Stockholms stad

Dataskyddsombudets årsrapport

2020

Socialförvaltningen

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.

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 och obligatoriska rapporteringsområden

I egenskap av ert Dataskyddsombud, fortsättningsvis kallad DSO, lämnas följande årsrapport. Rapporten överlämnas i samarbete med informationssäkerhetssamordnaren.

Under året har en inventering kring tredjelandsöverföring skett för att kartlägga vilka överföringar av personuppgifter som sker, i vilka fall det tecknats personuppgiftsbiträdesavtal, i fortsättningen hänvisat till som pub-avtal, och där avsaknad av pub-avtal behöver åtgärdas. Inventeringen har skett inom hela Stockholms stad till följd av Schrems II[1] fallet i EU domstolen i somras.

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig, i fortsättningen kallad 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 och informationssäkerhetssamordnarens slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter genomförd uppföljning och granskning.

[1] Den 16 juli 2020 meddelade EU-domstolen Schrems II-domen med betydande konsekvenser för användningen av amerikanska molntjänster. Kunder till amerikanska molntjänstleverantörer måste nu själva verifiera dataskyddslagarna i mottagarlandet, dokumentera sin riskbedömning och kommunicera med sina kunder.

3 Registerförteckning

3.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	281 registreringar
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Nej.
Har verksamheten lämpliga rutiner för registerföring?	Delvis.

3.2 Syfte

Det följer i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas, i fortsättningen kallat personuppgiftsbehandlingar, i verksamheten och dokumentera dem i en så kallad registerförteckning. Förvaltningens registerförteckning återfinns i verktyget Draftit Privacy records.

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgiftsbehandlingar finns och hur de hanteras. Registerförteckningen säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

3.3 Resultat

Det finns idag 281 personuppgiftsbehandlingar registrerade i verktyget Draftit Privacy records, 6 av dem är riskregistreringar.

DSO ser det som positivt att flertalet personuppgiftsbehandlingar är registrerade, att flera på förvaltningen börjat använda verktyget Draftit Privacy records och att det idag finns en kunskap inom förvaltningen att nya personuppgiftsbehandlingar ska införas i registerförteckningen. DSO bedömer dock att registerförteckningen inte är fullständigt. Samtliga behandlingar som är registrerade behöver ses över, dels för att se till att de är fullständigt i fyllda med korrekt och efterfrågad information men också för att avgöra om de

är korrekt registrerade som personuppgiftsbehandlingar i enlighet med GDPR och Dataskyddslagstiftning. Kunskap om vad en personuppgiftsbehandling är har ökat sedan de första registringarna genomfördes och det är därför som vissa registrerats men kan tas bort eftersom de i regel inte räknas som en personuppgiftsbehandling.

Registerförteckningen behöver även ses över för att lättare identifiera eventuella personuppgiftsbehandlingar som innebär en större risk för den enskilde, dessa kommer att kallas för riskbehandlingar. Här behöver man dels uppmärksamma registreringen av nya personuppgiftsbehandlingar men också gå igenom de som redan finns men inte har någon risk angiven. Vidare ska dessa vid behov kompletteras med aktuella risk- och konsekvensbedömningar[2] samt pub-avtal.

Förvaltningen har tagit fram ett dokument som fastställer roller och ansvarsfördelning avseende dataskyddsarbetet. En av rollerna är Dataskyddssamordnarna och de har behörighet till Draftit Privacy records. De har som uppgift att kontinuerligt se över och uppdatera befintliga, lägga till nya eller radera inaktuella personuppgiftsbehandlingar.

Verktyget Draftit Privacy records erbjuder vägledning för användarna i systemet både kring hur systemet är uppbyggt och fungerar men också juridisk vägledning utifrån GDPR. Behörigheter till verktyget Draftit Privacy records uppdateras kontinuerligt av DSO och begränsar användarnas tillgång till uppgifter utöver deras egen enhet.

3.3.1 DSO bedömning och rekommendationer

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

[2] Syftet med en konsekvensbedömning är att förebygga risker. Målet är att skydda människors fri- och rättigheter och minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk. Se punkt 2.4.

DSO bedömer att förvaltningen har en bra grundstruktur avseende registerförteckningen. De brister som idag finns i förvaltningens registerförteckning behöver dock åtgärdas. Bedömningen utgår från att registerförteckningen idag inte är fullständigt och att felaktiga registreringar finns inlagda, alltså personuppgiftsbehandlingar som inte anses vara en personuppgiftsbehandling i enlighet med GDPR och dataskyddslagstiftning.

Vid införandet av GDPR i maj 2018 genomfördes en stor inventering på förvaltningen för att identifiera eventuella personuppgiftsbehandlingar och riskbehandlingar. En uppföljning behövs för att säkerställa att arbetet fortlöper i verksamheterna. I nuläget har flera enheter registrerat behandlingar som saknar ett tydligt angivet syfte/ändamål med personuppgiftsbehandlingen och där det inte finns en uttömmande beskrivning.

SLK har i samarbete med Draftit Privacy records utformat mallar som vägledning i registrering av personuppgiftsbehandlingar. Dessa mallar är anpassade utifrån den verksamhet som bedrivs inom Stockholm stad. Samtliga dataskyddssamordnare har fått behörighet till mallen och kan registrera inom den. I registerförteckningen behöver det anges vem som är ansvarig för respektive behandling i förteckningen och likaså kopplas på eventuella riskbedömningar och pub-avtal, detta är också något som bör ses över och förbättras.

Med hänsyn till den verksamhet som bedrivs av förvaltningen inom till exempelvis socialtjänst och den mängd känsliga personuppgifter som hanteras gör DSO också bedömningen att antalet angivna riskbehandlingar är lågt.

4 Styrdokument

4.1 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?	Uppdateringar har skett under 2020, ännu inte utrett vad det lett till. Vägledning har utformats ytterligare.
Är dokumenten uppdaterade?	Delvis.
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja.

4.2 Syfte

Området syftar till att PUA bedriver ett systematiskt dataskyddsarbete och 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.

4.3 Resultat

På förvaltningens intranät finns en egen flik för dataskyddsfrågor dit alla medarbetare har åtkomst. På fliken finns till exempel vägledande dokument inom incidentrapportering, mallar för upprättande av pub-avtal med vägledning och instruktion, information och blanketter för samtycke, samt blanketter för risk och konsekvensbedömning. På fliken finns även generell information om dataskyddslagstiftning, kontaktuppgifter till dataskyddsombud, information om hur dataskyddsorganisationen är uppbyggd och hur ansvarsfördelningen ser ut samt vilka roller som finns. På fliken hänvisas även till en webbutbildning inom dataskydd och informationssäkerhet, som varje medarbetare uppmanas att genomföra. Dataskyddsombudet uppdaterar blanketter

och information löpande och följer rekommendationer från exempelvis tillsynsmyndighet.

Det finns idag en utarbetad rutin för inkomna registerförfrågningar.[3] Begäran om registerutdrag inkommer till Dataskyddsombud och skickas sedan vidare till Paraplysamordnare och systemansvarig för slagning i diarium och paraply. Rutin beskriver hur förfrågan ska spridas i organisationen för att få en begränsad spridning av personuppgifter utifrån de områden individen önskar.

Blanketter för incidentrapportering är uppdaterade utifrån den anmälan som görs till Integritetskyddsmyndigheten, i fortsättningen kallad IMY. Detta för att fånga relevant information och minska på komplettering av uppgifter mellan DSO och den som upprättar en incidentanmälan. Det finns även beslutat i rollbeskrivningen att DSO ansvarar för att diarieföra incidentanmälan samt skicka in de anmälningar som ska till Integrationsskyddsmyndigheten.

4.3.1 DSO bedömning och rekommendationer

	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

Brister som uppmärksammats handlar framförallt om att tydliggöra information inom förvaltningen och påminna för medarbetare i det dagliga arbetet. Blanketter och rutiner finns på plats men kunskapen om ansvarsfördelningen och fördelning av arbetsuppgifter inom olika dataskyddsfrågor, såsom registerförteckning och incidenthantering, saknas helt eller delvis. Utbildning är ett bra sätt att uppmärksamma medarbetare om hur en incident kan identifieras och hur man bedömer dess art och allvar. I och med att det idag finns en tidsfrist för att anmäla allvarliga personuppgiftsincidenter till Integritetsskyddsmyndigheten bör kunskap om vilka incidenter

[3] Dataskyddsförordningen (The General Data Protection Regulation) är till för att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Se avsnitt 2.5.

som ska anmälas eller ej samt hur samråd med dataskyddsombud kan se ut, ökas.

5 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	24
Är klassade personuppgiftsbehandlingar aktuella?	Ja

5.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. 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.

5.3 Resultat

Förvaltningens lokala verksamhetssystem har till viss del registrerats i Draftit Privacy record. Under året har dessa informationsklassats i KLASSA och har därmed aktuella klassningsprotokoll. Informationsklassningar har genomförts för 24 verksamhetssystem av 24 totalt registrerade i Draftit Privacy Records. Förvaltningen har tagit fram en plan för att systematiskt genomföra informationsklassningar löpande avseende de lokala verksamhetssystemen för att säkerställa aktuella klassningar.

5.3.1 Informationssäkerhetssamordnarens bedömning och rekommendationer

	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

Registreringarna i Draftit Privacy Records av personuppgiftsbehandlingar (exklusive verksamhetssystem) saknar till viss del ställningstagande gällande exempelvis säkerhetsfrågor. Eftersom förvaltningen hanterar känslig information är ett rimligt antagande att det finns behov av att komplettera informationen i Draftit Privacy Record med detta samt informationssäkerhetsklassa personuppgiftsbehandlingarna.

DSO tillsammans med informationssäkerhetssamordnare rekommenderar att alla chefer bör uppdras att säkerställa kompletta registreringar av sin verksamhets personuppgiftsbehandlingar. Det medför ett tydliggörande kring vad som behöver åtgärdas, som till exempel utse ansvarig för informationen i syfte att identifiera behov av och säkerställa genomförande av informationsklassning och denna sedan hålls uppdaterad.

DSO tillsammans med informationssäkerhetssamordnare rekommenderas stödja verksamheterna med workshops i kompetenshöjande syfte. Informationssäkerhetsklassningar genomförs enligt stadens riktlinje för informationssäkerhet i verktyget KLASSA. Informationssäkerhetssamordnare har utsett klassningsledare som tillsammans med ansvariga för personuppgiftsbehandlingen genomför klassningen.

6 Konsekvensbedömningar

6.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Delvis.
Är de genomförda bedömningarna aktuella?	Ja.

6.2 Syfte

Syftet med risk- och konsekvensbedömningen är att förebygga risker innan de uppkommer, ta fram rutiner och åtgärder för att hantera eventuella risker och kunna visa att vi följer dataskyddsförordningens krav.

6.3 Resultat

Förvaltningen använder idag verktyget Draftit Privacy records som förteckning för sina personuppgiftsbehandlingar. Året 2020 beslutade förvaltningen att köpa in ytterligare en del av verktyget kallat Draftit Privacy DPIA där risk och konsekvensbedömningar både kan genomföras och registreras. Aktuella konsekvensbedömningar finns registrerade i Draftit DPIA verktyget. Dessa är genomförda främst andra halvan av 2020 där funktioner som medarbetare, dataskyddsamordnare, informationssäkerhetsansvarig, it strateg och dataskyddsombud deltagit.

I Draftit Privacy records finns idag 6 riskregistreringar. Detta är samma antal som fanns registrerade även året innan vilket innebär att inga direkta förändringar har skett på området under 2020. I Draftit Privacy finns idag 6 riskregistreringar vilket dataskyddsombudet bedömer som ett lågt antal med tanke på de känsliga personuppgifter som behandlas inom förvaltningen.

För de 6 riskregistreringar som finns angivna har inte en risk och konsekvensanalys genomförts. Brister som har uppmärksammats är

ofullständiga personuppgiftsbehandlingar, alltså att de inte är fullständigt ifyllda avseende säkerhetsåtgärder, syfte och ändamål, eller ansvarig person. Dessa har därmed klassats till högre risk på grund av att informationen inte är fullständig.

Det som fungerat bra är att när nya personuppgiftsbehandlingar, där verksamheten initialt ser större risker med behandlingen, har dataskyddsombud och informationssäkerhetssamordnare tillfrågats kring bedömning av risker och konsekvenser innan uppstart.

6.3.1 DSO bedömer och rekommenderar

	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
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Här finns två kryss då situationen inte är analyserad fullt ut. Det är ett lågt antal riskregistreringar i Draftit i förhållande till den verksamhet förvaltningen bedriver. Samtidigt har funktionen Draftit Privacy DPIA börjat användas och mer fokus har riktats till risk och konsekvensbedömningar under hösten 2020 och vår 2021. Det finns ett ökat intresse och kunskap inom förvaltningen vilket är en bra utgångspunkt att ta fasta vid i fortsatta arbetet.

Med anledning av resonemanget ovan angående samma antal riskregistreringar 2019 som 2020 är märkvärt. Det är ett område som behöver utvecklas och satsas på kommande år. Det är av vikt att samtliga personuppgiftsbehandlingar värderas utifrån risker innan dessa startas upp eller genomförs. I nuläget är bedömningen från DSO att riskbedömningar genomförs men att ett fortsatt arbete med de registreringar som är gjorda fortlöper och att det antal riskregistreringar som idag finns säkerställs och överensstämmer mellan verksamhet och registerförteckning.

Det finns idag två sätt att genomföra risk och konsekvensbedömningar. Dels via blanketter och vägledande dokument på intranätet som sedan ska diarieföras enligt en egen process men också i det verktyg som just nämns Draftit DPIA. Av granskningen gör DSO bedömningen att detta försvårar för

medarbetare på förvaltningen då det råder förvirring kring vilken metod som ska användas. Eftersom att DPIA verktyget är relativt nytt är rekommendationen att först utvärdera verktyget för att sedan besluta om att gå vidare med en av metoderna för risk och konsekvensanalyser. Förslag för kommande år är att utvärdera verktyget DPIA, besluta om metod och sedan fokusera på information till verksamheter med en kompletterande utbildning inom den metod som valts. Detta är ett bra sätt att öka kunskapen och medvetenheten kring vikten av risk och konsekvensbedömningar. Förvaltningen behöver satsa på att bygga upp en struktur och en ökad kunskap för att lättare lyckas identifiera högriskbehandlingar.

7 Individens rättigheter

7.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	16
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga.

7.2 Syfte

Ett registerutdrag är en sammanställning över den registrerades personuppgifter som behandlas. Syftet med registerutdraget är att den registrerade ska få medvetenhet om att personuppgiftsbehandling sker och på laglig grund.

7.2.1 Resultat

Förvaltningen har rutiner avseende registerbegäran från enskild. Samtliga inkomna begäran om registerutdrag har under året behandlats inom utsatt tid. DSO hanterar administrationen kring inkomna begäran om registerutdrag.

Socialförvaltningen i Stockholm stad har tagit fram en blankett för begäran om registerutdrag tillgänglig för medborgare på stockholm.se. Denna blankett om begäran om registerutdrag berör socialförvaltningens verksamhet men när den inkommit har DSOs utredning visat att det oftast rör sig om efterfrågan av uppgifter från socialtjänsten inom stadsdelarna. Dataskyddsombud har initialt kontaktat den enskilde för att stämma av intentionen med begäran för att sedan vidarebefordra till rätt källa.

Flera av begäran om registerutdrag som inkommit till förvaltningen har varit ställda till fel instans. DSO har lyft detta inom stadens nätverk för dataskyddsombud och till SLKs dataskyddsombud under hösten 2020 men frågan har inte uppmärksammats ytterligare. Detta samarbete inom staden behöver förbättras och en struktur för begäran om registerutdrag bör struktureras tydligare mellan stadsdelar och förvaltningar. Vad förvaltningen behöver göra är att förtydliga rutiner för mottagen registerbegäran, hur man först kan kontrollera om den är rätt ställd till oss, vad vi kan bistå med för information och hur den hanteras.

16 inkomna begäran om registerutdrag har behandlats på förvaltningen genom att göra slagningar på personen enligt enskilds önskemål och enligt rutinerna som finns satta på förvaltningen.

7.2.2 DSO bedömer och rekommenderar

	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

DSOs rekommendation är att framförallt utöka samarbetet och dialogen inom staden kring just begäran om registerutdrag. En dialog kring aktuella blanketter och tillgänglighet för medborgaren bör diskuteras och upprättas likaså samarbetet inom staden vad gäller att hänvisa den enskilde rätt. Uppdraget landar på DSO under år 2020 lyftes ärendet till nätverket för dataskyddsombud inom staden samt SLK. Frågan kan leda till en ökad rättssäkerhet och tydlighet för medarbetare på förvaltningen och för DSOs utredningsarbete vid inkomna begäran.

8 Personuppgiftsincidenter

8.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Enskild meddelar felaktighet, medarbetare anger felaktighet
Hur många personuppgiftsincidenter har dokumenterats?	6 incidenter (2020-12-18) 3 rapporterade men ej diarieförda
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1 har rapporterats till IMY
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Samtliga

8.2 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.” Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter.

8.3 Resultat

Rapporteringar till IMY sker i regel i tid. Det som behöver förstärkas inom förvaltningen är dels förmågan att upptäcka och/eller identifiera en personuppgiftsincident. Den andra delen som kan förstärkas är att rapporteringen till eller kontakten med DSO och informationssäkerhetssamordnaren dröjer. Funktionsbrevlådan för DSO bevakas dagligen vilket innebär att anmälda incidenter behandlas snarast. Det finns rutiner, blanketter och vägledande dokument som stöd vid hanteringen.

8.3.1 DSO bedömer och rekommenderar

	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

Vad som framkommer av granskningen är att förvaltningen brister i incidentrapportering avseende skillnad mellan personuppgiftsincident och övriga incidenter. De brister som finns inom incidentrapportering har DSO identifierar handlar om att det finns en förvirring kring vad en personuppgiftsincident är dels kopplat till övriga incidenter inom förvaltningen och dels hur ärendets gång ser ut.

Det finns idag en god kompetens inom förvaltningen avseende rapportering av personuppgiftsincidenter och en dialog med DSO sker redan i tidigt skede. Däremot bör kunskap om vad en personuppgiftsincident är öka med anledning av vad som framkommit tidigare avseende skillnad mellan incident och personuppgiftsincident. DSO bedömer att mer information om tillvägagångssätt, ärendets gång och vägledning ska förtydligas och nå ut till respektive verksamhet och medarbetare.

DSOs bedömning har visat att det idag inte är helt klart i ärendets gång avseende när en personuppgiftsincident uppmärksammats, när DSO kopplas in och när en bedömning om incidentens art och allvar genomförs. Förtydliganden behöver ske avseende ansvarsfördelning mellan ansvarig chef och DSO vid utredning och rapportering av personuppgiftsincidenter. Detta behöver framförallt ske i de fall där incidenten anmäls till tillsynsmyndighet eftersom det då finns en tidsfrist att förhålla sig till. Ansvarig chef ska utreda och tillgodose anmälan relevant information medan DSO ska tillgodose vägledning och ansvara för att själva anmälan skickas in DSO har i sin bedömning sett att det finns behov av förtydliganden hur informationsutbytet och dialogen mellan ansvarig chef, inblandad medarbetare och DSO bör se ut.

9 Genomförda granskningar

- Tredjelansöverföringar och dokumenterade/diarieförda pub-avtal (särskilt fokus på tredjelandsöverföringar)
- Genomförda och protokollförda informationsklassningar
- Behörighetshantering

9.1 Tredjelansöverföringar

Till följd av Schrems II har förvaltningen uppmanats att identifiera och kartlägga eventuella tredjelandsöverföringar. Med anledning av detta har samtliga chefer tillfrågats och en genomlysning för att först identifiera eventuella överföringar till tredjeland genomförts. När dessa tydliggjorts har varje fall bedöms och utretts vidare. Överföring till tredjeland har stoppats och i några fall har det stoppats i väntan på en bättre lösning genom dialog med dataskyddsombud men framförallt med leverantör. I annat fall har förvaltningen ställt krav på leverantör som i sin tur valt att avstå från lagring i tredjeland och istället upphandlat underleverantörer inom EU eller inom Sverige. Som en del i ovanstående har även arbetet med att se över tecknade pub-avtal varit naturligt.

9.2 Genomförda och protokollförda informationsklassningar

Informationstillgångar ska enligt stadens riktlinje för informationssäkerhet vara informationssäkerhetsklassade med tillhörande protokoll. Under 2020 genomfördes uppföljning av genomförda informationssäkerhetsklassningar i syfte att säkerställa detta. De klassningar av lokala verksamhetssystem som saknat protokoll är kompletterade.

9.3 Behörighetshantering

Brister i behörighetshantering riskerar leda till att åtkomst till känslig information i verksamhetssystem ges till personer som inte längre ska ha åtkomst. Behörighetshanteringen avseende förvaltningens verksamhetssystem för journal har setts över och en förtydligande rutin har tagits fram. De brister som har identifierats har åtgärdats.

9.3.1 DSO och informationssäkerhetssamordnare bedömer och rekommenderar

Dataskyddsarbetet på förvaltningen sker idag mer reaktivt på grund av händelser som kräver åtgärd och inte proaktivt för att exempelvis registerförteckningar ska vara kompletta eller förhindra att incidenter sker. Förbättringsarbetet behöver förtydligas och genomföras med en större systematik.

I denna årsrapport framkommer att det genomförs regelbundna uppföljningar över hur väl kommunen uppfyller de lagkrav som finns vilket resulterat i ett medvetande om brister och att behov av åtgärder. Att säkerställa förvaltningens efterlevnad av GDPR är ett pågående arbete där en stor del av arbetet kvarstår för att efterleva lagen fullt ut. Socialnämnden och förvaltningsledningen bör säkerställa att:

- informationssäkerhetssamordnare och Dataskyddsombud involveras och rådfrågas i högre grad i alla frågor som rör skyddet av personuppgifter
- öka intresset för och säkerställa att GDPR arbetet fortskrider bland annat genom att använda de resultat som framkommit i intern revision och nulägesanalys för att prioritera åtgärder och genomföra dessa på ett systematiskt sätt med tillräckliga resurser.
- fokusera på risk och konsekvensbedömningar samt brister i efterlevnaden av GDPR och därmed införa kontrollåtgärder för detta
- säkerställa att utbildning i informationssäkerhet och dataskydd genomförs av samtliga medarbetare då dessa är obligatoriska och nödvändiga för att medvetenheten om hantering av personuppgifter ska vara tillräcklig
- Fortsatt arbete med Risk och konsekvensbedömningar utifrån vad som framkommer ur denna årsrapport.
- Genomföra informationssäkerhetsklassningar av förvaltningens personsuppgiftsbehandlingar.
- Utvärdering och uppföljning av arbetet och avtalet med Draftit DPIA, verktyget för risk och konsekvensbedömningar.
- Beslut kring att fortsätta med avtalat verktyg eller använda SLKs blanketter som ursprungligen används. Utred om process för diarieföring är aktuell och hur struktur för inrapportering ser ut.
- Följa upp arbetet med tredjelandsöverföringar. Under höst 2020 och vår 2021 har visst arbete kring projekt/enheter som samarbetar med USA och/eller tredjeland utretts. Flertalet har pausats i väntan på fler besked, andra har avslutats och en del av ställt krav på leverantör att ändra samarbetet med underleverantörer vilket gjort att avtalet på nytt kan fullföljas.