Stockholms stad

GDPR Årsrapport

2022

Spånga-Tensta
Stadsdelsförvaltning

GDPR årsrapport
Januari 2023

Dnr: ST 2023/12
Utgivningsdatum: 2023-01-17
Kontaktperson: Jessica Hillergård

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Spånga-Tensta har under år 2022 till min glädje som dataskyddsombud, prioriterat frågan om dataskydd och även informationssäkerhet. Flera brister i min rapport från 2021 har åtgärdats. Exempel på detta är aktiviteter med att uppdatera registerförteckningen, utse en intern grupp för medarbetarrepresentanter från verksamheterna och mål har satts upp för området i verksamhetsplanen för år 2023.

Jag är fortsatt nöjd med det arbete som förvaltningen gör när det sker personuppgiftsincidenter, men jag önskar en skriven rutin på intranätet.

Spånga-Tensta stadsdelsförvaltnings flytt föranleddes av en konsekvensbedömning av arkivet. På detta sätt kunde de risker som framkom under analysen omhändertas innan flytten.

DSO rekommenderar att tydliga ansvarsroller för dataskydd och informationssäkerhet utses i organisationen. Detta dokumenteras förslagsvis i den mall för tillämpningsanvisning som stadsledningskontoret tagit fram under 2022 och som följer stadens förvaltningsmodell PM^3.

De dataskyddsrisker som måste tas i beaktande under 2023 är länkad bland annat till att det kommer ske en hopslagning av Spånga-Tensta och Rinkeby-Kista stadsdelsnämnder i juli.

En gemensam risk för alla stadsdelsnämnder, bolag och förvaltningar inom Stockholm stad är att det saknas en tjänst för att e-posta säkert/ krypterat. Under hösten genomfördes en konsekvensbedömning av den tjänst stadsledningskontoret tagit fram kallat ”Säkra meddelanden”. Resultatet av de djupgående analyserna visade på brister och jag som dataskyddsombud kan inte rekommendera tjänsten i dagsläget. För att göra detta behöver riskerna först åtgärdas.

Jessica Hillergård

Dataskyddsombud

Innehåll

1 Inledning

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

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnden ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för nämndens 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 nämndens status och dataskyddsombudets slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter genomförd uppföljning och granskning.

2.1 Registerförteckning

2.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	201
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Nej

2.1.2 Syfte

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

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att 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

Registerförteckningen finns i ett digitalt verktyg kallat DraftIt och består av ett frågeformulär per personuppgiftsbehandling, vilket i sin tur blir funktionen av en checklista att alla krav i GDPR dokumenteras korrekt.

Registerförteckningen har uppdaterats under 2022 enligt framtagen handlingsplan. Rutin för att systematisera arbetet saknas.

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

2.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att tydliga ansvarsroller för dataskydd och informationssäkerhet, dvs vem som har ansvaret att uppdatera en informationsmängd i både registerförteckning för personuppgiftsbehandlingen en också utifrån informationssäkerhetskrav i KLASSA. Detta dokumenteras förslagsvis i den mall för tillämpningsanvisning som stadsledningskontoret tagit fram under 2022.

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?	Nej
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Nej
Är dokumenten uppdaterade?	Nej
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Nej

2.2.2 Syfte

Området syftar till att 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

Under 2022 antogs Stockholm stads nya informations-säkerhetsriktlinje. Stadsledningskontoret har därefter tagit fram en mall för tillämpningsanvisning. I det sistnämnda dokumentet förklaras och förtydligas stadsdelsförvaltningens lokala arbete med roller, informations- och dataskyddsrutiner etc. Denna tillämpningsanvisning finns *inte* antagen, implementerad och kommunicerad i förvaltningen.

Spånga-Tensta stadsdelsförvaltning saknar egna rutiner för dataskyddsarbetet. Den dokumentation är de generella dokument som finns framtagna på den stadsgemensamma GDPR-portalen på intranätet. Då de gemensamma ibland kan framstå som svåra att förstå och saknar kontaktuppgifter till de lokala funktionerna inom organisationen, så kan det vara lämpligt att en anpassning görs med en egen intranätssida. Ett pågående arbete finns för att ta fram årshjul. Det görs av den nystartade interna arbetsgruppen med dataskydd- och informationssäkerhetsambassadörer.

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

2.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att färdigställa tillämpningsanvisningen och därefter implementera och kommunicera den i organisationen. För att detta också ska få verkan i verksamheterna behöver medarbetare utses i de olika rollerna som följer stadens förvaltningsmodell. Detta betyder att det finns tydliga ansvarsroller och vem som gör vad i form av aktiviteter såsom behörighetskontroll, licenshantering, budgetansvar osv.

Det behöver tas höjd för att alla inte har åtkomst till datorer och intranät dagligen och information når inte fram till all personal. Lösningen med att ha information på affischer behöver övervägas om t.ex. vad en personuppgiftsincident är och vad man gör vid en sådan händelse. De organisationer som har sådana uppsatta har bättre förmåga att upptäcka och identifiera sådana.

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?	4
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

Under 2022 har flera gemensamma klassningar skett i verktyget KLASSA och en prioriteringsordning och arbetsfördelning för att dra nytta av fyrlingssamarbetet i Västerort[1]. Dock ska man beakta att samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Det kan vara i form av behörighetsbegränsning, skydd av lösenord på dokument osv. Detta dokumenteras i DraftIT, registerförteckningen.

Stadsdelsförvaltningen har börjat arbeta med metoden förklassningsprotokoll. Det är en protokoll-mall som skapats av stadsledningskontoret och syftar att få fram information inför en klassning i verktyget KLASSA. Protokollet har varit ett stöd i arbetet för att förstå om det finns personuppgifter i en process/system och kraven verksamheten har på tillgänglighet.

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

[1] Stadsdelsförvaltningarna i Bromma, Spånga-Tensta, Rinkeby-Kista och Hässelby-Vällingby arbetar tillsammans i dataskyddsfrågorna. Det kallas sedan 2018 ”Fyrlingen”.

2.3.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet rekommenderar att arbeta med förklassningsprotokoll och den metod staden tagit fram. I tillämpningsanvisningen tas också höjd för vem som har ansvaret att informationsklassningar och riskanalyser görs samt vem som ska genomföra dem. Rådet är att införa tillämpningsanvisningen och kommunicera denna.

2.4 Konsekvensbedömningar

2.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej
Har alla potentiella högriskbehandlingar konsekvensbedömts?	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

Organisationen arbetar med konsekvensbedömningar, främst de som är stadsgemensamma. Rutiner finns inte på plats utan man hänvisar till den centrala gemensamma intranätssidan. Aktiviteten idag sker individberoende, d.v.s. individer har kunskapen men inte bredden vilket kan försvåra processen.

2.4.4 DSO anger hur allvarliga bristerna är på en skala

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

2.4.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets råd är att sprida kunskapen om konsekvensbedömningen som verktyg till upphandling och sådan personal som är informationsansvariga. Eftersom det är ett individberoende i dagsläget så är det av vikt att flera förstår det och en rutin skapas och dokumenteras. Konsekvensbedömningen som verktyg skapar bättre kravställningar redan i designstadiet och förenklar/förtydligar i avtal och kommunikation med leverantörer. Rutin och ansvarsfördelning behöver formaliseras och dokumenteras. Förslagsvis sker det i tillämpningsanvisningen.

2.5 Individens rättigheter

2.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Kan ej anges då endast nekande registreras enligt Stadsarkivariens gallringsregler.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga då inga avvikelser framkommit

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

Stadsdelsförvaltningen saknar skriftliga rutiner på intranätet för hur individens rättigheter ska omhändertas för registerutdrag för medborgare. Processen för att få uppgifter rättade, raderade etc. behöver dokumenteras och kommuniceras. Dock löser man ut frågor vid behov, men det sker ad hoc.

2.5.4 DSO anger hur allvarliga bristerna är på en skala

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

2.5.5 DSO ger råd och rekommendationer till PUA

Idag sker arbetet av att enskilda individer kan lösa ut frågor. Därför är rådet att den interna arbetsgruppen för dataskydd tar fram en rutin/handledning som stöd tillsamman med nyckelfunktioner i verksamheten.

2.6 Personuppgiftsincidenter

2.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom individen/ personalen uppmärksammar dem alt meddelas av personuppgiftsbiträden.
Hur många personuppgiftsincidenter har dokumenterats?	18
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Rapport IMY: 1 Individen vid IMY-anmälan: 1
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	1

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

Organisationen är fortsatt bra på att upptäcka personuppgiftsincidenter och agera när dessa sker. Det saknas lättillgänglig rutin för hur man ska agera när det uppstår incidenter. Idag är det individberoende att arbetet sker.

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

2.6.5 DSO ger råd och rekommendationer till PUA

Kunskap om vad och hur man hanterar personuppgiftsincidenter är en färskvara. Det finns en tydlig korrelation mellan att personalen haft utbildning i dataskyddsförordningen och en ökad benägenhet att anmäla personuppgiftsincidenter.

Under 2023 behöver en instruktion publiceras som förklarar hur man agerar vid en personuppgiftsincident samt kommuniceras för att upprätthålla den goda kunskapen.

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskning

- *Granska intern kommunikation och utbildning*
- *Granskning av arkivflytt*

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) Granska intern kommunikation och utbildning
Under år 2022 har påminnelser skickats ut kontinuerligt om att medarbetare ska gå de utbildningar som finns inom dataskydd och informationssäkerhet på stadens gemensamma utbildningsplattform.

Information har framkommit att den statistik som kommer från utbildningsportalen är ibland fel. Det har visat sig att en del som genomgått utbildningen inte registrerats som genomförda. Därför ska siffrorna i ”pågående” tolkas som ”genomförd”. Resultatet är idag att ca 2/3 av medarbetarna har genomgått utbildningen.

Status	Antal av Status för genomförande
Genomförd	490
Har ännu inte påbörjats	371
Pågående	138
Totalsumma	999

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

Granskning 2 Granskning av arkivflytt
Under år 2022 skedde en större flytt när förvaltningen bytte lokaler. I och med detta skulle också det stora arkivet flytta fysiskt från de gamla lokalerna till nya. Detta skedde efter att risk- och konsekvensanalys genomfördes och åtgärder togs fram för att säkerställa att de registrerades rättigheter omhändertogs och ingen obehörig skulle få ta del av informationen. Dataskyddsombudet fick vara med under processen och har fått komma med råd när det har behövts. Stadsarkivet har också bidragit med sin expertis.

	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

3.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation inför 2023 är att säkerställa att personalen påminns kontinuerligt att gå den obligatoriska *årliga* utbildningen i dataskydd på utbildningsplattformen.

Önskvärt är att det blir ett krav att innan personalen får ut behörigheter och IT-utrustning måste man också genomgå kurserna på utbildningsplattformen i dataskydd och informationssäkerhet.

För den personal som inte har datorer som vardagligt arbetsredskap rekommenderas dessa verksamheter hittar en lösning där man går gemensamt vid ett APT, arbetsplatsträff, och sedan registreras det manuellt hos informationssäkerhetssamordnaren som har denna statistik.

4 Risker inom dataskydd

4.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Osäker e-posthantering med personuppgifter*
- *Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor*

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 Osäker e-posthantering med personuppgifter
Varje personuppgift som ska hanteras måste behandlas säkert. När en personuppgift e-postas med någon av stadens leveranser sker själva överföringen krypterat, men är okrypterad i in- och ut-boxen. Det är heller inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras på ett tillräckligt bra sätt.

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” eller ”TDialog”. Kvarstående aktivitet för verksamheten själv är att se över och bedöma vad tjänsten kan användas till. I ett större projekt med stadsdelsförvaltningarna i Bromma, Spånga-Tensta, Rinkeby-Kista, Hässelby-Vällingby och Hägersten-Älvsjö, har konsekvensbedömnings och informationssäkerhetsklassningsarbete samt riskanalys genomförts med verksamhetsrepresentanter, informationssäkerhetssamordnare och dataskyddsombud.

Flertalet risker kvarstår efter projektet och jag som DSO kan inte rekommendera i dagsläget att tjänsten används efter att jag tagit del

av analysmaterialet. Behovet är kvarstående från verksamheten att möjligheten att e-posta personuppgifter.

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

Risk 2 Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor

Vid arbete med KLASSA, vilket har varit fokus för stadsdelsförvaltningens informationssäkerhetssamordnare hösten 2022, framkommer det att det saknas dokumentation (både gemensam och lokal). Vid förfrågan kan sällan förvaltningsplan, systemdokumentation etc. tas fram av leverantören eller internt. Denna brist är allvarlig och gemensamma mallar för hur och vad dessa dokument ska innehålla behöver tas fram centralt. Risken är att man idag förutsätter det finns dokumentation för att det ”borde finnas” eller man ”antar” att det är på plats.

	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

4.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation för att minimera risken att personuppgifter e-postas utan tillräckligt skydd, är att de risker som kommit fram under projektet åtgärdas.

Genom att ta fram, implementera och kommunicera tillämpningsanvisningarna för informationssäkerhet och dataskydd kommer ansvaret bli tydligare för vem som ska ta fram dokumentationen som i dag saknas. Ett gemensamt arbete för utseende och innehåll behöver utföras.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granska intern kommunikation och utbildning*
- *Granska hopslagningen av stadsdelsnämnderna och dess förvaltningar i Rinkeby-Kista och Spånga-Tensta*

5.2 Syfte

Som nämnts tidigare 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

5.3.1 Granskning 1) Intern kommunikation och utbildning

Det är avgörande att för ett gott dataskydd att det finns en tillräcklig medvetenhet och kunskap inom organisationen om hur personuppgifter får och ska hanteras. Alla personer som hanterar personuppgifter, och de som bestämmer hur de ska hanteras, måste få en adekvat utbildning. Det är viktigt att utbildningen är aktuell och hålls uppdaterad. Förutom de grundläggande kunskaperna om begrepp, principer m.m. som alla behöver, finns det vissa grupper som därutöver kan behöva mer riktade utbildningsinsatser som ger djupare kunskaper.

Granskningen kommer att ske genom:

- Granska rutinerna för grundläggande utbildning till anställda och introduktion till nyanställda

- Granska genomförda utbildningsinsatser och sammanställ om möjligt statistik
- Granska grundutbildningens innehåll och säkerställ att den är aktuell

5.3.2 Granskning 2) *Granska hopslagningen av stadsdelsnämnderna och dess förvaltningar i Rinkeby-Kista och Spånga-Tensta*

Stadsdelsförvaltningarna Rinkeby-Kista och Spånga-Tensta ska slås ihop i juli 2023. Med detta kommer också en stor mängd nya personuppgiftsbehandlingar att uppstå. Dataskyddsombudet kommer att granska att de registrerades rättigheter omhändertas och den nya personuppgiftsansvariga nämnden är följsam med förordningen.

Granskningen kommer att ske genom:

- Kontroll att registerförteckningarna i stadsdelsförvaltningarna omhändertas på enligt korrekt livscykel och ny skapas.
- Konsekvensbedömning och riskanalyser genomförs för eventuella flyttar av arkiv.

6 Övrigt att rapportera

6.1 Sammanfattning

Det behövs oftast en arbetsgrupp som tar det praktiska ansvaret för dataskyddsarbetet, både att identifiera vad som behöver göras och att genomföra det. Det räcker sällan med ett ensamt dataskyddsombud eller en ensam ansvarig person, utan det krävs en laginsats. Dataskyddsombudet ska också ha en granskande roll vilket försvårar att också vara en projektledare för implementation och framtagande av styrdokument.

6.2 Övriga observationer

Observation 1 Intern arbetsgrupp för GDPR och informationssäkerhetsfrågor

Spånga-Tensta stadsdelsförvaltning har under 2022 startat en intern arbetsgrupp med representanter från verksamheten. Dessa kallas dataskydds- och informationssäkerhetsambassadörer. I rapporten från år 2021 togs det upp som en brist men är nu åtgärdad.

En sammankallande medlem för gruppen är utsedd för gruppen och som också har till uppgift att hålla ihop arbetet. Detta för att göra dataskyddsombudsrollen mindre operativ.