Stockholms stad

Bilaga 4

GDPR Årsrapport

2021

Spånga-Tensta Stadsdelsförvaltning

GDPR årsrapport
Januari 2021

Dnr: YYYY
Utgivningsdatum: 2021-01-27
Kontaktperson: Jessica Hillergård

1 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Spånga-Tensta har under år 2021 fortsatt haft ett ansträngt utgångsläge pga. pandemin. Utifrån dataskydd har detta inneburit att frågan prioriterats ned. Men det finns flera goda initiativ inom personalstyrkan där frågan är mycket aktuell. Ett par exempel är konsekvensbedömning innan upphandling av nytt dokumentationssystem, utredningsarbete om utlämning av personuppgifter m.m. Önskemålet är nu att stadsdelsförvaltningen fångar upp dessa och skapar en intern arbetsgrupp som kan överföra sina goda egenskaper och initiativ till hela organisationen. Denna grupp kan också vara aktuell att ta fram de lokala styrdokument som saknas. En brist som måste åtgärdas är arbetet med registerförteckningen som inte uppdaterats och saknar lokal rutin så att detta på sikt kan ske systematiskt.

Under året har flera personuppgiftsincidenter skett, 18 st. varav en fick ett visst medialt intresse. Organisationen agerar alltid snabbt och med tydliga åtgärder både för skademinimering, framåtblickande och kommunikationsmässigt. Den är väl förberedd och håller sig till utsatt incidentplan vilket är mycket bra. Antalet incidenter visar också på att organisationen har en öppenhet att våga tala om det och förstår varför man behöver göra det.

Spånga-Tensta stadsdelsförvaltning står inför en flytt och det är med fördel man tittar på sin samarbetspartner Bromma sdf som genomgick samma sak under 2021. Där uppmärksammades en del åtgärder som kan vara bra att ta med som lärdom utifrån dataskydd och informationssäkerhetsfrågorna.

Jessica Hillergård

Dataskyddsombud

Innehåll

2 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.

3 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.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	169
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nej

3.1.2 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.

3.1.3 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. SLK har beslutat under år 2019 att de tidigare Excel-listor med registerförteckningar som skapades 2018, ska digitaliseras i verktyget DraftIt. När listan fördes över från Excel till DraftIt under 2019 framkom kunskapsluckor om personuppgiftsbehandlingarna. Detta då den initiala Excel-listan inte var så utförlig jämfört mot de tillkomna krav som vuxit fram på dokumentation sedan GDPR:s införande i maj 2018. När arbetet skulle återupptas 2020 kom pandemin som en försvårande faktor och inventeringsarbetet sköts framåt. Under år 2021 har pandemin fortsatt satt sina spår DSO kontrollerar hur många behandlingar som registrerats

Totalt har 169 behandlingar registrerats i DraftIt varav inga är markerade som inaktiva, det hade betytt att dessa inte längre är aktuella men för att bibehålla spårbarhet finns de kvar i förteckningen. Det finns åtgärder upplagda för delar av de personuppgiftsbehandlingar som behöver kompletteras, kontrolleras eller på annat sätt bearbetas vilket finns dokumenterat i verktygets kommentarsfält. Detta kan bestå i att det saknas information om säkerheten, vem som är ansvarig för personuppgiftsbehandlingen, information till den registrerade, personuppgiftsbiträdesavtal korrekt, tredjelandsöverföringar eller inte osv.

Registerförteckningen är upprättad internt inför GDPR:s införande i maj 2018. Registerförteckningens arbete saknar en skriven rutin hur den ska fungera utan sker idag ad hoc och är beroende av kunskap hos den enskilde anställde.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

Motiveringen till att det anses vara en allvarlig brist är att inga uppdateringar genomförts under år 2021. Det saknas också handlingsplan för 2022 och det saknas intern arbetsgrupp som har i uppdrag att arbeta med frågorna.

3.1.5 DSO ger råd och rekommendationer till PUA

Då det saknas ansvarig person för varje registrering, d.v.s. en anställd som de facto utför dem, behöver en sådan rutin och personer utses och dokumenteras hos Spånga-Tensta stadsdelsförvaltning. Detta för att vid en incident man snabbt ska kunna lokaliseras en kontaktyta som förstår omfattningen och påverkan. Den person som är ansvarig är med fördel en person som arbetar med personuppgiftsbehandlingen i sina ordinarie arbetsuppgifter.

I årsrapporten för 2020 föreslogs att den skulle skapas en intern arbetsgrupp med medlemmar ur förvaltningens olika verksamheter för GDPR-arbete. I årsrapporten för 2020 omnämndes de som GDPR-ambassadörer. Målbilden är att dessa ambassadörer ska utbildas i verktyget DraftIt, då dessa ska kunna uppdatera registerförteckningen vid behov i samarbete med de ansvariga personerna för respektive personuppgiftsbehandling. Det underlättar vid de årliga genomgångarna av personuppgiftsbehandlingarna och det framtida systematiska dataskyddsarbetet.

Det är av största vikt att en intern arbetsgrupp för dessa frågor startas och arbetet med registerförteckningen tas upp igen.

3.2 Styrdokument

3.2.1 Sammanfattning

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

3.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i 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.

3.2.3 Resultat

Spånga-Tensta stadsdelsförvaltning har egen handledning för hur incidenter ska hanteras. I övrigt hänvisar man till de generella dokument som finns framtagna på den gemensamma 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 handledning.

Spånga-Tensta finns representerad i en styrgrupp för de fyra stadsdelarna i Västerort. Där har bland annat ett årshjul antagits som än inte är implementerat i verksamheterna.

En ny informationssäkerhetsriktlinje väntas antas av kommunalfullmäktige 2022. Denna behöver anpassas och implementeras för förvaltningen när detta skett. Exempel på dokument som behöver tas fram lokalt är rutinen för arbete på distans, digitala möten och rutin för arbetet med registerförteckningen.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
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

Bedömningen är baserad på att en uppdaterad informationssäkerhets och IT-riktlinje saknas. Den befintliga i Stockholm stad är från 2014.

3.2.5 DSO ger råd och rekommendationer till PUA

Texten som finns i de stadsgemensamma dokumenten på intranätet kan ibland vara svår att förstå för personalen. En ny informationssäkerhetsriktlinje väntas antas av kommunalfullmäktige 2022. Denna behöver anpassas och implementeras för förvaltningen när detta skett. Exempel på dokument som behöver tas fram lokalt är rutinen för arbete på distans, digitala möten och rutin för arbetet med registerförteckningen.

Det behöver också 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.

Årshjul och övriga dokument som tas fram av en intern arbetsgrupp för GDPR behöver implementeras och kommuniceras i förvaltningen.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	1
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

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

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

3.3.3 Resultat

Det finns en registrerat i 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.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

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

3.3.5 DSO ger råd och rekommendationer till PUA

När personuppgiftsbehandlingarna inventerats och progressen med kontaktpersoner och ansvariga utsetts är nästa naturliga steg att dessa också kan KLASSA:s för de system som är aktuella för detta. DSO:s rekommendation är att detta följs upp taktar med den inventeringsplan som behöver tas fram av den interna GDPR-gruppen när denna tillsats.

I samarbetet för fyrlingen kan ett samarbete ske för att underlätta arbetet med KLASSA då det ser snarlikt ut i informationshanteringen.

3.4 Konsekvensbedömningar

3.4.1 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

3.4.2 Syfte

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

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

3.4.3 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.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

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

3.4.5 DSO ger råd och rekommendationer till PUA

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

3.5 Individens rättigheter

3.5.1 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

3.5.2 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.

3.5.3 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 etc. behöver dokumenteras och kommuniceras.

Informationen till personalen omnämns i eget kapitel se 4 Granskning.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

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

3.5.5 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.

3.6 Personuppgiftsincidenter

3.6.1 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: 2 Individen vid IMY-anmälan: 1
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	2

3.6.2 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.

3.6.3 Resultat

Organisationen är bra på att upptäcka personuppgiftsincidenter och agera när dessa sker. Det visar bland annat förmågan att alltid hålla tidsgränsen på rapporteringen till IMY. Förvaltningen hade en större personuppgiftsincident hösten 2021 som det också rapporterades om i media. Denna var en förlust av personuppgifter till ett större antal registrerade. Efter incidenten skett sammankallades team med nyckelfunktioner såsom ledning och kommunikatör för att skapa strategi framåt hur man skulle agera. Organisationen är bra på att hantera händelser och det märks att den är tränad och kompetent.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

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

3.6.5 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 2022 behöver instruktionen som förklarar hur man agerar vid en personuppgiftsincident kommuniceras igen för att upprätthålla den goda kunskapen.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *”GDPR-Information” till den anställde*

4.2 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.

4.3 Genomförda granskningar och deras resultat

Granskning 1 ”GDPR-Information” till den anställde
När dataskyddsombudet deltagit vid klassningar i verktyget KLASSA under 2021 har detta varit ett område som kommit upp som en varningsflagga. Det har funnits oklarhet om det finns information till den registrerade anställda och vad som meddelas.

HR har dokument anställning som innehåller information som behandlar sekretess och behörighetstilldelning.

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

4.4 DSO ger råd och rekommendationer till PUA

Den nyanställde ska informeras om dataskyddsförordningen (och informationssäkerhet). En utbildning finns framtagen om båda områdena på Utbildningsplattformen och borde vara krav att genomgå innan man tilldelas tjänstekort och behörigheter.

Rekommendationen är att ha en checklista där viktiga punkter såsom att fastställa identitet med id-handling, genomgångna utbildningar i informationssäkerhet och dataskyddsförordningen etc. kan kontrolleras enkelt.

Spånga-Tensta stadsdelsförvaltning behöver ta fram en lokal beskrivning för vad, hur och varför man behandlar personuppgifter om sina anställda. I detta dokument kan man också med fördel teckna ner information om vad man bör tänka på om man som anställd får sekretessmarkering, vad som gäller om sekretess när man slutar mm.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Brist på kunskap om dataskyddsförordningen*
- *Registerförteckningen*

5.2 Syfte

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

5.3 Resultatet av riskkartläggningen

Risk 1 Brist på kunskap om dataskyddsförordningen
En konsekvensbedömning avseende dataskydd enligt artikel 35 i GDPR ska alltid göras om en planerad personuppgiftsbehandling kan medföra en hög risk för de registrerade individerna. Detta förutsätter att det finns en allmän förståelse i organisationen för att dataskyddsansvariga kan behöva bli inblandade i en mängd olika sammanhang i verksamheten när personuppgifter förekommer, och i synnerhet innan personuppgifter börjar behandlas i stor skala eller med hjälp av ny teknik.

Flera medarbetare har goda kunskaper och arbetar med dataskyddsfrågorna men det sker ad hoc och är individberoende. Det är inte ett prioriterat område och risken är att man släpar efter i efterlevnaden av lagstiftningen. Risken är också att brist på förståelse skapar frustration och man ser det som ett hinder och inte en möjlighet att lagstiftningen finns.

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

Risk 2 Registerförteckningen

Registerförteckningen är inte uppdaterad och plan för uppdatering saknas. Detta är problematiskt och diskuteras också i kap. 3.1.

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

5.4 DSO ger råd och rekommendationer till PUA

Spånga-Tensta behöver fått ut GDPR-arbetet i hela organisationen utifrån det systematiska perspektivet. Detta genomsyras i alla granskningsområden där risken blir tydlig och mognadsgraden är låg, d.v.s. det finns inga fasta kommunicerade rutiner men det finns ad hoc lösningar och engagerad personal som kan lösa ut det pga. att de har en grundförståelse. Det kan beskrivas i små kunskapsöar vilket räddar upp situationer.

Den riskreducerande åtgärden är att informera personalen i GDPR och hur efterlevnad ska ske efter att styrdokumenten tagits fram.

Risk 2 Registerförteckningen omhändertas i kap 3.1.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Registerförteckningen*
- *Styrande dokument*

6.2 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.

6.3 Planerade granskningar

Granskning 1 Registerförteckningen

Se vidare kap 3.1 Registerförteckningen

Granskning 2 Styrande dokument

Se vidare kap 3.2.

7 Övrigt att rapportera

7.1 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.

7.2 Övriga observationer

Observation 1 Avsaknad av intern arbetsgrupp för GDPR och informationssäkerhetsfrågor

Spånga-Tensta stadsdelsförvaltning är den enda i fyrlingen som saknar intern arbetsgrupp för dataskydds och informationssäkerhetsfrågor. Detta lyser genom arbetet med klassningar, registerförteckning osv vilket är ryggraden i dataskydds- och informationshanteringsarbetet. Det är viktigt att frågorna prioriteras under år 2022.

Observation 2 Flytt av arkiv

Spånga-Tensta ska byta lokaler och flytta arkivet. Det är med fördel man kan dra synergieffekt av Brommas tidigare flytt och deras olika analyser inom dataskydd och säkerhet.

Observation 2 Sociala media och Schrems II

Under året har flera frågetecken vuxit fram i hela fyrlingen vad gäller sociala media. Rinkeby-Kistas kommunikatörer har drivit denna fråga då man anser att det behövs tydligare gemensam riktlinje för staden. Ett sådant arbete har påbörjats av SLK Kommunikationsavdelning hösten 2021. De tidigare mallar och handledningar som funnits för riskanalys för om ett konto hamnar under artikel 49 har under sommaren dömts ut som att vara icke-acceptabla som underlag.

I och med detta har en stor förvirring uppstått för stadsdelsförvaltningarna om när de kan använda sociala media och hur man ska agera.