Stockholms stad

GDPR Årsrapport

2023

Bromma Stadsdelsförvaltning

GDPR årsrapport
Januari 2024

Dnr: BRO 2024/43
Utgivningsdatum: 2024-01-15
Kontaktperson: Jessica Hillergård

Sammanfattning

I egenskap av ert 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. Bland annat kan det omnämnas att regleringar kommer ske inom områdena AI, IoT (Internet of Things) och DMA, Förordningen om Digitala Marknader[2] vilket alla påverkar stadsdelsförvaltningens dagliga arbete. År 2023 var också året då terrorhotsnivån i Sverige höjdes och flertalet uppmärksammade incidenter med attacker mot myndigheter och organisationer skedde. Det i sin tur har också lett till en ny syn på behov av säkerhetskontroller och krisorganisationer vilket inte varit så tydligt tidigare.

Som Dataskyddsombud, DSO, för Bromma sdf. har jag främst arbetat med frågan om ZoomX under år 2023. Kraven på digital kommunikation och lösningar för detta har varit stora sedan första dagarna av pandemin. Det befintliga verktyget Skype har börjat bli föråldrat och uppdateras inte av leverantören i den takt som behövts. Stockholm stad har nu implementerat en europeisk variant av Zoom kallad ZoomX och är baserad i Tyskland. Verktyget implementerades under hösten 2023. I spåren av detta har också flera andra tankar om verktyg för kommunikation också diskuterats inom organisationen då nya krav tillkommit. Bland annat behövs lösningar för socialtjänsten för säkra möten över starkare kryptering och identifiering.

Året har fortsatt inneburit behov och krav på säkra digitala meddelanden, en tjänst att kunna skicka e-post krypterat. Vid rapportens framtagande finns det nu ett pågående projekt på

---

[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.

[2] Förordningen om digitala marknader; Syftet är att hindra så kallade grindvakter från att bland annat ställa oskäliga villkor för företag och slutanvändare och att säkerställa öppenhet när det gäller viktiga digitala tjänster. EU-kommissionen utsåg i september 2023 för första gången sex grindvakter: Alphabet, Amazon, Apple, ByteDance, Meta och Microsoft. Detta gjorde de med stöd av olika kriterier i DMA som avgör om ett företag är en grindvakt. Efter att ha betecknats som grindvakter har företagen sex månader på sig att följa listan över vad de får göra och inte får göra enligt DMA, så att slutanvändare och företagsanvändare av grindvakternas tjänster får mer valmöjligheter och större frihet.

stadsledningskontoret för att genomföra en stadsgemensam konsekvensbedömning. En remiss för underlag är framtaget och nästa steg är work-shops med verksamhetsrepresentanter. Med arbetet har också behovet av en process som styr stadsgemensamma konsekvensbedömningar synliggjorts ytterligare i nätverket av DSO: er till SLK.

Ett förnyat inriktningsbeslut (KS 2023/241) kom hösten 2023 angående användande av tredjelandsöverföringar i Stockholm stad. Detta har öppnat upp för att stadsdelsförvaltningen kan fatta beslut i frågorna men med förbehållet att exit-plan behöver finnas på plats. Detta då överenskommelsen mellan USA och EU/EES bygger på en så kallad ”President order” och kan rivas upp av en ny amerikansk president efter valet 2024 eller vid en rättslig prövning. Detta ställer i sin tur höga krav på förvaltningen av informationstillgångar.

År 2023 har implementeringen av styrmodellen PM^3 fått mest uppmärksamhet ute i verksamheten. Det är en del av stadens arbete med informationssäkerhet som bland annat pekar ut ansvarsroller och ett sätt att bli mer systematiskt. Förklassningar har genomförts och roller har tilldelats medarbetare.

År 2024 kommer med stor sannolikhet fortsatt bli prioriteringar inom kontinuitetsplanering för att kunna hantera informationssäkerhet och dataskydd i krig och kris. Omvärlden har blivit kallare och vi ser en ökad påverkan efter så kallade hybridattacker där myndigheter och företags hemsidor stängs ner. Det är ett sätt att skapa otrygghet och instabilitet i samhället för antagonister. Flera aktioner är också riktade mot kommun vad gäller att sprida desinformation om socialtjänsten. Allt detta påverkar oss dagligen och min förhoppning är att jag nästa år kan ge en ljusare bild i min sammanfattande omvärldsbevakning och inledning.

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 *dokumenteringsskyldighe*t. 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?	114
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 i 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.

Totalt har 114 behandlingar registrerats i DraftIt. Under år 2023 har översyn gjorts av DSO samt en granskning mot hanteringsanvisningen.

Arbetet med registerförteckningen saknar en skriven rutin. Idag sker detta ad hoc och är beroende av kunskap hos den enskilde anställde. Med införande av PM[3] kommer denna arbetsuppgift bli tydligare och lättare att genomföra då ansvaret är utpekat på en specifik roll.

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

Nästa steg för förvaltningens arbete med registerförteckningen är att implementera de roller som anges i förvaltningsmodellen PM[3] som Stockholms stads verksamheter ska följa. I den finns roll för vem som är informationsansvarig, den som är ansvarig att utföra

kontroller osv. I rollbeskrivningen ska det också framkomma vem som är ansvarig för att hålla registerförteckningens olika personuppgiftsbehandlingar uppdaterade och lägga in nya behandlingar.

För att underlätta arbetet med registerförteckningen kan man med fördel lyfta in hanteringsanvisningen från Stadsarkivet som stöd för att förtydliga i vilka processer som behandlingarna går in under.

2.2 Styrdokument

2.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	JA
Håller innehållet i de existerande dokumenten lämplig kvalitet?	JA
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	JA
Är dokumenten uppdaterade?	JA
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 Dataskyddsförordningen 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

En stor förbättring har skett under 2023 vad gäller styrdokument inom stadsdelsförvaltningen. (För år 2022 markerades bristerna som omfattande, orange i nedan skala.) Tillämpningsanvisningen har tagits fram och med den också flertalet rutiner och handledningar.

En uppdatering av intranätet ledde under en period att styrdokument försvann och en viss förvirring om kontaktvägar och rutiner uppstod. En brist som kvarstår till viss del då synligheten för dokument är komplicerad och styrs inte av stadsdelens information först utan centrala mer övergripande texter. Det är också en hel del begreppsförvirring (dataskydd blandas in på sidor för informationssäkerhet och tvärt om) och det är svårt att hitta information för verksamheterna.

Svårigheterna att hitta information på intranätet gör att bedömningen blir gul. Kvalitet och innehåll är grönt.

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

Bromma stadsdelsförvaltningsnämnd rekommenderas att om möjligt påverka synligheten för interna styrande dokument på intranätet.

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?	45 st. Förklassningar av system
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 år 2023 har fortsatt arbete skett med förklassningsprotokoll och då i tre steg vilka är: A-klassning i designfasen, B-klassning vid införandet och C-klassning vid årlig uppföljning. Protokollet från dessa ska signeras av informationsägaren, i dagsläget direktören, och har konkretiserat skyddsvärdet för informationen och då även personuppgifterna som kan ingå i dessa. Dataskyddsombudet har blivit inbjuden till sådana vid flertalet tillfällen och metoden börjar sätta sig i organisationen parallellt med implementeringen av förvaltningsmodellen PM[3]. Arbetet har tagit ett stort kliv fram och en prioriteringsordning har följts.

Värt att notera är att det inte är informationstillgången som klassats utan systemet/informationsbäraren.

Samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Detta kan vara behörighetsbegränsning, skydd av lösenord på dokument osv. Detta dokumenteras i DraftIT. En klassificeringsstruktur med märkning av dokument finns inte

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

.

2.3.5 DSO ger råd och rekommendationer till PUA

Tidigare år har klassningar skett ad hoc och varit drivna av enskilda individer. Med PM[3] har detta problem reducerats då ansvariga inom organisationen utsetts. Organisationen är dock ung och fortsatt utbildningsinsatser behövs.

Rekommendationen från DSO är att fortsätta se till nästa steg i införandet förvaltningsmodellen av informationssäkerhet och klassificera de processer som ingår i hanteringsanvisningen. Identifierar man processer och inte ser endast till system, blir klassningen av information än mer konkret och verklig.

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

Organisationen arbetar med konsekvensbedömningar. Rutiner finns på plats i tillämpningsanvisningen. Aktiviteten sker dock individberoende, d.v.s. individer har kunskapen men inte bredden vilket kan försvåra processen med att använda verktyget. Med införande av PM[3] blir ansvaret tydligare för vem som ska tillse att resurs avsätts för att uppgiften konsekvensbedömning sker.

Under året har en stor konsekvensbedömning skett gemensamt i staden för ZoomX och ett projektarbete är uppstartat för förskolans nya närvaroplattform. Det har synliggjorts under året hur viktigt det

är med gemensam konsekvensbedömningsprocess och behovet av att ha utsedd ledare för det. Det uppstår ofta tidspress i det här arbetet då konsekvensbedömningar görs väldigt sent i framtagande av tjänster. Värt att notera är att stadsdelsförvaltningen själv löser ut sina egna aktiviteter inom konsekvensbedömningar utan drabbas negativt i det gemensamma arbetet.

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

Konsekvensbedömningen som verktyg skapar bättre kravställningar redan i designstadiet och förenklar/förtydligar i avtal och kommunikation med leverantörer. I förvaltningsmodellen PM[3] är det ett ansvarsområde som tilldelas en specifik roll. Vid implementering av modellen kommer det att förflytta individberoendet vilket det är idag, till ett mer systematiskt använt verktyg.

Nämnden behöver också fortsatt arbeta för att process för gemensamma konsekvensbedömningar i staden implementeras, därav den gula bedömningen.

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 Integritetsskyddsmyndighetens, IMY:s sida, med sanktioner som

följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

2.5.3 Resultat

På intranätet finns information om den registrerades rättigheter och vad de innebär. Dock har den interna rutinen inte publicerats där utan finns endast hos registrator. (Togs fram under slutet av år 2022.)

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

Nämnden rekommenderas att granska intranätets interna rutiner och externwebbens information under 2024. Detta då informationen på intranätet gjordes om under 2023 och extern-webben likaså.

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?	19
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Rapport IMY: 2 Individen vid IMY-anmälan: 0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	2

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 Dataskyddsförordningen 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

De incidenter med personuppgifter som skett hos Bromma stadsdelsförvaltning under 2023 är fortsatt av olika art och är främst av typen att de är information som kommit fel vid utskick eller obehörig åtkomst. Ingen anmälan har skett till tillsynsmyndigheten efter 72h. Medarbetare agerar bra vid större incidenter och löser sina arbetsuppgifter. En organisation att omhänderta lessons learned saknas och är nästa steg att utveckla i detta arbete.

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

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.

Nämnden rekommenderas att ta fram en organisation att omhänderta lessons learned. Det är en naturlig del av det förbättringsarbete som en mer mogen verksamhet kan ta nästa steg emot.

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskningar:

- Granska intern kommunikation och utbildning
- Implementationen av nya informationssäkerhetsriktlinjen och dess tillämpningsanvisningar

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
Granskningen som genomförts är hur utbildning och information om dataskydd skett i organisationen under 2023. En genomgång av utbildningarna har också gjorts och där finns inget att anmärka på faktainnehåll.

Staden har tagit fram flera utbildningar inom informationssäkerhet och dataskydd. Ett av de problem som flaggats av Dataskyddsombuden i staden är brist på möjlighet till uppföljning och att Dataskyddsombudet får ”tjata” på medarbetarna att gå de årliga obligatoriska utbildningarna. Som ett led av ett förbättringsarbete har staden tagit fram en årlig certifiering. Det innebär att det automatiskt sker ett utskick till medarbetarnas mail att de ska genomgå en obligatorisk utbildning. Strax innan sommaren 2023 startade certifieringarna av informationssäkerhet och under hösten certifiering i dataskydd. Dataskyddsombudet har uppmärksammats på att certifieringsutbildningarna infördes utan att någon informerades. Detta är beklagligt och berodde på att inte heller DSO eller Informationssäkerhetssamordnare fick information

om införandetidpunkt. Önskvärt är att det informeras tydligare från centrala funktioner i staden när en sådan förändring sker.

Uppföljning av statistik har ej kunnat genomföras då fel i rapportuttaget skett i beställningsportalen. Felet har påpekats av flera ISAM i staden till SLK IKT vid årsskiftet.

En rekommendation från 2022-års dataskyddsrapport har fångats upp av centrala funktioner. Det var att det ska finnas utbildning även för den personal som inte har egen dator. Under 2024 ska en sådan implementeras och genomföras i anslutning till exempelvis informationsmöte eller APT. Hur statistik från deltagande ska redovisas har inte framkommit vid den här rapportens framtagande.

	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

Granskning 2 Implementationen av nya informationssäkerhetsriktlinjen och dess tillämpningsanvisning

Arbetet med att implementera tillämpningsanvisningen har fortskridit med att bland annat ta fram en PM[3]-organisation och utse nyckelroller samt identifiera system och informationsmängder. I tillämpningsanvisningen finns också flertalet rutiner publicerade som omhändertar administrativa skyddsåtgärder.

Kvarstående är samtlig dokumentation för respektive informationsägare att ta fram via sina informationsansvariga. (Det kan vara rutiner med kontroller etc.) Detta så att tillämpningsanvisningen med informationsklassning blir ett stöd för att rutiner tas fram som visar verkligheten och individbetroendet minskar och arbetet med informationstillgångar samt personuppgifter blir mindre sårbart.

	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 utbildningarna inom informationssäkerhet och dataskydd genomförs i organisationen. Dessa är obligatoriska och ska genomföras årligen. Ombesörja att den utbildning som implementeras för medarbetare utan egen dator är adekvat och korrekt samt statistik om deltagande fångas upp.

Trots den certifiering som införts behöver det fortfarande påminnas om i organisationen att medarbetarna ska gå utbildningarna och att tid avsätts för detta av cheferna i organisationen.

Dataskyddsombudets råd är att fortsätta arbetet med att implementera PM[3] och göra arbetet med informationstillgångar/ personuppgifter mindre individberoende. På det sättet kommer mognadsgraden öka i organisationens informationssäkerhets- och dataskyddsarbete.

4 Risker inom dataskydd

4.1 Sammanfattning

Relevanta risker inom verksamheten:

- Osäker e-posthantering med personuppgifter (Kvarstår)
- Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)
- Tredjelandsöverföringar (Ny)
- Skyddade personuppgifter inom förskolan (Ny)

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 utboxen. Det är också 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, är att se över och bedöma vad tjänsten kan användas till. I ett större projekt med stadsdelsförvaltningarna i Bromma, Järva, Hässelby-Vällingby och Hägersten-Älvsjö, har konsekvensbedömnings och informationssäkerhetsklassningsarbete samt riskanalys genomförts med verksamhetsrepresentanter, informationssäkerhetssamordnare och dataskyddsombud.

Jag som DSO kan inte rekommendera i dagsläget att tjänsten används efter att jag tagit del av analysmaterialet. Samtidigt är

behovet kvarstående från verksamheten att möjligheten att e-posta personuppgifter säkert och krypterat.

Vid denna rapports framtagande är ett projekt med att en gemensam konsekvensbedömning med systembeskrivning, informationsklassning och riskanalys ska ske 2024 av SLK. Detta för att kunna besvara de risker som framkommit inom de verksamheter som gjort ena konsekvensbedömningar och riskanalyser. Rekommendationen att inte använda tjänsten utan att analysmaterialet finns på plats kvarstår, då riskerna inte har besvarats av systemförvaltaren och informationsmängderna som ska skickas i det är så pass känsligt och skyddsvärt.

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 (Kvarstår)

Vid arbete med KLASSA, vilket har varit fokus för stadsdelsförvaltningen i år, framkommer det att det saknas dokumentation (både gemensam och lokal). Vid förfrågan kan sällan förvaltningsplan, systemdokumentation etc. tas fram av leverantören eller den egna förvaltningen. 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

Risk 3 Tredjelandsöverföringar (Ny)
Det nya inriktningsbeslutet från stadsledningskontoret som kom under hösten 2023 innebar en öppning för stadsdelsförvaltningarna att använda leverantörer som använder sig av tredjelandsöverföringar. Förutsättningen är att verksamheten har en väl utformad exit-plan om överföringsmekanismen ”Data Privacy Framwork” ogiltigförklaras likt ”Privacy Shield” gjorde år 2020 och ”Safe Harbour” innan dess.

Flertalet leverantörer erbjuder idag endast molntjänster och de stora leverantörerna av sådana är amerikanskägda. Därav är detta en risk som behöver uppmärksammas extra.

	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 4 Skyddade personuppgifter inom förskolan (Ny)
Problem har uppdagats under år 2023 att det finns brister inom hanteringen av skyddade personuppgifter inom förskolan. Det gäller både för personal och barn med vårdnadshavare.

	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.

Risken att tredjelandsöverföringsproblematiken kommer att uppstå igen är sannolikt rätt stor. Nätaktivistorganisationen NOYB, Non Of Your Business, har sagt att man kommer göra en rättslig prövning och då trolige redan årsskiftet 2023-2024. Samtidigt bygger överföringsmekanismen på en presidentorder vilken kan rivas upp av nästa president efter valet 2024. Nämnden rekommenderas att ta höjd för risken och bestämma aptiten för vad man är villig att riskera när man ingår nya avtal med leverantörer där överföringar till tredjeland sker. Rådet är också att ha en tydlig exitplan och genomlysa marknaden i förstahand inom Sverige och EU/EES.

Vid införandet av nya skolplattformen behöver perspektivet skyddade personuppgifter omhändertas särskilt. Nämnden rekommenderas att granska detta extra noggrant 2024. (Se kapitel 5 Granskning 1.)

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granskning 1* Granska förskolans införande av nya skolplattformen
- *Granskning 2* Hur väl fungerar den nya ej digitala dataskyddsutbildning?
- *Granskning 3* Har användandet av de tre e-tjänsterna inom socialasystem implementerats

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 Granska förskolans införande av nya skolplattformen

Under 2023 upphandlades två stycken nya verktyg för förskolan som ska ersätta den befintliga skolplattformen. Införandet ska ske under 2024 Q2 och Q4. Historiskt sett vid det förra införandet fanns flertalet problem med att omhänderta bland annat dataskyddsreglerna och personer med skyddad identitet.

Syftet med att specifikt granska detta är att på djupet förstå att historiken inte upprepar sig där personuppgifter inte skyddats tillräckligt utifrån gällande lagstiftningar.

5.3.2 Granskning 2 Hur väl fungerar den nya ej digitala dataskyddsutbildning?

Den nya dataskyddsutbildningen som ska tas fram för medarbetare som inte har tillgång till egen dator behöver granskas kvalitativt och hur många som deltagit i den samt deras omdöme om den.

5.3.3 Granskning 3 Har användandet av de tre e-tjänsterna inom socialsystem implementerats?

Under åren 2022-2023 har tre nya e-tjänster för socialasystem tagits fram. Dessa var: Digital orosanmälan, Ansökan om ekonomiskt bistånd samt Digital föräldraskapsanmälan. Indikationer har framkommit att man fortfarande inte ger rådet att använda delar av dessa leveranser då det finns osäkerheter kring dem. Under 2024 ska dessa e-tjänster granskas av DSO i syfte att se hur och om de används.

6 Övrigt att rapportera

6.1 Projektgrupp för informationssäkerhet och dataskydd

Under våren 2023 skapades en projektgrupp för att ta fram och implementera tillämpningsanvisningen för informationssäkerhet. Gruppen har letts av Maria Palme med deltagande av arkivarie, informationssäkerhetssamordnare, Dataskyddsombud, telefonisamordnare och vid behov även andra medarbetare med specialistkunskap. Gruppen har bland annat utbildat ledningsgruppen i PM^3-modellen, informationssäkerhet, hantering av allmänna handlingar mm. Inför och vid olika revisioner har gruppen stöttat varandra med kunskap då vissa funktioner var nya inom organisationen 2023.

Projektet har med sina gemensamma ögon kunnat bidra med en helhetssyn på området dataskydd och informationssäkerhet. Nämnden ges rådet att fortsätta med denna projektgrupp.

6.2 Gemensamt arbete inom Trillingen

Under år 2023 slogs stadsdelsnämnderna i Rinkeby-Kista och Spånga-Tensta ihop till Järva. Det innebar att jag som DSO fick en Trilling att arbeta med istället för den tidigare Fyrlingen. Synergieffekterna är fortfarande desamma och det blir särskilt tydligt när det sker en incident eller vid införanden av nya tjänster. Under 2024 kommer också ett mer regelbundet arbete ske mellan stadsdelsförvaltningarnas informationssäkerhetssamordnare, ISAM, och dataskyddsombudet. Detta för att dra nytta av varandras arbete och kunskaper då respektive ISAM har helt olika bakgrund inom teknik, arkivkunskap osv.