Stockholms stad

Bilaga 7

GDPR Årsrapport

2020

Spånga-Tensta stadsdelsnämnd

GDPR årsrapport
April 2021

Dnr: YYYY
Utgivningsdatum: 202X-MM-DD
Kontaktperson: Jessica Hillergård Dataskyddsombud

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse 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”). DSO:n 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 nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

1 Bakgrund ... 3

2 Sammanfattning ... 5

3 Obligatoriska rapporteringsområden ... 6

3.1 Registerförteckning ... 7

3.2 Styrdokument ... 10

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar ... 13

3.4 Konsekvensbedömningar ... 15

3.5 Individens rättigheter ... 17

3.6 Personuppgiftsincidenter ... 19

4 Genomförda granskningar under året ... 22

4.1 Sammanfattning ... 22

4.2 Syfte ... 22

4.3 Genomförda granskningar och deras resultat ... 22

4.4 DSO ger råd och rekommendationer till PUA ... 23

5 Risker inom dataskydd ... 24

5.1 Sammanfattning ... 24

5.2 Syfte ... 24

5.3 Resultatet av riskkartläggningen ... 24

5.4 DSO ger råd och rekommendationer till PUA ... 24

6 Planerade granskningar under det nya verksamhetsåret ... 26

6.1 Sammanfattning ... 26

6.2 Syfte ... 26

6.3 Planerade granskningar ... 26

2 Sammanfattning

I egenskap av ert dataskyddsombud lämnar jag följande årsrapport.
Spånga-Tensta stadsdelsnämnd har ett dataskyddsombud som delas med Rinkeby-Kista, Bromma och Hässelby-Vällingby stadsdelsnämnder. I detta samarbete finns en styrgrupp med representanter från samtliga stadsdelsförvaltningars ledningsgrupper. Inom gruppen sker informationsspridning samt inhämtning av gemensamt uppkomna behov. Genom denna grupp har synergieffekter i det systematiska dataskyddsarbetet snabbt kunnat identifieras. Det är dock viktigt att poängtera att varje enskild stadsdelsförvaltning arbetar självständigt med dataskyddsförordningen inom den egna organisationen.

År 2020 har varit ett utmanande år för hela samhället och har inte lämnat någon opåverkad. På grund av den pågående pandemin fick aktiviteter inom dataskyddsområdet skjutas upp och senareläggas då fokus har varit att upprätthålla de samhällsviktiga funktionerna hos förvaltningen, ibland med hårt ansträngd personalstyrka.

Men, jag som DSO vill lyfta fram några av de viktiga punkter som genomförts trots pandemin. Det har utförts konsekvensbedömningar för Esset och Office365 för förskolan i samarbete med SLK, alla stadsdelsförvaltningar och Utbildningsförvaltningen.

Spånga-Tenstas stadsdelsförvaltnings personal är bra på att identifiera personuppgiftsincidenter. Man är nyfiken och vågar fråga om lösningar och se GDPR som en möjlighet. Nästa steg är att flytta kunskapen från nyckelpersoner till hela organisationen.

Därför är min rekommendation att:

- Uppdatera inventering av registerförteckningen (3 år gammal)
- Utse ägare till de olika personuppgiftsbehandlingarna så att dessa hålls uppdaterade systematiskt.
- Informera, komplettera och implementera styrdokument
- Återuppta arbete med att utbilda och informera
- Införa en intern arbetsgrupp för GDPR

Jessica Hillergård
Dataskyddsombud

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 eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda 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.

Totalt har 169 behandlingar registrerats i DraftIt. 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. Vid den inventering som ska ske 2021 kommer dessa kunskapsluckor att fyllas på enligt plan.

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 individerna.

3.1.4 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

3.1.5 DSO ger råd och rekommendationer till PUA

Då det saknas ansvarig person för varje personuppgiftsbehandling som de facto utför dem, behöver en sådan rutin och personer införas och tillsättas hos Spånga-Tensta stadsdelsförvaltning.

Rådet från DSO betyder att utvalda funktioner inom Spånga-Tensta behöver utbildas i verktyget DraftIt och dessa ska fungera som GDPR-ambassadörer och verka som kontaktpersoner för personuppgiftsbehandlingarna. Det underlättar vid de årliga genomgångarna av personuppgiftsbehandlingarna enligt årshjulet och det systematiska arbetet. GDPR-ambassadörerna ska kunna vid behov lägga till nya personuppgiftsbehandlingar, alternativt kontakta DSO för stöd att lägga in dem.

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?	NEJ
Är dokumenten uppdaterade?	NEJ
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	NEJ

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

Vid dataskyddsförordningen införande så fördes ett centralt GDPR-projekt vid SLK som skulle ta fram gemensamma dokument för hela staden. Spånga-Tensta finns representerad i en styrgrupp för de fyra stadsdelarna i Västerort. Där har bland annat ett årshjul antagits som än inte är kommunicerat.

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

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.

Spånga-Tensta behöver skapa en egen intranätssida med ett lättare språk och kan med fördel utvecklas med länkar till t.ex. en ingående instruktion om personuppgiftsincidenthantering som finns förmedlad av styrgruppen men som ej implementerats. (Se kap personuppgiftsincidenter.) 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 i styrgruppen för GDPR i Västerortssamarbetet behöver antas och implementeras för stadsdelen.

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?	0
Är klassade personuppgiftsbehandlingar aktuella?	N/A

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.

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 inget 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 ”GDPR-ambassadörer” 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 och påbörjas när inventering av personuppgifter är klar.

I samarbetet för fyrlingen kan ett samarbete ske för att underlätta arbetet med KLASSA då det ser snarlikt ut i informationshanteringen. Under 2021 kommer också en ny informationssäkerhetsriktlinje från staden och denna behöver ses över och implementeras.

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?	Kan ej anges
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

Stadsdelsförvaltningen har deltagit vid flera konsekvensbedömningar under året. Bland annat vid införandet av elektroniska körjournaler med hastighetsövervakning, ESSET, O365 i förskolan mm. Esset och O365 har dock inte lett till beslut än hos nämnden då de inte färdigställts och sköts av Utbildningsförvaltningen. Resultatet av konsekvensbedömningen av elektroniska körjournaler har lett till ett förhandssamråd med Integritetsskyddsmyndigheten, IMY. I diskussion med IMY bestämdes att fem pilot-förhandsamråd skulle sändas in där Spånga-Tensta ej ingick.

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

Konsekvensbedömningar är idag beroende av individers kunskap och metoden behöver beskrivas i ett styrdokument. Behov finns också att se över delegationen för vem som får godkänna eller avslå dataskyddsombudets rekommendationer samt godkänna eller avslå de åtgärder som tas fram i konsekvensbedömningen. Idag ska den färdiga konsekvensbedömningen gå till nämnden, vilken är personuppgiftsansvarig, för godkännande/avslag samt ett TJUT vilket är omständligt och inte effektivt. Delegation kan med fördel tas fram och nämnden kan med fördel hållas informerade löpande istället.

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 har tydliga rutiner på intranätet för hur individens rättigheter ska omhändertas för registerutdrag för medborgare. Processen för att få uppgifter rättade, raderade etc. behöver dock dokumenteras och kommuniceras.

Informationen som går ut till de anställda behöver ses över och uppdateras vid anställning och avslutande. Det behöver bli tydligt hur länge uppgifter sparas, vart de lämnas ut, vilka uppgifter som delas med andra osv.

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

Se över texten med instruktionen löpande på intranätet och uppdatera vid behov.

Granska de processer som beskrivs i 3.5.3 och komplettera redan befintlig information i anställningsavtal och sida på intranätet.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom individen/ personalen uppmärksammar dem
Hur många personuppgiftsincidenter har dokumenterats?	12
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	De berörda: 6 Inte de berörda: 6
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten IMY?	4

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

De incidenter med personuppgifter som skett hos Spånga-Tensta stadsdelsförvaltning under 2020 är av olika art. Och är främst av arten att de är information som kommit fel vid utskick eller obehörig åtkomst. Det som sällan anmäls är uppgifter som förstörts eller förkommit.

Staden har också haft en större gemensam incident då det uppstod fel i förskole och fritidshemsplaceringar för förskolan. Plattformen finns hos personuppgiftsbiträdet Utbildningsförvaltningens IKT-enhet. Anmälan i detta fall skedde till Integritetsskyddsmyndigheten. (Nuvarande IMY.)

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 2021 behöver instruktionen som förklarar hur man agerar vid en personuppgiftsincident kommuniceras. Mognadsgraden hos personalen är idag beroende av att nyckelfunktioner finns på plats- Nästa mål är att organisationen blir trygg i agerandet utan nyckelpersonerna och kan utveckla processen.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Registerförteckning*
- *Ledningens kunskap/ engagemang*

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 Registerförteckningen

Se kapitel 3.1

Granskning 2 Ledningens kunskap/ engagemang

Ett bra systematiskt arbete med dataskyddsförordningen börjar med ledningens engagemang. År 2020 var ett år med stora utmaningar och en ny direktör tillsattes. Intervju genomfördes med honom vid årsskiftet och detta var ett givande samtal. Ledningsgruppen har också haft dragning om GDPR. Nämnden har inte utbildats/ informerats av DSO.

	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

När krisen är över med pandemin behöver arbetet återupptas med information till ledningsgruppen och kortare utbildningar löpande under året av DSO.

DSO rekommenderar också att nämnden, som är formellt personuppgiftsansvarig, får utbildning årligen i dataskyddsförordningen och vilka grunderna i denna är.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevant risk inom verksamheten:

- *Brist på kunskap om dataskyddsförordningen*

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

	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

5.4 DSO ger råd och rekommendationer till PUA

Spånga-Tensta behöver fått ut GDPR-arbetet i hela organisationen. Detta genomsyras i alla granskningsområden där risken blir tydlig och mognadsgraden är låg, d.v.s. det finns inga fasta rutiner men det finns ad hoc lösningar och engagerad personal som kan lösa ut det. Den riskreducerande åtgärden är att utbilda personalen i GDPR och hur efterlevnad ska ske. Finns en medvetenhet om vad en

personuppgiftsincident är kommer också sådana att identifieras, förstår man vikten av att göra en konsekvensbedömning och tänka till före blir också detta ett kraftfullt verktyg som sparar tid och pengar.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Personuppgiftsbiträden (2 st.)*
- *Efterlevnad av Schrems II-domen*

6.2 Syfte

Avsikten med att välja ut två områden för granskning är för att kunna planera och avsätta tid för detta under det kommande året. Att granska två personuppgiftsbiträden är också ett av de mål som tagits fram under 2020 då det är både relevant för granskning, möjligt att mäta och en del av dataskyddsombudets arbetsuppgift.

6.3 Planerade granskningar

Granskning 1

Spånga-Tensta har ett flertal personuppgiftsbiträden inom verksamhetens olika områden. För att kontrollera att de uppfyller PUB-avtalen väljs 2 st. ut för att granskas med skriftliga frågor under våren 2021. Dessa kommer sedan att redovisas till personuppgiftsansvarig vid årsrapporten 2021.

Den metod som ska användas är ett skriftligt formulär med frågor till de personuppgiftsbiträden som valts ut. I personuppgiftsbiträdets avtal ska det finnas inskrivet att de ska underkasta sig en sådan granskning. (Vid behov kan även deras lokaler granskas men pga. pågående pandemi begränsas denna granskning under 2021.)

Granskning 2

I juli 2020 föll en dom i EU-domstolen kallad Schrems II som innebär att tredjelandsöverföringar som hänvisar till Privacy Shield inte längre är möjliga att genomföra. Under 2021 ska detta vara ett fokusområde för DSO att granska samt informera PUA:s representanter, ledning och personalen inom Spånga-Tensta.

Granskningen kommer ske genom att:

- Kartlägga leverantörer, tjänster vid personuppgiftsinventering och inhämta PUB-avtal med instruktioner (Inventeringsprojekt)
- Identifiera genom PUB-avtalens instruktioner vilka som har tredjelandsöverföringar till USA/tredjeland (DSO)
- Frågeställningar om oklarheter om överföringar (Informationsägaren)
- Riskvärdering och Analys (DSO och informationsägaren)

När granskningen är genomförd kan beslut slutligen fattas om eventuella mitigerande åtgärder och/ eller om personuppgiftsbehandlingen kan fortgå med en anmälan till IMY.