Stockholms stad

GDPR Årsrapport

2022

Bromma Stadsdelsnämnd

GDPR årsrapport
Januari 2023

Dnr: BRO 2022/504
Utgivningsdatum: 2022-01-17
Kontaktperson: Jessica Hillergård

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Under året som gått har stadsdelsförvaltningen varit aktiva i att uppdatera registerförteckningen, en brist som togs upp i förra årets rapport. Förvaltningen har också deltagit vid flera gemensamma konsekvensbedömningar och informationssäkerhetsklassningar.

Fyra utbildningstillfällen för rollen ”behöriga beställare” har genomförts under året med inriktning på dataskydd och informationssäkerhet.

Stadsdelsförvaltningen har haft 25 stycken personuppgiftsincidenter under året, varav 4 stycken har anmälts till tillsynsmyndigheten IMY, Integritetsskyddsmyndigheten.

Under år 2022 antogs stadens nya informationssäkerhetsriktlinje. Under sommaren kom sedan den mall för tillämpningsanvisning som ska bryta ner riktlinjen i hur verksamheten ska arbeta. Under arbetet med anpassningen av anvisningen för Bromma stadsdelsförvaltning, framkommer tydligt att nämnden behöver implementera stadens förvaltningsmodell PM^3.

En gemensam brist och stor 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. För att göra det behöver riskerna först åtgärdas.

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 2022 har registerförteckningen uppdaterats av verksamheterna själva med hjälp av dataskyddsambassadörerna.

Arbetet med registerförteckningen saknar en skriven rutin. Idag sker detta ad hoc och är beroende av kunskap hos den enskilde anställde. Rutinen behövs för att det ska bli ett systematiskt arbete och inte personberoende.

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

För att registerförteckningen ska hållas aktuell och uppdaterad behövs en skriftlig rutin vem som är ansvarig för arbetsuppgiften och när personuppgiftsbehandlingar som hen ansvarar för ska följas

upp årligen. Det kan med fördel tecknas ned i tillämpningsanvisningen.

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

Bromma stadsdelsförvaltning har egen handledning för hur personuppgiftsincidenter ska hanteras samt en förklaring om vad GDPR innebär. Dessa finns publicerade på Bromma stadsdelsförvaltnings intranät. I övrigt hänvisas till de generella dokument som finns framtagna på den gemensamma GDPRportalen på intranätet. Då de gemensamma rutinerna 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 handledning.

Ett arbete med att ta fram årshjul och tillämpningsanvisning är påbörjat under hösten 2022.

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

Bromma stadsdelsförvaltningsnämnd rekommenderas att fortsätta arbetet med tillämpningsanvisningen och utse roller enligt stadens förvaltningsmodell PM^3. När detta är klart behövs en implementations- och kommunikationsplan tas fram.

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?	3 st. i KLASSA 3.5 1 st. i KLASSA 4.0
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

Informationsklassning sker efter förklassningsprotokoll framtaget av SLK. Dokumentet ger en första bedömning och stöd innan den större aktiviteten med verktyget KLASSA. Ett gemensamt arbete sker mellan stadsdelsförvaltningarna i ”Fyrlingen”, dvs. Bromma, Spånga-Tensta, Rinkeby-Kista och Hässelby-Vällingby. En handlingsplan med prioritering för gemensamma klassningar är framtagen av Fyrlingens informationssäkerhetssamordnare.

Det finns 1 st. system registrerade i verktyget KLASSA 4.0. Tillsammans med de andra förvaltningarna finns ytterligare 6 st. dokumenterade som framtagna handlingsplaner vilket är utkomsten från verktyget KLASSA.

Dock ska man beakta att 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.

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
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

.

2.3.5 DSO ger råd och rekommendationer till PUA

Utmaningen som identifierats i arbetsuppgiften med informationsklassning är bristen på förståelse för uppgiften inom

verksamheten. DSO rekommenderar att ledningen beslutar att implementera den tillämpningsanvisning som tagits fram, och roller utses så att arbetet kan systematiseras då det idag sker ad hoc.

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 inte på plats 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 att de genomförs.

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 skapa en rutin och 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.

Konsekvensbedömningen som verktyg skapar bättre kravställningar redan i designstadiet och förenklar/förtydligar i avtal och kommunikation med leverantörer.

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 tydliga skriftliga rutiner på intranätet för hur individens rättigheter ska omhändertas för registerutdrag för medborgare. Processen för att få uppgifter rättade, raderade o.s.v. behöver dock dokumenteras och kommuniceras. Under senhösten 2022 har en rutin för utlämning tagits fram som inte har kommunicerats och implementerats vid den här årsrapportens upprättande.

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 med att omhänderta den registrerades rättigheter genom att enskilda individer kan lösa ut frågor. Därför är rådet att den interna arbetsgruppen för dataskydd tar fram en rutin/handledning som stöd förutom den rutin för utlämning som redan är framtagen.

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?	25
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Rapport IMY: 4 Individen vid IMY-anmälan: 3
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	4

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

De incidenter med personuppgifter som skett hos Bromma stadsdelsförvaltning under 2022 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.

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.

Under 2023 behöver instruktionen som förklarar hur man agerar vid en personuppgiftsincident kommuniceras igen för att upprätthålla den goda kunskapen.

3 Genomförda granskningar under året

3.1 Sammanfattning

Genomförda granskningar:

- Granska intern kommunikation och utbildning
- Fungerar processerna för att hantera de registrerades rättigheter

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

Staden har två obligatoriska utbildningar för medarbetare och konsulter. De två finns tillgängliga digitalt på utbildningsplattformen. De två kallas ”dataskydd och ”informationssäkerhet för medarbetare i staden”. Förutom dessa två finns en informationssäkerhetsutbildning särskilt för chefer inom Stockholm stad.

Det har visat sig vid uppföljning att det finns felaktigheter i den statistik som kommer från stadsledningskontoret. Därför ska siffrorna i ”pågående” tolkas som ”genomförd”.

Vid möten med andra stadsdelsförvaltningar har det lyfts att flera inte har egen dator utan vill istället utföra utbildningen gemensamt vid en arbetsplatsträff, APT. Ett utbildningssätt inte Bromma gör idag.

Status E-utb. dataskydd	Antal av status för genomförande
Genomförd och påbörjad	592
Har ännu inte påbörjats	1396
Totalsumma	1988

Fördjupad utbildning i dataskydd och informationssäkerhet har genomförts vid fyra tillfällen under året. Deltagare har alla haft rollen ”behörig beställare” och är chef inom Bromma stadsdelsförvaltning.

	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 Fungerar processerna för att hantera de registrerades rättigheter

När en begäran inkommer till Bromma stadsdelsförvaltning påbörjas direkt en rad aktiviteter. Dessa sker inom rimlig tid men är personberoende att det sker på rätt sätt. Under hösten 2022 omhändertogs problemet med personberoendet av den nya arkivarien som arbetat fram en skriftlig rutin för utlämnanden.

	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. En rutin behöver tas fram för hur den personalen utan tillgång till egen dator, ska kunna genomföra utbildningarna samt att detta fångas upp statistiskt.

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.

Rutinen för utlämnande behöver kommuniceras i verksamheten under 2023. En rutin för att omhänderta övriga rättigheter för den registrerade behöver tas fram.

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 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, Spånga-Tensta, Rinkeby-Kista, Hässelby-Vällingby och HägerstenÄlvsjö, 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 säkert.

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 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

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 så att tjänsten ”Säkra meddelanden” kan användas.

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.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

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

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.

- 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

5.3.1 Granskning 2 Implementationen av nya informationssäkerhetsriktlinjen och dess tillämpningsanvisningar

Under 2023 kommer DSO att granska implementationen, dvs. förståelsen i verksamheten, och kommunikationen av styrdokument.

Detta kommer ske genom att DSO följer upp att rollfördelning och ansvarsförhållanden är omhändertagna i verksamheterna. Detta kan bestå av stickprov att förvaltningsplaner är framtagna och att granska behörigheter finns på plats och utförs.

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. 2022 slutade den person som varit sammankallande för gruppen och en ny har utsetts. Förhoppningen är då att gruppens arbete kan upptas igen år 2023.

Under år 2022 har ett arbete påbörjats med att ta fram årshjul och utveckla utbildningarna i informationssäkerhet och dataskydd. Detta har lett till flera åtgärder och flera punkter som tas upp i internkontrollen 2023. En bra utveckling för att synliggöra området för verksamheten.