Stockholms stad

GDPR Årsrapport

2021

Skarpnäcks stadsdelsnämnd

GDPR årsrapport
Januari 2022

Dnr: SKA 2021/405
Utgivningsdatum: 2022-01-07
Kontaktperson: Fabian Lind

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

2 Sammanfattning

I egenskap av ert dataskyddsombud lämnar jag följande årsrapport.

Skarpnäcks stadsdelsnämnd har under 2021 tagit flera steg framåt i GDPR-arbetet, men det finns fortfarande en del utvecklingsområden. De obligatoriska rapporteringsområden som behandlas i denna rapport samt status för dessa är:

Registerförteckning – Arbetet med att stärka kunskapen om registerförteckningen samt att föra över denna i verktyget DraftIt pågår.
Styrdokument – Rekommendation att ta fram egna pedagogiska styrdokument som når ut till de anställda, gärna på en egen sida på intranätet för GDPR.
Tekniska och organisatoriska åtgärder för personuppgifts-behandlingar – Klassning av personuppgiftsbehandlingar inledd, organisatoriskt rekommenderas att säkerställa att alla anställda går relevanta utbildningar.
Konsekvensbedömningar – Rekommendation att göra konsekvensbedömning till en naturlig del av de processer där det är relevant.
Individens rättigheter – Rekommendation att sprida information till de anställda om de skyldigheter som finns gentemot individer vars personuppgifter de behandlar.
Personuppgiftsincidenter – Hög kunskap, rekommenderas att informera kontinuerligt om vad de är samt hur de hanteras för att behålla denna.

Chefer har under året utsett s.k. personuppgiftsredogörare, eller GDPR-ambassadörer på sina respektive enheter som har fått utbildning i GDPR och verktyget för registerförteckning, DraftIt. Detta har bidragit till att stärka kunskapen om GDPR i verksamheterna, även om flera insatser för detta kommer att krävas kontinuerligt. Att kunskap om registerförteckningen sprids i verksamheterna är också mycket positivt, eftersom det är en av grunderna för ett framgångsrikt GDPR-arbete men också för arbetet med informationssäkerhet.

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 och personuppgiftsincidenter.

Nedan redogörs för nämndens 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?	88
Har nödvändiga uppdateringar gjorts?	JA
Bedöms registerförteckningen vara fullständig?	NEJ
Har verksamheten lämpliga rutiner för registerföring?	JA

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).

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 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 verksamheten 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

Registerförteckning sker i verktyget DraftIt sedan 2019 då det ersatte de tidigare Excelfilerna från 2018.

PUA har genomfört en utbildning i DraftIt i förvaltningen under året för utvalda medarbetare på olika enheterna, för att de ska få kunskaper att kunna hantera registerförteckningen för sin verksamhet. Det är ett sätt att föra arbetet med registerförteckning närmare verksamheterna som behandlar personuppgifter, öka deras kunskap, samt att göra det till en naturlig del av arbetet i dessa verksamheter.

En del personuppgiftsbehandlingar är dock ännu inte införda i DraftIt utan endast noterade i tidigare Excelfiler. Totalt finns 88 personuppgiftsbehandlingar inlagda i DraftIt, och arbetet med att föra över uppgifter och komplettera fortsätter.

Registerförteckningen är ursprungligen upprättad internt inför GDPR:s införande i maj 2018. En registerförteckning uppdateras ständigt allt eftersom verksamheternas personuppgiftbehandlingar förändras. Tillsammans med tidigare Excelfiler kan registerförteckningen i DraftIt anses ge en god bild av PUA:s personuppgiftsbehandlingar. Att risken betecknas som orange nedan beror på registerförteckningens viktiga roll i GDPR-arbetet samt att överföringen till DraftIt, det verktyg där registerförteckningen ska finnas, inte är klar.

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

PUA har i början av året lyft frågan om att stärka personskyddsarbetet i förvaltningen genom en tydligare organisation. Förvaltningsledningen beslutade då att varje verksamhet skulle utse en personuppgiftsredogörare/GDPR-ambassadör. PUA har därefter genomfört en utbildning i DraftIt för dem. DSO råder PUA att fortsätta med arbetet att stärka dessa rollers kapacitet och kunskap och se till att kunskapen om GDPR och rutinerna för registerförteckning säkerställs inom verksamheterna.

PUA uppmanas också att under kommande år ytterligare förankra kunskap om GDPR och registerförteckning även på ledningsnivå. De personuppgiftredogörare/GDPR-ambassadörer som utsetts på varje enhet får utbildning i DraftIt och kan dessutom användas som ett stöd i enhetens arbete med att följa GDPR i allmänhet.

Antal registrerade behandlingar ovan avser de som är införda i DraftIt. Registerförteckningen kompletteras fortfarande av de tidigare Excellistorna. PUA råds att verka för att hela registerförteckningen ska finnas i DraftIt, vilket kan uppnås genom fortsatt utbildning av och stöd till verksamheterna. Det är också viktigt att fånga in de personuppgiftsbehandlingar som är kopplade till processer som involverar flera enheter. Bedömningen är också att arbetet skulle underlättas av att en stödjande funktion inrättades för verksamheterna i deras arbete med en uppdaterad registerförteckning.

Risken bedöms som orange, mycket på grund av hur grundläggande en bra registerförteckning är för PUA:s övriga arbete med personuppgifter. Det bör dock betonas att PUA kommit en bra bit på väg även om arbete återstår.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	JA
Håller innehållet i de existerande dokumenten lämplig kvalitet?	JA
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	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 medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i verksamheterna 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 styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, till exempel att dokumentationen är uppdaterad och aktuell.

En brist inom området bör ses som en brist i förhållande till lagkrav, men det finns fler nyanser 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 ineffektivitet 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 kunskap. Det drabbar verksamheter på flera sätt och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut.

3.2.3 Resultat

På stadens intranätssida ”Dataskyddsförordningen (GDPR) och personuppgiftsbehandling” rekommenderas att alla verksamheter ska ta fram förvaltningsspecifik styrande dokumentation. PUA har tagit fram styrande dokumentation som finns på en sida för arkiv, dokumenthantering och offentlighet på intranätet.

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
	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

3.2.5 DSO ger råd och rekommendationer till PUA

Flera av stadens texter som finns på intranätet kopplade till arbetet med GDPR kan vara skrivna på ett avancerat språk som kan vara svårt att förstå. DSO råder PUA att skapa en egen sida om GDPR för Skarpnäcks stadsdelsförvaltning på intranätet. Det finns bra information om personuppgiftshantering under en intranätssida om arkiv, dokumenthantering och offentlighet. Det är dock oklart hur känd denna sida är bland medarbetarna, varför en utökad sida för GDPR-arbetet kan behövas. Dokument och instruktioner bör också vara tydligt skrivna och på ett enkelt språk så att alla medarbetare kan ta del av dem. Det är även bra att utse en ansvarig för sidan för att säkerställa att informationen där samt dokumenten uppdateras kontinuerligt.
Det behöver också tas höjd för att alla inte har åtkomst till datorer och intranät dagligen och att information inte når fram till all personal. Förvaltningen kan se över behov av information och dialog på arbetsplatsträffar eller genom anslag om till exempel vad

en personuppgiftsincident är och vad man gör vid en sådan händelse.

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 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 faktiskt 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

PUA har under året genomfört klassning av systemet ParaInn inom ramen för stadens arbete med att följa NIS-direktivet.[1] Övriga stadsdelar klassar andra system. Det rör sig om s.k. normerande klassningar vilket innebär att stadsdelsförvaltningarna delar sina klassningar av olika system med varandra, eftersom stadsdelarna använder samma stadsövergripande system.

Resultatet av klassningen är svårt att se just nu, då vi inväntar den klassning som också görs centralt av stadsledningskontoret och TietoEvry gällande alla system.

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

Flera klassningar av PUA:s system kommer att initieras under 2022, där behöver rätt prioritering göras av vilken ordning systemen bör klassas i. Klassningar bör också i fortsättningen göras om varje år.

Vad gäller organisatoriska skyddsåtgärder, så rekommenderas verksamheterna att säkerställa att personalen känner till råd och riktlinjer för hantering av personuppgifter, då många system hanterar känsliga personuppgifter. Rutiner kring behörigheter ska

1 NIS-direktivet syftar till att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU. Det europeiska NIS-direktivet är svensk lag. Källa: SKR https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/informationssakerhet/nisdirektivet.19091.html

finnas nedskrivna och rekommenderas att ingå i introduktion av ny personal.

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?	NEJ
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

PUA har under året genomfört en konsekvensbedömning av hantering av personuppgifter i samband med att projekt Smarta lås började implementeras i hemtjänsten. Då PUA var den första stadsdelen att införa Smarta lås var man också först med att göra en konsekvensbedömning av personuppgiftsbehandlingar inom ramen för projektet. Konsekvensbedömningen som gjordes har delats med andra förvaltningar inför deras respektive införande av Smarta lås. PUA har genomfört konsekvensbedömningen med stöd av stadens mall och i nära samarbete med de ansvariga för projektet.

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

Konsekvensbedömning behöver beskrivas i ett styrdokument och dess betydelse kommuniceras. Det är viktigt att dess genomförande inte blir helt beroende av enskilda medarbetares detaljkunskaper. Konsekvensbedömningar behöver också bli en naturlig del av verksamhetens processer där det är relevant, ett exempel på detta är vid upphandlingar. PUA gör dock få egna upphandlingar utan deltar ofta i stadsövergripande sådana, och detta gör att denna fråga behöver lyftas på stadsövergripande nivå. DSO ska alltid involveras i, men inte själv genomföra, konsekvensbedömningar.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	2
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	2

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 dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Integritetsskyddsmyndighetens (”IMY”) 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

Rutin för tillgodoseende av individens rättigheter finns på intranätet, på sidan för arkiv, dokumenthantering och offentlighet. Det är dock oklart hur känd den är i verksamheterna.

Det är oklart vilken information som går ut till anställda om hur länge deras uppgifter sparas efter att anställning avslutas t.ex.

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

Det finns en bra rutin för detta på intranätet. DSO rekommenderar dock att denna sprids och blir mer känd i verksamheterna, gärna på en egen sida för GDPR som beskrivs i det föregående. DSO rekommenderar att det säkerställs att rutinens påbud om att enheter och verksamheter utser en kontaktperson som handlägger dessa förfrågningar följs, då detta kommer underlätta för verksamheten att möta de förfrågningar som kommer.

PUA rekommenderas också att säkerställa att information går ut till de anställda om hur deras personuppgifter behandlas och hur länge de sparas etc.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Förvaltningens personal uppmärksammar dem
Hur många personuppgiftsincidenter har dokumenterats?	15
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	till IMY: 6 rapporterats, 9 inte till berörda: 5 rapporterats, 10 inte
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.”

I en verksamhet kan förekomma många andra typer av incidenter, som inte involverar personuppgifter. Det är viktigt att hålla den saken i åtanke, så att årsrapporteringen inte omfattar annat än just personuppgiftsincidenter. Vidare är det en grundförutsättning för hanteringen av personuppgifter att incidenter över huvud taget upptäcks, samt att verksamheten förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som dataskyddsförordningen kräver.

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. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.
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 och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. 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:s sida. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

3.6.3 Resultat

Samtliga personuppgiftsincidenter som kommit till DSO:s kännedom inom 72-timmarfristen och där rapportering till IMY förordats har rapporterats i tid. De gånger det inte gjorts är det för att verksamheterna uppmärksammat eller märkt incidenterna mer än 72 timmar efter att de skett.

De flesta incidenter som sker är av karaktären handlingar eller mail med personuppgifter når fel mottagare av misstag. En av incidenterna rör Skolplattformen och påverkade flera verksamheter i staden.

Kunskapen om vad personuppgiftsincidenter är och hur de hanteras bedöms som relativt hög inom verksamheterna. Information om hur en incident ska hanteras ingick i den DraftIt- och GDPR-utbildning som gavs till utsedda personer under våren. Sådan kunskap kan dock vara en färskvara och det är nödvändigt med kontinuerlig information och utbildning för att den ska upprätthållas.

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

PUA rekommenderas att fortsätta utbilda och informera kring personuppgiftsincidenter i verksamheterna för att förebygga att incidenter sker. Personuppgiftsincidenter är tyvärr något som alltid kommer att inträffa i någon utsträckning, men information om vad en personuppgiftsincident är och hur de ska hanteras kan hjälpa till att minska antalet. Det finns tydliga korrelationer mellan att personal haft utbildning i GDPR och antalet personuppgifter som anmäls. Utbildning kan exempelvis ges i samband med arbetsplatsträffar. Utsedda personuppgiftsredogörare/GDPR-ambassadörer kan också bli lokala experter inom området och ett stöd för sina kollegor i arbetet med att förebygga personuppgiftsincidenter. Det är också viktigt att säkerställa att information om hantering av personuppgiftsincidenter når alla nyanställda.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Registerförteckning*
- *Kunskap om GDPR i verksamheterna – deltagande i obligatorisk utbildning i dataskydd och informationssäkerhet*
- *Dataskyddsombudets roll*

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 – Kunskap om GDPR i verksamheterna - Deltagande i obligatorisk utbildning i dataskydd och informationssäkerhet

Det har tagits fram obligatoriska utbildningar i dataskydd och informationssäkerhet som är gemensamma för alla Stockholms stads verksamheter. Statistiken visar att ca 70 % av alla PUA:s anställda med egen dator har genomgått utbildningarna. Vilka som ännu inte har genomgått utbildningarna har kommunicerats till respektive chef för att detta ska kunna åtgärdas i närtid. Många av PUA:s anställda har inte tillgång till egen dator i sitt arbete. Dessa har ofta genomgått utbildningarna i samband med APT och liknande. Det går inte att ta fram statistik för grupper som deltagit i utbildningen, så några siffror för dessa anställda går inte att få.

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

Granskning 3 – Dataskyddsombudets roll

DSO är i dagsläget även arkivhandläggare och nämndsekreterare. En av grunderna i DSO:s roll är att vara oberoende gentemot verksamheten som den granskar. Detta är svårt att uppnå med en delad roll, vilket kan vara värt att uppmärksamma för PUA.

	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

Gällande registerförteckning, se 3.1.

Gällande kunskap om GDPR i verksamheterna och deltagande i de obligatoriska utbildningarna är det viktigt att ta i akt personalomsättningen, och säkerställa att nyanställda går utbildningen under sin första tid som anställd. Information om utbildningen finns med i material som alla nyanställda får, men det är viktigt att cheferna säkerställer att den nyanställda faktiskt går utbildningen under de första veckorna.

DSO har idag en roll som inte är helt frikopplad från verksamheten. PUA råds att se över DSO:s roll så att den kan bli den fullt oberoende granskande funktion som det är tänkt.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Bristande kunskap om GDPR i verksamheterna*

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

	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

PUA råds att i alla lägen arbeta för att säkerställa personalens och ledningens kunskaper om frågor relaterade till GDPR. Ett av medlen för detta är de obligatoriska utbildningar som tagits fram centralt. Se 4.3 för fler detaljer.

Större informationsinsatser om GDPR i alla verksamheter har inte genomförts under de senaste åren. Det är bra att utbildning genomförts under året men det kan vara läge att genomföra större insatser igen med tanke på personalomsättningen. Ett bra sätt är exempelvis att besöka verksamheters APT och ge information med möjlighet att ställa frågor.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Registerförteckning*
- *Informationsklassning*

6.2 Syfte

Som nämnts ovan 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

Granskningen av PUA:s registerförteckning kommer att fortsätta under kommande år.

Granskning 2

Planerade klassningar av system under kommande år kommer att utgöra en grund för granskning av hur verksamheterna arbetar i dessa system. Det kommer att klargöras huruvida rätt rutiner finns för hur verksamheterna hanterar personuppgifter i systemen.

7 Övrigt att rapportera

7.1 Sammanfattning

Ett stort projekt PUA varit inblandat i under året är införandet av elektroniska körjournaler. Införandet har blivit försenat på grund av tredjelandsöverföring av personuppgifter.

7.2 Syfte

I juli 2020 föll en dom i EU-domstolen , Schrems II, som innebär att tredjelandsöverföringar som hänvisar till Privacy Shield inte längre är möjliga att genomföra.

7.3 Övriga observationer

Observation 1

Införandet av elektroniska körjournaler i PUA:s verksamhet har blivit försenat på grund av en identifierad tredjelandsöverföring.