Stockholms stad

GDPR Årsrapport

2021

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.
Under år 2021 har pandemin fortfarande varit en påverkande faktor för organisationen. Men under hösten lättade trycket och den interna arbetsgruppen för dataskydds- och informationssäkerhetsfrågor startades. Den består nu av nyckelpersoner inom organisationen. En handlingsplan för arbete med registerförteckningen och informationssäkerhet under 2022 har tagits fram.

Organisationen har haft 12 personuppgiftsincidenter under år 2021. Av dessa har 6 st. anmälts till IMY. De anställda är bra på att rapportera avvikelser och agerar direkt med att se vad som kan behöva förbättras.

En brist som framkommit är att ett av de viktigaste styrdokumenten, stadens riktlinje för informations- och IT-säkerhet är från 2014. Den nya är nu ute för beslut av kommunalfullmäktige i januari 2022.

Sociala media har i efterdyningarna av Schrems II domen 2020, blivit problematiskt för stadsdelsförvaltningarna att använda. På grund av tredjelandsöverföringar behövs tydlig motivering och riskanalys tas fram för att dokumentera de val som görs. Önskvärt är att SLK Kommunikation arbetar vidare med denna fråga som de startat hösten 2021 så att stadsdelsförvaltningen kan fortsätta sitt arbete med användande av sociala media.

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 *dokumenteringsskyldighe*t. 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?	287
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
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

Under hösten 2021 har Informations och GDPR-arbetsgruppen tagit fram en utförandeplan för kvarstående inventeringsaktiviteter för att uppdatera den befintliga registerförteckningen men också ur ett informationssäkerhetsperspektiv.

Totalt har 287 behandlingar registrerats i DraftIt varav 114 st. är markerade som inaktiva, det betyder 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. Vid den inventering som ska ske 2022 kommer dessa kunskapsluckor att fyllas på enligt plan.

Ruin för arbete med registerförteckningen saknas.

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
	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

Bedömningen motiveras utifrån att handlingsplan finns framtagen.

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 Hägersten-Älvsjö stadsdelsförvaltning. Detta för att vid en incident 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.

Den interna arbetsgruppens medlemmar för GDPR, behövs 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 enligt årshjulet och det systematiska arbetet.

Den handlingsplan som initierats av informationssäkerhets- och GDPR- arbetsgruppen för inventering och uppdaterings av registerförteckningen är en bra väg framåt. För att lyckas genomföra detta behöver tid och resurs avsättas och frågan prioriteras.

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?	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

Ett av de dokument som är viktigast för dataskyddsarbetet är att det finns en implementerad och aktuell informationssäkerhets- och IT-riktlinje. Den som anges vara antagen för Stockholm stad är från 2014.

Lokala rutiner finns för dataskydd och GDPR, personuppgiftsincidenter, arkiv och gallring och personuppgiftsbiträdesavtal.

Det saknas styrdokument för arbete på distans, lokala rutiner för konsekvensbedömningar etc. Där hänvisas istället till den centrala gemensamma intranätssidan för Stockholm stad.

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. Det har stadsdelsförvaltningen löst bland annat med en egen intranätssida med ett lättare språk och kan med fördel utvecklas ännu mer. Det saknas en ansvarig/ utpekad person med ansvar för sidan. Idag står en funktionsbrevlåda som kontakt.

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 arbetsgruppen för GDPR behöver antas och implementeras för stadsdelen. En rutin och plan för hur kommunikationen till samtlig personal i frågan behöver tas fram.

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?	I Klassa: 4
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

Informationsklassning sker efter protokoll framtaget av SLK. Denna har börjat användas under hösten 2021. Dokumentet ger en första bedömning och stöd innan den större aktiviteten med verktyget KLASSA.

Det finns 4 stycken *system* registrerade 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.

En handlingsplan finns framtagen för organisationens arbete med både informationssäkerhet och dataskydd samt en inventeringsplan. Detta gör att bristen anses vara mindre allvarlig då det pågår ett arbete med frågorna.

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
	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

3.3.5 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 presenterats av den interna informationssäkerhets- och GDPR-gruppen.

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. Då registerförteckningen inte uppdaterad, kan det inte heller anges om alla personuppgiftsbehandlingar som behöver konsekvensbedömmas har identifierats. Dock har det vid behov som framkommit skett konsekvensbedömningar.

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 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.

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 dock dokumenteras och kommuniceras. Dock sker inga avvikelser då personalen är engagerad och löser ut frågor som uppstår. Flera begäran från individer sker i stadsdelsförvaltningen årligen.

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.

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?	12
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Rapport IMY: 6 Individen vid IMY-anmälan: 3
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	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

Hägersten-Älvsjö har en relativt god uppmärksamhet på att upptäcka personuppgiftsincidenter. När en sådan skett vill personalen också åtgärda eventuella brister och ser över rutiner omedelbart. Det har också kompletterats med utbildningar under året efter att det skett avvikelser.

I de fall incidenterna anmälts för sent beror på att fokus lagts på utrednings- och åtgärdsarbete och andra anmälningar likt Lex Sarah.

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.

Det saknas krav på genomgången utbildning innan tjänstekort och behörigheter tilldelas samt ID-kontroll. Det finns ingen egen beskrivning av hur personuppgifter behandlas i stadsdelen. Idag hänvisas personalen till den gemensamma intranätssidan för staden.

På intranätet finns stöd i arbetet med när en person avslutar sin anställning i organisationen. Dock saknas att man påminner om sekretessen även efter avslutad tjänst.

Det finns ingen egen beskrivning av hur personuppgifter behandlas i stadsdelen. Idag hänvisas personalen till den gemensamma intranätssidan för staden.

Det finns ett krav att personalen årligen ska genomgå de digitala utbildningar som finns på utbildningsplattformen.

	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

Informationen till personalen i organisationen finns delvis nedtecknad i dokumentationen och behöver kompletteras med de brister som identifierats i kap 4.3.

Det är bra att det finns krav att personalen ska genomgå utbildningarna på utbildningsplattformen. Det behöver nu tas fram en rutin och kontroll så att dessa genomförs.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Brist på kunskap om dataskyddsförordningen*
- *Inbyggt dataskydd och dataskydd som standard*
- *Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor.*

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.

I dagsläget har flera medarbetare goda kunskaper och arbetar systematiskt med dataskyddsfrågorna. Dock sker det inte i hela organisationen. 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 Inbyggt dataskydd och dataskydd som standard

Tanken är att inbyggt dataskydd och dataskydd som standard enligt artikel 25 i GDPR ska genomsyra hela utvecklingsprocessen och varje IT-systems hela livscykel, överallt där personuppgifter förekommer. Hur pass komplext arbetet i praktiken blir med att implementera detta beror helt på sammanhanget och behandlingarna. Det finns alltså ingen universallösning, utan inbyggt dataskydd och dataskydd som standard är något som varje organisation måste förhålla sig till på en principiell, strategisk nivå och sedan arbeta med utifrån de egna förutsättningarna.

	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 3 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. 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 finns.

	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

5.4 DSO ger råd och rekommendationer till PUA

Hägersten-Älvsjö behöver fått ut GDPR-arbetet i hela organisationen utifrån det systematiska perspektivet. Det kravet på att det är obligatoriskt att genomgå utbildningarna på utbildningsplattformen är bra och behöver följas upp att det genomförs. Förutsättningen att alla går utbildningen är att ledningen och nämnden också har förståelse för vad riskerna är och betyder för organisationen. Därför rekommenderas ledningsgruppen att genomgå den specifika digitala utbildning för chefer som finns framtagna inom området och som är publicerat på Stockholm stads utbildningsplattform samt att nämnden har utbildningen även den årligen.

Under arbetet med registerförteckningen kan man med fördel se över om det finns system att bygga in mer dataskydd som standard. Ett exempel kan vara automatisk gallring av papperskorgen efter ex en månad osv.

Formatmallar för dokumentation behöver tas fram gemensamt i staden. Rutiner och handledningar behöver skapas centralt och även en implementations och kommunikationsplan. Skapas bara klassningar utan uppföljande dokumentation är det bara pappersprodukter och inte riskminimerande dokument som omhändertar problem.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

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

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

6.3.1 Granskning 1 Granska 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

6.3.2 Granskning 2 Fungerar processerna för att hantera de registrerades rättigheter?

Ett av huvudsyftena med dataskyddsförordningen är att värna om enskilda individers rättigheter i sammanhang där deras personuppgifter behandlas och registreras. Därför måste alla organisationer vara medvetna om att man endast kan behandla personuppgifter om man respekterar individens fri- och rättigheter, och har rutiner för att bemöta och uppfylla dessa rättigheter när det blir aktuellt. Bestämmelserna om rättigheterna finns i artiklarna 12-21 i GDPR. Det handlar bland annat, men inte enbart, om rätten till registerutdrag och rätten till radering. Under 2022 kommer följande att granskas:

- Granska om organisationen har klart för sig när de olika rättigheterna gäller
- Granska organisationens rutiner för att hantera förfrågningar från de registrerade om att utöva sina rättigheter enligt artiklarna 12-21 i GDPR
- Granska hur organisationen i praktiken hanterat begäran om registerutdrag.
- Granska hur organisationen i praktiken hanterat begäran om radering.
- Granska om organisationen svarar i tid på förfrågningar från de registrerade

Granska hur organisationen dokumenterar (och gallrar) i samband med hantering av förfrågningar från registrerade

6.3.3 Inhämtande av information från den registrerade vid ersättningsbedömning

År 2021 kontaktades dataskyddsombudet med en frågeställning om kravet på detaljerna i informationen som behövs vid bedömningen om bidrag. Denna fråga har lyfts till berörd enhet men frågan visar sig vara inte helt okomplicerad. En granskning kommer därför genomföras under 2022 för att fastställa om rutiner och uppgiftsminimeringskravet efterföljs i de delar av stadsdelsförvaltningen som inhämtar denna typ av information.

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.

Under 2021 har en intern arbetsgrupp införts för dataskyddsarbetet och är i uppstartsutförande. Där ingår flera nyckelroller såsom informationshantering, IT- och informationssäkerhetssamordnare osv.

7.2 Övriga observationer

Observation 1 Sociala media och Schrems II

Under året har flera frågetecken vuxit fram bland kommunikatörerna i stadsdelsförvaltningen. Behovet av att använda sociala media är stort. Och man 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.