Stockholms stad

Dataskyddsombudets årsrapport

2021

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”). Dataskyddsombudet 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

Under året har fortsatt kartläggning och inventering kring tredjelandsöverföring skett inom hela Stockholms stad till följd av tidigare Schrems II[1] fallet i EU domstolen. Under hösten 2021 har delåtgärder presenterats inom ramen för tredjelandsöverföring.

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. Vidare presenteras slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter genomförd uppföljning och granskning.

3 Registerförteckning

3.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	288 registreringar.
Har nödvändiga uppdateringar gjorts?	Delvis.
Bedöms registerförteckningen vara fullständig?	Delvis.

[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.

Har verksamheten lämpliga rutiner för registerföring?	Ja.

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 personuppgiftsbehandlingar vilka finns och hur de hanteras. Registerförteckningen säkerställer att verksamheten beaktar att det ska finnas en laglig grund inom ramen för all personuppgiftsbehandling.

3.3 Resultat

Det finns idag 288 personuppgiftsbehandlingar registrerade i verktyget Draftit Privacy records, sex av dem är riskregistreringar. Sammanfattningsvis är det sju registreringar fler än under 2020. DSO ser det som positivt att flertalet personuppgiftsbehandlingar är registrerade, att förvaltningen börjat använda verktyget Draftit Privacy records i större utsträckning och att det idag finns en större kunskap inom förvaltningen att nya personuppgiftsbehandlingar ska införas i registerförteckningen. DSO bedömer dock att registerförteckningen inte är fullständig och att utvecklingsområdet från tidigare år, år 2020, kvarstår. 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 gällande lagstiftning. Fortsatt implementering av risk- och konsekvensanalys bör ske i samband med registreringar i systemet Drafit Privacy Records.

Registerförteckningen behöver även ses över för att lättare identifiera eventuella personuppgiftsbehandlingar vilken innebär en större risk för den enskilde, dessa kommer att kallas för riskbehandlingar. Här behöver man dels uppmärksamma registreringen av nya personuppgiftsbehandlingar dels 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

[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.

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. En viss uppdatering av listan har skett under senare halvåret 2021.

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

DSO bedömer att förvaltningen har en bra grundstruktur avseende registerförteckningen. Registreringarna vilka registrerats i Drafit Privacy Records år 2021 har till stor del varit fullständiga där behandlingen, ändamål samt övriga nyckeluppgifter är kompletta. De brister som idag finns i förvaltningens registerförteckning behöver dock åtgärdas. Främst behöver gamla registreringar ses över samt att ändamål i förhållande till gällande laglig grund behöver förtydligas. Det är inte ovanligt att en registrering har flera lagliga grunder utan att uppge vad som hör till respektive behandlingsåtgärd

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 pubavtal, detta är också något vilket fortsatt 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 för år 2021 är lågt. Den sammanfattande bedömningen utgår från att registerförteckningen idag inte är fullständig i dess helhet och är ett fortsatt utvecklingsområde.

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?	Ja.
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 i fråga om hantering av 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 pubavtal med vägledning och instruktion, information och blanketter för samtycke, begäran om registerutdrag, rättelse och radering samt

blanketter för risk- och konsekvensbedömning. På fliken finns även generell information om dataskyddslagstiftning, kontaktuppgifter till dataskyddsombud, information om hur dataskyddsorganisationen är uppbyggd, hur ansvarsfördelningen ser ut samt vilka rollförteckning. På fliken hänvisas till en webbutbildning inom dataskydd och informationssäkerhet vilken 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 paraplysystem. 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, 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 framför allt om att tydliggöra information inom förvaltningen och påminna medarbetare i det dagliga arbetet. Blanketter och rutiner finns tillgängligt men kunskapen om ansvarsfördelningen och fördelning av arbetsuppgifter inom

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

olika dataskyddsfrågor, såsom registerförteckning och incidenthantering, saknas delvis. Fortsatt informationsspridning bör även ske ut i verksamheterna avseende intranätet och relevanta styrdokument inom området. Vissa styrdokument kommer även att läggas till på intranätet (tredjelandsöverföring). I och med att det idag finns en tidsfrist för att anmäla allvarliga personuppgiftsincidenter till Integritetsskyddsmyndigheten bör kunskap om vilka incidenter vilka ska anmälas eller inte 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 vilka finns i verksamheten har informationsklassats?	27.
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 27 verksamhetssystem. Förvaltningen har tagit fram en plan för att systematiskt genomföra informationsklassningar löpande avseende de lokala verksamhetssystemen för att säkerställa aktuella klassningar.

5.3.1 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

DSO 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.

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 2021 har förvaltningens DSO även fått tillgång till fler funktioner i Draftit genom

Draftit Expert. Det innebär bland annat att tillgång och behörigheter utökats genom möjlighet till rättsdata, dokument och andra processer inom ramen dataskyddslagstiftningen samt dataskyddsarbetet. Syftet har främst varit att hålla staden uppdaterat på området samt ha rätt verktyg för att sköta dataskyddsarbetet på ett optimalt vis.

I Draftit Privacy records finns idag sex riskregistreringar. Detta är samma antal vilka fanns registrerade även året innan vilket innebär att inga direkta förändringar har skett på området under 2021. Sex riskregistreringar bedömer dataskyddsombudet som ett lågt antal med tanke på de känsliga personuppgifter som behandlas inom förvaltningen. För de sex riskregistreringar som finns angivna har inte en risk och konsekvensanalys genomförts. Vissa brister vilka har uppmärksammats är ofullständiga personuppgiftsbehandlingar, d.v.s. 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.

En generell förbättring är att dataskyddsombudet och informationssäkerhetssamordnare tillfrågats kring bedömning av risker och konsekvenser innan uppstart av nya personuppgiftsbehandlingar.

6.3.1 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

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 i det fortsatta arbetet. 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.

7 Individens rättigheter

7.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	13.
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.

7.3 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 primärkälla.

Flera av begäran om registerutdrag som inkommit till förvaltningen har varit ställda till fel instans. DSO har lyft detta inom stadens nätverk för dataskyddsombud även under 2021 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.

13 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.

7.3.1 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

Fortsatt rekommendation är att 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. Frågan kan leda till en ökad rättssäkerhet och tydlighet för medarbetare på förvaltningen och för DSOs utredningsarbete vid inkomna begäran. Fortsättningsvis, i syfte att öka digitalisering och individen säkerhet, bör möjligheter att se över huruvida den enskilde kan skicka in begäran om registerutdrag per säkra meddelanden eller därmed jämförbart arbetssätt.

8 Personuppgiftsincidenter

8.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Enskild meddelar felaktighet, medarbetare anger felaktighet.
Hur många personuppgiftsincidenter har dokumenterats?	17 incidenter.

Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	3 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 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
x	Inga brister av nämnvärd betydelse identifierade

Det finns idag en god kompetens inom förvaltningen avseende rapportering av personuppgiftsincidenter och en dialog med DSO sker ofta, men inte alltid i tidigt skede.

DSO:ns bedömning har visat att det idag inte alltid är helt klart i ärendets gång avseende när en personuppgiftsincident uppmärksammats, när DSO kopplas in samt 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 ske i de fall där incidenten anmäls till tillsynsmyndighet 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 till IMY. 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. Men anledning av ovanstående markeras riskerna i dels gula dels gröna kolumnen.

9 Genomförda granskningar

9.1 Tredjelansöverföringar

Till följd av Schrems II har förvaltningen under år 2020 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. 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 framför allt med leverantör. Efter sommaren 2021 har vissa samarbeten startats upp igen med anledning av tillfälliga lösningar. Som en del i ovanstående har även arbetet med att se över tecknade pub-avtal varit naturligt.

Under senare delen av hösten 2021 har juridiska avdelningen yttrat sig i frågan om överföring till tredjeland baserat på EU-kommissionens adekvansbeslut. Beslutet innebär att kommissionen har bedömt att dataskyddet i ett visst mottagande tredjeland erbjuder motsvarande skydd för de registrerade som EU:s dataskyddsförordning. Om det inte finns ett sådant adekvansbeslut får personuppgiftsansvarig eller biträde endast överföra personuppgifter till ett tredjeland efter att ha vidtagit lämpliga skyddsåtgärder.[4] En lämplig skyddsåtgärd är EU-kommissionens standardiserade dataskyddsbestämmelser (standardavtalsklausuler), vilka tillämpas tillsammans med en genomförd riskanalys som grund för överföring till tredjeland. EU-kommissionen har den 4 juni 2021 beslutat om nya standardavtalsklausuler

[4] (EU) 2021/914 om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med dataskyddsförordningen. Genomförandebeslut och annex återfinns genom; Standard contractual clauses for international transfers | European Commission (europa.eu).

vilka skulle börja tillämpas från den 27 september 2021, samt Europeiska dataskyddsstyrelsen har den 18 juni 2021 publicerat en rekommendation för hur en riskanalys ska genomföras.

Juridiska avdelningen kommer inom snar framtid att revidera mallen för personuppgiftsbiträdesavtal, vilken kommer att kompletteras med en separat tillkommande mall för standardavtalsklausulen. Standardavtalsklausuler har företräde över personuppgiftsbiträdesavtalet vad gäller personuppgifter som överförs till tredjeland.

Avtal som ingåtts med stöd av dessa äldre standardavtalsklausuler ska anses garantera lämpliga skyddsåtgärder fram till den 27 december 2022 under förutsättning att de behandlingar som är föremål för avtalet förblir oförändrade och att användningen av dessa klausuler säkerställer att överföringen av personuppgifter omfattas av lämpliga skyddsåtgärder. För nya avtal som ingås från den 27 september 2021 ska de nya standardavtalsklausulerna användas. De nya klausulerna innehåller en avtalsmall för olika situationer beroende på parternas rollfördelning för personuppgiftsansvaret. Det är inga färdiga avtal att hänvisa till såsom de tidigare klausulerna. En del information behöver fyllas i för att avtalet ska bli fullständigt. Det pågår ett arbete med att uppdatera mallen för standardavtalsklausul samt mallen för personuppgiftsbiträdesavtal. Mallarna kommer att publiceras på Intranätet (under GDPR). Relevant övrig information om tredjelandsöverföring finns att läsa på intranätet.

9.2 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. De brister som har identifierats har åtgärdats.

9.2.1 Bedömning och rekommendationer

Förvaltningen har fortsatt arbetat med att få ett uppdaterat personuppgiftsregister vilket är grundförutsättning för att lyckas med dataskyddsarbetet. Parallellt har förvaltningen satt en tydlig organisation kring hur dataskyddsfrågorna ska omhändertas och slagit fast en anvisning hur förvaltningen ska arbeta med dataskydd.

Dataskyddsarbetet på förvaltningen behöver ske mer proaktivt för att exempelvis registerförteckningar ska vara kompletta eller förhindra att incidenter sker. Förbättringsarbetet behöver förtydligas och genomföras med en större systematik. Ett frekvent förekommande önskemål från tjänstepersoner är utökade informationsinsatser och utbildningar till följd av regelverkets komplexitet och frånvaro av prejudikat. Dataskyddsombudet rekommenderar därför att samtliga medarbetare genomför e-utbildningar inom området, vilka tillhandahålls på intranätet.

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

- Informationssäkerhetssamordnare och dataskyddsombud involveras och rådfrågas i högre grad i samtliga frågor vilka omfattas av skyddet av personuppgifter.
- Fortsatt arbete med risk- och konsekvensbedömningar och införande av kontrollåtgärder för detta.
- Fortsatt utvärdering och uppföljning av arbetet och avtalet med Draftit DPIA, verktyget för risk och konsekvensbedömningar.
- 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.
- Genomföra informationssäkerhetsklassningar av förvaltningens personsuppgiftsbehandlingar.
- Fortsatt kartläggning av biträdessituation samt nyteckning av biträdesavtal inom respektive nämnd/verksamhet.
- Undersöka möjligheter för implementering av tekniska lösningar vid den enskildes begäran om registerutdrag.
- Implementering och förankring av slutgiltiga styr- och stöddokument inom ramen för tredjelandsöverföringar.