Protokoll 1/2024

fört vid S:t Erik Markutveckling ABs sammanträde fredagen den 8 mars 2024 kl. 14:00-15:30, Stadshus AB - Riddaren

Ledamöter	Thomas Andersson Vice ordförande Johanna Magnusson Sidrah Schaider ersätter Anette Scheibe Lorentzi
Övriga närvarande	Anna Ullberg Ekonomichef Magnus Thulin Sekreterare
Paragraf	§7
Sekreterare	Magnus Thulin

§ 7
Dataskyddsombudets årsrapport 2023

STEM 2024/2

Beslut

Anmälan av årsrapporten godkänns.

Handlingar i ärendet

- 1519440 (Godkänd - R 1) Dataskyddsombudets årsrapport 2023
- 1517399 Dataskyddsombudets årsrapport 2023

Handläggare
Doris Serrato
Telefon: 08-50829921

Till
Styrelsen

Dataskyddsombudets årsrapport 2023

Förslag till beslut
Anmälan av årsrapporten godkänns.

Ärendet
S:t Erik Markutveckling anmäler i detta ärende dataskyddsombudets årsrapport 2023.

Magnus Thulin
tf VD

Bilaga
Dataskyddsombudets årsrapport 2023

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Magnus Thulin, tf VD	2024-02-29

Stockholms stad

GDPR Årsrapport

2023

S:t Erik Markutveckling AB

GDPR årsrapport
Januari 2024

Dnr: STEM 2024/2
Utgivningsdatum: 2024-01-08
Kontaktperson: Jessica Hillergård

Sammanfattning

I egenskap av S:t Erik Markutveckling AB:s dataskyddsombud lämnar jag följande årsrapport.
Dataskyddsåret har varit fullt av både upp och nergångar. Den 25:e maj firade GDPR 5 år sedan införandet och mycket har hänt och kommer hända. En snabb omvärldsbevakning pekar på att GDPR och det kommande NIS2-direktivet[1] kommer att ligga till grund för flera kommande förordningar inom EU. År 2023 var också året då terrorhotsnivån i Sverige höjdes och flertalet uppmärksammade incidenter med attacker mot myndigheter och organisationer skedde.

S:t Erik Markutveckling AB har under 2023 fortsatt arbeta systematiskt dataskyddsarbetet och arbetet sker efter ett årshjul. Under slutet av år 2022 engagerades också en medarbetare för tjänsten som informationssäkerhetssamordnare vilket har drivit arbetet framåt ytterligare under 2023.

En granskning har skett av ett biträde under året med en större brist framkom initialt då biträdets kontaktvägar inte fungerade. (E-postadresser för dataskyddsfrågor på deras hemsida.) Efter att avtalsparterna kontaktats uppvisar de samtliga dokument som efterfrågades. Bristen att biträdet kan ha svårt att uppfylla den registrerades rättigheter då kontaktvägar för allmänheten inte fungerar, är således något jag som DSO rekommenderar att det följs upp under 2024.

Jessica Hillergård

Dataskyddsombud

S:t Erik Markutveckling AB

[1] NIS2; Syftet med NIS2-direktivet är att harmonisera de olika medlemsländernas cybersäkerhetskrav och tillämpning av säkerhetsåtgärder samt stärka medlemsländernas samarbete för samhällsviktiga tjänster. NIS2-direktivet fastställer miniminivåer för regelverket och mekanismer för ett effektivt samarbete mellan tillsynsmyndigheterna i varje medlemsland.

Innehåll

Sammanfattning **3**

1 Bakgrund **5**

2 Obligatoriska rapporteringsområden **6**

2.1 Registerförteckning 7

2.2 Styrdokument 10

2.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar 12

2.4 Konsekvensbedömningar 14

2.5 Individens rättigheter 16

2.6 Personuppgiftsincidenter 18

3 Genomförda granskningar under året **20**

3.1 Sammanfattning 20

3.2 Syfte 20

3.3 Genomförda granskningar och deras resultat 20

3.4 DSO ger råd och rekommendationer till PUA 21

4 Risker inom dataskydd **22**

4.1 Sammanfattning 22

4.2 Syfte 22

4.3 Resultatet av riskkartläggningen 22

4.4 DSO ger råd och rekommendationer till PUA 23

5 Planerade granskningar under det nya verksamhetsåret **24**

5.1 Sammanfattning 24

5.2 Syfte 24

5.3 Planerade granskningar 24

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 bolagsstyrelsen behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud DSO. Dataskyddsombudet har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för styrelsen att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen. I rapporten får styrelsen insyn i vad dataskyddsombudets granskningar visat av verksamheten och status avseende integritet och dataskydd. Årsrapporten syftar till att styrelsen ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur styrelsen som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

2 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som personuppgiftsansvarig, PUA, som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är:

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter
- personuppgiftsincidenter

Nedan redogörs för bolagets status och dataskyddsombudets slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter dataskyddsombudets genomförda uppföljning och granskning.

2.1 Registerförteckning

2.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	15
Har nödvändiga uppdateringar gjorts?	JA
Bedöms registerförteckningen vara fullständig?	JA
Har verksamheten lämpliga rutiner för registerföring?	JA

2.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister eller register av register).

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att PUA får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna om individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

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

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamhetens har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

2.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

15 st.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Ja, finns dokumenterat i wordlogg och spårbarhet i Samarbetsytan STEM GDPR.

DSO bedömer hur fullständig registerförteckningen är

STEM använder sig av en Excelfil på en samarbetsyta för registerförteckningen. Den har samtliga områden som ska dokumenteras ifyllda.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

I årshjulet finns aktivitet nedtecknad när registerförteckningen ska kontrolleras och uppdateras vid behov.

2.1.4 DSO anger hur allvarliga bristerna är på en skala

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

2.1.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets råd är att fortsätta uppdatera registerförteckningen enligt årshjulet.

2.2 Styrdokument

2.2.1 Sammanfattning

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

2.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

En brist inom detta område bör förstås ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör lyftas fram till PUA. Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till bristande kvalitet i hur verksamheten utför aktiviteterna, men även till att verksamheten slösar värdefulla resurser när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

2.2.3 Resultat

S:t Erik Markutveckling har en GDPR-handbok där samtliga rutiner och kontaktpersoner finns beskrivna. Lokal anvisning för informationssäkerhet finns som kompletterande styrdokument och antogs samt implementerades 2023. Kontinuitets- och avbrottsplan saknas. (Se kapitel 4 Risker inom dataskydd.)

2.2.4 DSO anger hur allvarliga bristerna är på en skala

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

2.2.5 DSO ger råd och rekommendationer till PUA

Under 2024 kommer staden ta fram nya vägledningar för kontinuitetshantering. Dessa nya vägledningar behöver implementeras under kommande år för att dataskydd ska kunna omhändertas även vid en kris.

2.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

2.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Samtliga
Är klassade personuppgiftsbehandlingar aktuella?	JA

2.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att en klassning faktisk initieras.

Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s årsrapportering.

Viktigt är också att notera att Dataskyddsombudet omhändertar den registrerades intresse och informationssäkerhetssamordnaren har fokus på verksamhetens krav på informationen i form av tillgänglighet, riktighet och konfidentialitet. Verktyget för DSO är i första hand registerförteckningen och dokumentationen där.

Informationssäkerhetssamordnaren har KLASSA som verktyg för att se till att verksamhetens krav efterlevs i form av dokumentation i förvaltningsplaner, systembeskrivningar etc.

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare. Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll.

2.3.3 Resultat

STEM har valt att ta fram en egen klassificeringsguide baserat på de lagkrav som man efterlever förutom GDPR. I registerförteckningen anges klassning utifrån guiden.

2.3.4 DSO anger hur allvarliga bristerna är på en skala

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

2.3.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets råd är att vid den årliga genomgången av registerförteckningen också kontrollera att de tekniska och organisatoriska kraven efterlevs.

2.4 Konsekvensbedömningar

2.4.1 Sammanfattning

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

2.4.2 Syfte

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

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

2.4.3 Resultat

Under år 2023 har en konsekvensbedömning genomförts av STEM. Den var som en del av införandet av det digitala kommunikationsverktyget ZoomX.

2.4.4 DSO anger hur allvarliga bristerna är på en skala

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

2.4.5 DSO ger råd och rekommendationer till PUA

Vid varje ny upphandling av tjänst eller system bör dataskyddsombudet rådfrågas om konsekvensbedömningsfrågan behöver lyftas in som ett hjälpmedel för att få rätt kravspecifikation.

2.5 Individens rättigheter

2.5.1 Sammanfattning

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

2.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

Dataskyddombudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd hur processer och rutiner för att tillgodose rättigheterna bör utformas.

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningen krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från

Intetgritetsskyddsmyndighetens, IMY:s sida, med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

2.5.3 Resultat

I GDPR-handboken finns beskriven rutin för olika scenarion av begäran från en registrerad. Dock har det inte varit aktuellt med någon form av begäran av en registrerad under 2023.

2.5.4 DSO anger hur allvarliga bristerna är på en skala

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

2.5.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet ger som rekommendation att granska rutinen årligen för att hålla den uppdaterad.

2.6 Personuppgiftsincidenter

2.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	N/A
Hur många personuppgiftsincidenter har dokumenterats?	0
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	0

2.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska

personers rättigheter ska de berörda registrerade personerna, utan dröjsmål underrättas.

Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad osv.

2.6.3 Resultat

Då organisationen har en väldigt liten andel personuppgiftsbehandlingar med ett fåtal registrerade, så är det lätt att se om det sker personuppgiftsincidenter. Under 2023 har inga skett som rapporterats av STEM eller personuppgiftsbiträden.

2.6.4 DSO anger hur allvarliga bristerna är på en skala

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

2.6.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att ha en information om vad en personuppgiftsincident innebär med personalen årligen, så att kunskapen inte glöms bort.

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskningar:

- *Personuppgiftsbiträde*

3.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

3.3 Genomförda granskningar och deras resultat

Granskning 1 Personuppgiftsbiträde

Dataskyddsombudet har granskat ett personuppgiftsbiträde. En fullständig redovisning finns i rapport delgiven STEM i december 2023. Metoden var att skicka ut ett formulär med frågor via de e-postadresser som fanns angivna på biträdets hemsida. Initialt fick DSO inget svar, vid nästa förfrågan användes en mer allmän adress och då kom svar att frågan skickats vidare. Därefter hände inget. Efter påminnelser togs sedan ärendet upp med avtalsparten och då levererades svar på frågor och dokument som efterfrågats.

Bristen som kvarstår att granska till 2024 är att kommunikationsvägarna för registrerade d.v.s. den allmänna e-postadressen omhändertar frågor om dataskydd och eventuella begäran från registrerade.

	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 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet ger rådet att kontrollera biträdet under 2024 igen att deras kontaktvägar fungerar för de registrerade. Se kapitel 5.

4 Risker inom dataskydd

4.1 Sammanfattning

Relevanta risker inom verksamheten:

- Brist på kontinuitetshantering
- Registrerades rättigheter kan inte utövas hos biträde

4.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

4.3 Resultatet av riskkartläggningen

Risk 1 Kontinuitetshantering

Stockholm stad har under 2023 granskat sin dokumentation kring området kontinuitetshantering. Resultatet var att det fanns brister i de styrdokument som finns framtagna av stadsledningskontoret, SLK. Vid genomläsning finner jag som DSO inget stöd om hur dataskydd och informationssäkerhet omhändertas i händelse av att kontinuitetsplaner behöver aktiveras. STEM är en liten organisation och har däremot redan börjat tänka i dessa banor. Som ett gott exempel finns påbörjade diskussioner om reservbatterier/ powerbanks till personal. STEM följer det stödmaterial som stadsledningskontoret producerar, vilket gör att det saknas dokumentation likt det SLK fått anmärkning på som brist.

	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

Risk 2 Registrerades rättigheter kan inte utövas hos biträde
I granskningen framkom brist att biträde inte svarade på sina offentliga dataskyddsadresser. Det innebär en svårighet för registrerade som önskar utöva sina rättigheter. Vid granskningen svarade biträdet att de skulle åtgärda sina brister, därav en lägre nivå.

	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 DSO ger råd och rekommendationer till PUA

STEM behöver uppdatera sina kontinuitetsplaner när stödmallar kommer från SLK.

Ett nytt försök att testa biträdets förmåga att svara på de offentliga dataskyddsadresserna när en registrerad söker utöva sina rättigheter.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Personuppgiftsbiträde*

5.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett *riskbaserat synsätt*, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

5.3 Planerade granskningar

Granskning 1 Personuppgiftsbiträde

Under 2023 granskades personuppgiftsbiträde. Då var kommunikationsvägarna bristfälliga i de offentliga kanalerna. Under 2024 ska dessa prövas igen.

Resultatet presenteras i dataskyddsombudets årsrapport.

Signerat av

Detta dokument har signerats digitalt av följande personer

Namn	Datum
Anders Thomas,Andersson	2024-03-12
Johanna Charlotta,Magnusson	2024-03-11
Per Magnus,Thulin	2024-03-11