Stockholms läns sjukvårdsområde
Sjukvårdsdirektören

ANMÄLAN
2023-02-01

SLSO 2023-0371

Årsrapport GDPR för verksamhetsåret 2022

Årsrapport GDPR för verksamhetsåret 2022 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2023-01-20

Diarienummer
SLSO 2023-0371

Årsrapport GDPR

För verksamhetsåret 2022

Innehållsförteckning

1. Inledning 3

2. Dataskyddsombudets organisation 3
2.1 Bedömning 3
2.2 Åtgärd 3

3. Dataskyddsombudets arbete i dataskyddsfrågor 4
3.1 Bedömning 4
3.2 Åtgärd 5

4. Registerförteckning 6
4.1 Bedömning 6
4.2 Åtgärd 7

5. Medborgares rättigheter 7
5.1 Bedömning 7
5.2 Åtgärd 8

6. Personuppgiftsincidenter och tillsyn 8
6.1 Bedömning 8
6.2 Åtgärd 9

7. Styrdokument 10
7.1 Bedömning 10
7.2 Åtgärd 10

8. Omvärldsbevakning 10
8.1 Bedömning 13
8.2 Åtgärd 13

9. Konklusion 13

1. Inledning

Dataskyddsombudet (DSO) ska enligt artikel 38 i GDPR rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå, vilket för Stockholms läns sjukvårdsområde (SLSO) är nämnden, då SLSO:s nämnd har det yttersta ansvaret för verksamhetens personuppgiftshantering enligt artikel 24 i GDPR.

Denna rapport avser att uppfylla dessa krav och sammanfatta dataskyddsombudens iakttagelser och arbete under det gångna året.

2. Dataskyddsombudets organisation

Av artikel 24 i GDPR följer att SLSO ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att organisationens personuppgiftsbehandlingar följer GDPR. Organisatoriska åtgärder som en tydlig och fastställd dataskyddsorganisation hjälper till att säkerställa ordning och reda när det gäller dataskydd, personuppgiftshantering och informationssäkerhet

2.1 Bedömning

DSO upplever, likt föregående år, arbetet i dataskyddsfrågorna som reaktivt snarare än proaktivt och för att nå ett långsiktigt tillika proaktivt arbete i frågorna kring dataskydd behöver en organisation kring DSO etableras. Etableringen av en organisation kring dataskydd och informationssäkerhet påbörjades av SLSO:s informationssäkerhetssamordnare under 2020 men fick av förklarliga skäl under 2021 stå tillbaka på grund av den pågående pandemin.

2.2 Åtgärd

Under 2022 har DSO tillsammans med informationssäkerhetssamordnaren uppvaktat fem verksamheter och informerat om behovet av en dataskyddsorganisation för SLSO. De verksamheter som har besökts har i sin tur utnämnt representanter som ska vara dataskyddskoordinatorer för respektive verksamhet. Koordinatorernas uppgift blir att besvara enklare frågor om dataskydd för att avlasta dataskyddsombuden och informationssäkerhetssamordnare. De ska även sprida information om dataskydd i sina respektive verksamheter.

Under hösten har det hållits två introduktionsmöten för dataskydds-koordinatorerna. Målet framgent är två mötesdagar för dataskyddskoordinatorer per termin. Syftet med mötesdagarna är att ge tillfälle för samtal och vidareutbildning i frågor om dataskydd och informationssäkerhet.

3. Dataskyddsombudets arbete i dataskyddsfrågor

Enligt artikel 39 ska Dataskyddsombudet övervaka och ge råd till den personuppgiftsansvarige så att kraven i GDPR uppfylls. Detta kan ske genom information och utbildning till de anställda, delta i bedömningar som rör skyddet av personuppgifter som till exempel vid konsekvensbedömningar enligt art. 35 (DPIA). En sådan bedömning ska göras om behandling av personuppgifter avser användning av ny teknik, stor omfattning av personuppgifter som kan medföra stora risker för fysiska personers fri- och rättigheter som till exempel inom vården där känsliga personuppgifter hanteras.

3.1 Bedömning

DSO kan konstatera att verksamheterna – till stor del nu har förstått kravet att göra en bedömning av dataskyddet i varje ny situation där personuppgifter kommer att hanteras. I de allra flesta fall behöver det endast göras en så kallad grundläggande bedömning av personuppgiftshanteringen, inte en konsekvensbedömning avseende dataskydd enligt art. 35. För ändamålet att göra en grundläggande bedömning tillhandahåller SLSO en mall som är till fyllest för att konstatera syfte med personuppgiftsbehandlingen, vilka personuppgifter som kommer att hanteras, val av skyddsåtgärder samt utifrån vilken rättslig grund som personuppgifterna hanteras.

Den av Regionledningskontoret (RLK) framtagna metod för konsekvensbedömningar som togs fram 2021 har inte behövts användas under det gånga året. RLK:s regiongemensamma metod upplevs av DSO som mycket gedigen men tidskrävande. Metoden svarar dock upp mot de krav som ställs på en konsekvensbedömning enligt art.35.

En återkommande frågeställning och utmaning som ofta uppstår i samband med nya personuppgiftsbehandlingar är huruvida verksamheterna får använda sig av molntjänstbaserade IT-lösningar. I tillägg till de juridiska utmaningarna med molntjänster inom EU/EES så tillkommer situationer då leverantörer använder molntjänster som även överför person- eller patientuppgifter utanför EU:s/EES gränser vilket medför att det uppstår så kallade tredje landsöverföringar. Sådan personuppgiftsbehandling är i grunden förbjuden men kan accepteras under vissa förutsättningar.

Vidare så kan DSO konstatera att det saknas en ändamålsenlig bedömningsprocess inom SLSO vid anskaffning och bedömning av molntjänster vilket bland annat innebär att DSO i regel blir inkopplad när personuppgiftsbiträdesavtal ska skrivas. IMY publicerade under det gånga året en sammanställning gällande användningen av molntjänster inom offentlig sektor. I sammanställningen framkommer det bland annat en relativt enhetlig bild att det är svårt att hitta molntjänster som är förenliga med dataskyddsregelverket, svårigheter att förhandla med molntjänstleverantörer och därmed svårt att påverka utformningen eller

villkoren för tjänsten samt att myndigheternas kontroll av molntjänstleverantörer skiljde sig åt i både omfattning och tidsperspektiv. I samband med molntjänstfrågan har DSO även noterat att ett flertal statliga myndigheter tagit principbeslut huruvida molntjänster får användas eller ej vilket i dagsläget inte finns inom SLSO.

I samband med hälso- och sjukvårdsförvaltningens (HSF) delegationsbeslut att ge SLSO i uppdrag att genomföra en fördjupad förstudie för att undersöka om applikationen Alltid öppet kan tjäna som systemstöd för smittspårning konstaterade DSO att Vårdportalen är att likställa med ett journalsystem. Vårdportalen är vårdpersonalens vy i informationsflödet kopplat till applikationen Alltid öppet som ägs av SLSO.

Initialt togs Alltid öppet fram för att öka vårdens tillgänglighet genom att möjliggöra tidsbokning till digitala sjukvårdsmöten inom hälso- och sjukvård. För att uppnå det syftet hanterades kategorier av personuppgifter i en omfattning som gjorde att Alltid öppet inte var att anse som ett journalsystem. Detta faktum ändrades i samband med covid-19 pandemin då applikationens användningsmöjligheter förändrades genom att till exempel patienten tillika vårdtagaren uppmanas att fylla i frågeformulär inför vaccination eller mottagningsbesök – patientuppgifter är känsliga personuppgifter enligt art.9 i GDPR började därmed hanteras i stor skala i applikationen.

Enligt patientdatalagen som kompletterar GDPR, anses en patientjournal bestå utav en eller flera uppgifter om en patient. Som patientuppgift räknas orsak till vården, uppgifter om patienten, diagnos, planerade och genomförda åtgärder. Om dessa uppgifter dessutom används i samband med en vårdprocess så är det informationsmängden att anse som en patientjournal. Eftersom dessa kriterier är uppfyllda för informationshantering i Alltid öppet anser DSO och jurist på SLSO att Alltid öppet således är att betrakta som ett journalsystem.

Den samlade bedömningen av det generella kunskapsläget gällande dataskydd är att det bland medarbetare fortsatt finns både kunskapsluckor och en del samarbetssvårigheter gällande de skyldigheter som SLSO har enligt GDPR. De verksamheter som har uppenbara kunskapsbrister anser DSO vara någorlunda inringade och åtgärder om dessa beskrivs nedan. Dataskyddsombudet har under verksamhetsåret gett råd och stöd i löpande frågor som inkommit från både medarbetare och allmänheten.

3.2 Åtgärd

I syfte att förbättra och effektivisera SLSO:s arbete med bedömningar av IT-tjänster i vilket molntjänster är en viktigt del, så har SLSO:s IT-direktör tagit initiativ till återkommande it-säkerhetsforum med start i januari 2023. IT-säkerhetsforumet kommer bland annat hantera frågor gällande molntjänstanvändning och dess bedömning utifrån kraven i GDPR, Region

Stockholms riktlinje för informationssäkerhet och SLSO:s IT-arkitektur. Det är önskvärt att SLSO:s nämnd ger DSO i uppdrag att skriva fram beslutsunderlag för huruvida SLSO:s verksamheter får använda molntjänstlösningar där personuppgifter förs ut utanför EU/EES området.

Gällande Alltid öppet så kommer DSO under 2023 medverka i arbetet med komplettering av konsekvensbedömning avseende dataskydd samt övriga aktiviteter då plattformen numera är att anses som ett journalsystem.

De åliggande som DSO har är beskrivna i art 39 i GDPR. Från flera håll har det dock lyfts rekommendationen att personuppgiftsansvarig bör ta fram en uppdragsbeskrivning för DSO.

För att höja kunskapsnivån kommer DSO under verksamhetsåret fortsätta med utbildnings- och informationsinsatser riktade mot ledningsgrupper, enheter och övriga anställda samt verksamhetsanpassade utbildningar efter beställning från verksamheten. Under 2022 hade DSO till exempel ett specifikt önskemål om att hålla föredragningar om personuppgiftsincidenter.

Sedan tidigare har även en generell utbildning gällande GDPR tagits fram och erbjuds via den regiongemensamma plattformen, Lärtorget. Utbildningen är sedan 2022 obligatorisk för alla anställda inom SLSO och DSO kommer under året att arbeta för att synliggöra utbildningen i syfte att öka kunskapen om dataskydd.

4. Registerförteckning

SLSO ska enligt artikel 30 föra ett register över de personuppgiftsbehandlingar som utförs under dess ansvar, en så kallad registerförteckning. Under det gånga året har IT-stödet Draftit implementerats som en digital registerförteckning över alla nya personuppgiftshanteringar. Parallellt med Draftit finns även den gamla excelfil som innehåller de registreringar om SLSO:s personregister som registrerades innan Draftit i dåvarande IT-stödet PUH. Avvägningen att inte migrera de gamla registreringarna från PUH till Draftit har gjorts på grundval av det faktum att sättet och informationsmängderna i de två olika systemen skiljer sig väsentligt åt.

4.1 Bedömning

Personuppgiftsbehandlingar tillkommer och förändras ständigt. Genom att implementera den nya digitala plattformen Draftit så har en avlastning skett för DSO då huvudansvaret för anmälningen läggs på registeransvarig. Systemet är användarvänligt och intuitivt däremot finns det förbättringsbehov av systemet vilket även uppmärksammats av regionledningskontoret som också för en dialog med leverantören. RLK,

som är upphandlande part för Region Stockholms alla ingående förvaltningar och bolag, kommer under 2023 att sondera marknaden efter likartade IT-stöd för att utvärdera om nuvarande IT-stöd är det mest optimala och funktionella stöd som kan användas när det gäller personuppgiftsregistreringar och tillhörande processer så som konsekvensbedömning avseende dataskydd.

4.2 Åtgärd

DSO kommer delta i utvärderingen av Draftit tillsammans med RLK och verka för att Draftit utvecklas.

5. Medborgares rättigheter

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt GDPR. Dessa rättigheter innebär i korthet att de registrerade ska få information om när, hur och varför deras personuppgifter behandlas. Personuppgifterna ska vara korrekta. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade eller att få ut eller flytta sina uppgifter.
Dessvärre har endast hälften av Sveriges befolkning kunskap om GDPR och rätten till information hur myndigheter och andra aktörer hanterar individers personuppgifter enligt Integritetsskyddsmyndighetens (IMY) rapport Digital integritet 2022.

Som individ har man bland annat rätt att få veta vad för slags information som finns hos en aktör som kan kopplas till individen själv samt varför aktören hanterar information, ändamålet med hanteringen och utifrån vilken rättslig grund informationen hanteras.

Enligt reglerna i patientdatalagen som kompletterar GDPR har medborgare dessutom rätt få veta vem som haft åtkomst till deras patientjournal genom så kallat utdrag av logglista.

5.1 Bedömning

Få förfrågningar inkom under det gånga året gällande individers registerutdrag vilket tros bero på individers okunskap om sina rättigheter att få veta vad som registreras om dem, vilket även IMY påpekade i sin rapport.

DSO konstaterar att det finns fortsatta tekniska svårigheter att leverera ett komplett och strukturerat registerutdrag via ett IT-stöd. Detta beror på strukturella förutsättningar. Exempelvis, om en före detta anställd önskar registerutdrag från tidigare anställningar måste flera enheter kontaktas för att få fram önskad information. Däremot kan uppgifter i till exempel

journal och e-post med enkelhet tillhandahållas. DSO har även uppmärksammat att utlämning av så kallade logglistor enligt PDL/GDPR har haft olika utformning inom Region Stockholm då instruktionerna inte varit helt homogena.

I arbetet med registerutdrag har DSO en sammanhållande funktion för att delegera ut uppdrag till de olika enheterna som kan inneha olika slags dokument och information.

5.2 Åtgärd

Region Stockholms policyråd har under sista delen av 2022 arbetat med att ta fram och rekommendera en gemensam instruktion för utlämnande av loggutdrag. De uppdaterade dokumenten som till stor del bygger på SLSO:s tidigare dokument är tänkta att gälla för alla vårdgivare inom Region Stockholm och SLSO informerade via intranätet om denna uppdatering i januari 2023.

6. Personuppgiftsincidenter och tillsyn

En personuppgiftsincident är 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 hanterats. Dessa incidenter ska utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmälas till Integritetsskyddsmyndigheten (IMY).

6.1 Bedömning

Givet SLSO:s storlek så får antalet inrapporterade incidenter anses vara relativt lågt. En eventuell låg rapporteringsgrad är brist i dataskyddet, dels för att det strider mot GDPR att inte dokumentera och rapportera incidenter, dels att det försvårar arbetet med att identifiera brister och arbeta med ständiga förbättringar för att förebygga att nya personuppgiftsincidenter ska inträffa.

Det låga antalet inrapporterade personuppgiftsincidenter beror troligen på bristande medvetenhet om vad en personuppgiftsincident är. Det kan dock konstateras att verksamheterna i ökad utsträckning söker DSO:s bedömning huruvida en negativ händelse utgör en personuppgiftsincident eller inte, vilket är glädjande och får anses vara ett tecken på ökad kunskap inom området.

De flesta incidenter som har rapporterats till DSO är majoriteten av det slag som har kategoriserats enligt IMY:s definitioner som ”obehörigt röjande genom felaktigt utskick av mejl/brev/sms” samt ”obehörig åtkomst någon inom eller utanför organisationen har tagit del av information som denne saknade behörighet till”.

IMY fick den 20 april 2022 in ett klagomål där det uppgavs att klagandens förälder kontaktats av en person som fått hem klagandens provsvar i samband med ett annat utskick från en verksamhet inom SLSO. Ett brevutskick innehållande känsliga personuppgifter hade således kommit en obehörig person tillhanda. Mot bakgrund av detta så beslutade IMY att inleda en tillsyn för att utreda om SLSO vidtagit lämpliga tekniska och organisatoriska säkerhetsåtgärder enligt artikel 32 i GDPR för att skydda personuppgifterna i samband med brevutskicket.

Tillsynen bestod i ett antal frågor gällande SLSO:s kännedom om det inträffade, hur personuppgifterna som skickades via brev skyddades samt om det finns utformade instruktioner/rutiner för hantering av personuppgifter i samband med brevutskick.

Enligt verksamhetens lokala rutin, skriver läkare eller sekreterare brev till patienter och kuverteras samt frankeras av en receptionist som lägger brevet på postlådan vid dagens slut. Personuppgifterna är därmed skyddade från obehörig personal. Det faktum att brevet hamnade fel berodde på den mänskliga faktorn. I samband med händelsen har vårdcentralen ytterligare skärpt noggrannheten vid kuvertering och har påmint om vikten av att personen som lägger breven i kuvert inte blir störd under sin arbetsuppgift.

IMY:s utredning visar att det rör sig om ett misstag i ett enskilt fall som inte kan anses ha orsakats av bristande rutiner eller avsaknad av ytterligare lämpliga tekniska eller organisatoriska åtgärder från nämndens sida. IMY konstaterar därför att utredningen i ärendet inte visar att nämnden brustit i sina skyldigheter enligt artikel 32 i GDPR vid den behandling som tillsynen omfattar.

Frågorna besvarades av verksamhetschef från berörd verksamhet samt tillförordnad sjukvårdsdirektör som företrädde SLSO:s nämnd i ärendet.

6.2 Åtgärd

DSO har genomfört särskilda informationsinsatser till primärvårdens verksamhetschefer för att informera om vad som utgör en personuppgiftsincident samt vikten att göra incidentanmälan till IMY då även underlåtenhet att rapportera känd incident kan medföra sanktionsavgifter.

Fortsatt informationsspridning via SLSO:s intranät Insidan och dataskyddskoordinatornätverket kommer att genomföras för att bibehålla och öka medvetenhet kring personuppgiftsincidenter och reglerna i GDPR.

7. Styrdokument

En grundläggande princip i GDPR är den s.k. ansvarsskyldigheten vilket innebär att SLSO måste kunna visa att organisationen lever upp till förordningens krav. Den ansvarige, vilket ytterst är SLSO:s nämnd, har således bevisbördan för detta och dokumentationen blir därför en viktig del för upprätthållande av rättssäkerhet. Vid eventuell tillsyn kan avsaknad av dokumentation innebära att tillsynsmyndigheten är mer benägen att tilldöma sanktionsavgifter. Med andra ord ställer GDPR höga krav på dokumentation.

SLSO har följande styrdokument för dataskydd:

- Personuppgiftshantering – övergripande anvisning för SLSO
- Personuppgiftsincident – övergripande anvisning SLSO
- E-postanvändning – övergripande anvisning för SLSO
- Registerutdrag – övergripande anvisning
- Riktlinje för informationssäkerhet inom Region Stockholm
- Region Stockholms Verksamhetsskyddspolicy

För att SLSO ska kunna bedriva ett systematiskt och kvalitativt dataskyddsarbete krävs att relevant information finns lättillgänglig för alla medarbetare. Samtliga styrdokument finns samlade för anställda att ta del av på intranätet samt i ärende- och dokumenthanteringssystemet Platina/EDIT.

7.1 Bedömning

Kommunikation via intranätet är ett sätt att öka kunskapen om dataskydd samt skapa förutsättningar för verksamheten att kunna följa GDPR:s bestämmelser. Informationstexter som är en viktig del i arbetet finns framtagna och tillgängliga via intranätet.

7.2 Åtgärd

Årlig översyn av den övergripande anvisningen för personuppgiftshantering och vidareutveckla eventuella dokument för strategiska ställningstagande gällande SLSO:s dataskydd. Slutligen ska det under året ske fortlöpande översyn av informationssidan på intranätet.

8. Omvärldsbevakning

En noggrann och omfattande omvärldsbevakning är av stor vikt då tolkning av både GDPR och avgörande i EU-domstolen är under konstant förändring vilket har bäring på SLSO:s hantering av personuppgifter.

Här nedan följer ett axplock av avgörande och notiser som har bäring även för SLSO:s räkning.

Användning av tjänstemobiler
IMY ålade Tullverket en sanktionsavgift om 300 000 kr med anledning av att några anställda i sina tjänstemobiler använt molntjänsten Google Foto. Tjänstemännen hade kopplat sina privata Google Foto-konton till sina tjänstemobiler som automatiskt synkat de foton och filmer som tagits i tjänsten till en amerikansk molntjänst, en så kallad tredje landsöverföring. Det låga värdet av sanktionsavgiften motiverades med att användningen av Google Foto inte var tillåten inom myndigheten samt att Tullverket vidtagit både tekniska och organisatoriska åtgärder för att förebygga liknande incidenter, bland annat genom att förtydliga riktlinjer och begränsa möjligheterna att ladda ner applikationer.

Region Uppsala hantering av känsliga personuppgifter
Region Uppsalas regionstyrelse och styrelsen för Akademiska sjukhus ålades sanktionsavgifter om 300 000 respektive 1, 6 miljoner på grund av bristande hantering av patientuppgifter.

Första utredningen gällde e-post med patientuppgifter (känsliga personuppgifter enligt artikel 9 GDPR) inklusive personnummer som hade skickats automatiserat till berörda vårdförvaltningar inom regionen. Utöver detta hade även e-post med patientuppgifter skickats manuellt till forskare och läkare inom regionen. Överföringen av e-posten var krypterad men informationen (de känsliga personuppgifterna) i e-postmeddelandet var inte krypterade vilket är nödvändigt för att uppnå en god säkerhet genom kryptering.

Akademiska Sjukhuset som drabbats av den större sanktionsavgiften hade skickat e-post med patientuppgifter till patienter och remittenter i tredjeland, alltså länder utanför EU/EES. IMY:s granskning omfattade även lagringen av patientuppgifter i sjukhusets e-postserver. IMY konstaterade att sjukhuset granskat säkerheten för de personuppgifter som behandlats men har inte granskat lagligheten i själva tredjelandsöverföringen och därmed brustit i sina skyldigheter gentemot GDPR.

Diabetes- app
Region Dalarnas primärvårdsverksamhet hade ett önskemål om att upphandla en applikation för diabetesvården. Applikationen och dess sensorer ger diabetessjuksköterskor och läkare möjlighet att följa patienternas blodsockervärden i realtid.

Applikationen samlar in patientdata och dessa känsliga personuppgifter hanteras i en molntjänst och servrar som är geografiskt lokaliserade utanför EU/EES. En tredjelandsöverföring av känsliga personuppgifter behövde således bedömas lämplig eller olämplig. Region Dalarnas regionjurist och dataskyddsombud, har tillsammans med sina kolleger kommit fram till att användningen av diabetsappen kan vara en så kallad olaglig tredjelandsöverföring och därmed inte förenlig med GDPR.

Trots tjänstemännens avrådan så beslöt regionstyrelsen i Region Dalarna likväl att inhandla applikationen för att öka patientsäkerheten. IMY:s enhetschef på enheten för myndigheter, vård och utbildning, kommenterade beslutet med att GDPR varken är något valbart eller en prioriteringsfråga: *”Det är regler som EU och Sveriges riksdag antagit, som ska värna den mänskliga rättigheten till privatliv*”.

Myndigheters molntjänstanvändande
IMY gjorde en undersökning tillsammans med europeiska dataskyddstyrelsen i februari 2022 för att få information om huruvida myndigheter och förvaltningar använder molntjänster. Sju myndigheter inkom med svar till tillsynsmyndigheten.

I rapporten framkom intressanta fynd såsom att myndigheter använde molntjänster som verksamhetsstöd för att hantera anställdas personuppgifter. Det finns bristande kunskaper hos molntjänstleverantörer om grundläggande dataskyddsregler vilket i sin tur ställer stora krav på upphandlande myndigheter. Rapporten visar även att kravställning och dialog med molntjänstleverantörer visar sig vara relativt enspårig då det är svårt att förhandla med molntjänstleverantörer för att kunna påverka användningen av själva tjänsten.

Schrems II
Schrems II-målet fortsätter att påverka arbetet med personuppgifts-hanteringen. EU-domstolen slår fast att Privacy Shield-avtalet mellan EU och USA inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA vilket innebär att det inte längre är tillåtet för personuppgiftsansvariga i EU att med Privacy Shield som grund överföra personuppgifter till mottagare i USA. Överläggningar mellan EU och USA pågår för att undanröja rättsliga hinder för flödet av personuppgifter men det finns i dagsläget ingen överenskommelse.

Utmaningar med så kallade tredjelandsöverföringar är inte bara aktuell när det gäller överföring av personuppgifter till USA utan även andra länder som har avvikande rättslig regling avseende den personliga integriteten. Detta medför att en eventuell ny överenskommelse mellan EU och USA inte kommer att lösa problemet då flera amerikanska molntjänstleverantörer även har underleverantörer i länder som befinner sig utanför EU/EES som har bristande integritetslagstiftning. I många fall tillhandahåller dessa underleverantörer support åt molntjänstleverantören och kommer på så sätt åt personuppgifter.

IMY:s rapport om dataskyddsarbete i praktiken
I dagarna kom IMY:s rapport som berör dataskyddsombudens förutsättningar att bedriva dataskyddsarbete. Rapporten bygger på en enkät som besvarats av dataskyddsombud i närmare 800 verksamheter.

Tillsynsmyndigheten konstaterar att endast hälften av DSO:erna upplever att de får gehör för dataskyddsfrågor från ledningen eller den personuppgiftsansvariga. I likhet med ovanstående beskrivning, upplever endast hälften av dataskyddsombuden att de blir involverade i god tid. Många dataskyddsombud vittnar även om att verksamheterna ser dataskyddsförordningen som ett hinder. IMY konstaterar, utan att den högsta ledningen engagerar sig i dataskyddsfrågorna kommer verksamheten ha fortsatta utmaningar i implementeringen och efterlevnaden av dataskyddsreglerna och dataskyddsombuden kommer ha en utmanande roll att fylla.

8.1 Bedömning

DSO delar uppfattningen till stor del kring resultaten i IMY:s rapport. Det finns fortfarande delar av SLSO:s verksamhet som upplever att dataskyddsarbetet är obstruerande och det händer likväl att DSO blir för sent involverad i ärenden där reglerna för GDPR blir tillämpliga.

8.2 Åtgärd

DSO fortsätter att hålla sig á jour för att arbeta proaktivt med personuppgiftshantering. För att kunna göra detta kommer DSO fortsätta att delta i nätverksträffar och utbildningar samt bevaka praxis och nyheter och informera berörda när informationen är relevant för dem.

9. Konklusion

Likt föregående år anser DSO att det fortsatt krävs fokus på att öka förståelsen inom organisationen genom både fysiska och digitala utbildningsinsatser samt upprättande av nya rutiner. Genom uppbyggnad av datakoordinatorsnätverket hoppas DSO på en ökad spridning av kunskap av information om dataskydd och informationssäkerhet ute i verksamheterna.

Slutligen kan DSO konstatera att Schrems II-domen fortsatt har en signifikant påverkan på SLSO:s personuppgiftshantering och framför allt påverkar bedömningen huruvida en molntjänst kan användas eller om personuppgifter får föras ut utanför Sveriges gränser.
Att person- och patientuppgifter flödar genom molntjänster som tillhandahålls av leverantörer som befinner sig utanför Sverige eller EU/EES anses som obehörigt röjande enligt reglerna inom offentlighet- och sekretesslagen och GDPR då de registrerades personliga integritet inte kan säkerställas utanför Sveriges eller EU:s gränser. Individerna förlorar även kontrollen över sina personuppgifter.

DSO anser att det vore önskvärt att SLSO:s nämnd tar ställning till om ingående verksamheter överhuvudtaget får använda molntjänster eller inte samt ger DSO i uppdrag att skriva fram ett beslutsunderlag för nämndbeslut.

Rapporteringssätt och regelbundenheten kan utökas och utvecklas om SLSO:s nämnd så önskar.

Stockholm, januari 2023

Camilla Heise Löwgren
Dataskyddsombud

Henrik Strand
Dataskyddsombud