mappen ”Gemensam SBK” finns ett antal mappar som innehåller personuppgifter. Följande brister har identifierats:

- Information, inkl. personuppgifter såsom namn och personnummer, om praktikanter och sommarvikarier finns tillgängligt. Denna information bör inte finnas tillgänglig i en öppen/icke behörighetsstyrd mapp. Det ifrågasätts också om principen om lagringsminimering är uppfylld, dvs. om personuppgifterna fortfarande behövs för ändamålet.

- Tidrapporter som innehåller personuppgifter finns tillgängliga. Denna information bör inte finnas tillgänglig i en öppen/icke behörighetsstyrd mapp.

- Bilder på anställda från fester finns tillgängligt. Det ifrågasätts om det finns laglig grund för sådan behandling.

- I en mapp som heter ”Värdegrund” finns namn och efternamn på kursdeltagare. Denna information bör inte finnas tillgänglig i en öppen/icke behörighetsstyrd mapp.

- I en mapp som heter ”ÖP” förekommer bilder på barn och ungdomar från event. Det ifrågasätts om det finns laglig grund för sådan behandling och om principen om lagringsminimering är uppfylld. Personuppgifter om barn anses dessutom särskilt skyddsvärda i GDPR. Personuppgifterna bör oavsett inte finnas tillgängliga i en öppen/icke behörighetsstyrd mapp.

E-post

Vad gäller personuppgifter i e-post är uppfattningen hos medarbetare på SBK att e-posten används som ett arkiv. Det föreligger oklarheter kring när ett e-postmeddelande ska flyttas till ett organiserat system. Det anses också saknas medvetenhet kring att personuppgifter i e-post är personuppgifter och hur behandlingen ska gå till.

Viss information om personuppgifter i e-post finns på intranätet. Informationen är dock mer inriktad på betydelsen av allmänna handlingar snarare än personuppgiftsbehandling. SBK har också en ny handbok för informationshantering där det finns en sida om e-post. Informationen bedöms som tillräcklig sett till ett dataskyddsperspektiv. Men liksom instruktioner och övriga styrande dokument är det inte tillräckligt att informationen *finns*, medarbetare bör också bli underrättade om *att* informationen finns och vad medarbetaren själv har för ansvar för att följa det som anges. Sådan underrättelse kan med fördel ges både skriftligen och muntligen.

4.5.3 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

4.5.4 DSO ger råd och rekommendationer till PUA

Verksamheten bör rensa mapparna enligt ovan. Det är också viktigt att verksamheten kommunicerar tydligt till medarbetare hur och var personuppgifter får behandlas.

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. Resultatet av riskbedömningen utgör sedan underlag för identifiering av granskningsområden. Risker identifieras, utöver vid olika typer av riskanalyser, i samband med att dataskyddsombudet genomför granskningar samt vid löpande stöd och råd till verksamheten. Att

genomföra en ny riskbedömning under år 2024 har därför inte bedömts vara nödvändigt.

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 DSO ger råd och rekommendationer till PUA

Brister som identifierats avseende behandlingsregistret samt personuppgifter i ostrukturerad data bedöms vara omfattande, DSO rekommenderar därför att SBK prioriterar att vidta åtgärder för att reducera dessa brister. SBK bör därför fortsatt arbeta med uppdatering av behandlingsregistret och främja rutiner för uppdatering vid nya och förändrade behandlingar. SBK rekommenderas även säkerställa att hanteringen av personuppgifter i ostrukturerad data uppfyller kraven enligt GDPR. DSO kan involveras vid behov av råd och stöd.

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. Inte sällan orsakas en stor del av de personuppgiftsincidenter som inträffar av den s.k. mänskliga faktorn.[2]

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”.

Mot bakgrund av identifierade brister avseende ostrukturerad data bör verksamheten tillse att medarbetarna blir informerade om gällande rutiner. Sådan underrättelse kan med fördel ges både skriftligen och muntligen.

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.

7.3 Övriga observationer

Samtliga medarbetare inom SBK ska genomföra en grundutbildning i dataskydd varje år.

Kontoret bör säkerställa att medarbetare även erbjuds mer riktad utbildning samt kompetensutveckling inom dataskydd som är anpassad efter deras behov och ansvarsroll. Detta har utförts till viss del, t.ex. för ekonomifunktionen, HR och bostadsanpassningsenheten. Området ostrukturerad data och

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

hantering av personuppgifter i e-post är exempel på utbildningsområden där ett särskilt behov finns av utbildning mot bakgrund av de brister som identifierats i avsnitt 4.5. Dataskydd bör även 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.