Stockholms läns sjukvårdsområde
Sjukvårdsdirektören

ANMÄLAN
2022-01-18

SLSO 2022-0301

Årsrapport GDPR för verksamhetsåret 2021

Årsrapport GDPR för verksamhetsåret 2021 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2022-01-27

Diarienummer
SLSO 2022-0301

Årsrapport GDPR

För verksamhetsåret 2021

Innehållsförteckning

1. Inledning 3

2. Dataskyddsombudets organisation 3
2.1 Bedömning 3
2.2 Åtgärd 3

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

4. Registerförteckning 5
4.1 Bedömning 5
4.2 Åtgärd 6

5. Medborgares rättigheter 6
5.1 Bedömning 6
5.2 Åtgärd 6

6. Personuppgiftsincidenter 6
6.1 Bedömning 7
6.2 Åtgärd 7

7. Styrdokument 8
7.1 Bedömning 8
7.2 Åtgärd 8

8. Omvärldsbevakning 9
8.1 Bedömning 9
8.2 Åtgärd 9

9. Konklusion 9

1. Inledning

Dataskyddsombudet (DSO) ska enligt artikel 38 i dataskyddsförordningen 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 dataskyddsförordningen.

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

2. Dataskyddsombudets organisation

Av artikel 24 i dataskyddsförordningen följer att SLSO ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att organisationens personuppgiftsbehandlingar följer dataskyddsförordningen. 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. DSO och externa revisorer bedömer att arbetet rimligen kan återupptas under 2022.

2.2 Åtgärd

Givet en förhoppning att den ansträngda arbetssituationen under pågående covid-19 pandemi förbättras, behöver DSO driva på arbetet i skapandet av en dataskyddsorganisation tillsammans med SLSO:s informationssäkerhetssamordnare. Arbetet kan lämpligen påbörjas inom de mer administrativa verksamhetsstöden inom SLSO för att sedan spridas inom kärnverksamheten.

3. Dataskyddsombudets arbete i dataskyddsfrågor

Enligt artikel 38 ska dataskyddsombudet på ett korrekt sätt och i god tid delta i alla frågor som rör skyddet av personuppgifter som till exempel konsekvensbedömningar enligt art. 35. 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 har under 2021 upplevt utmaningar när det gäller konsekvensbedömningar avseende dataskydd där SLSO:s verksamhet upplever nuvarande metod som något omständlig och tidskrävande. Som konsekvens av detta har diskussioner uppstått där en del verksamheter har uttryckt en vilja att använda mall och metod från andra bolag/nämnder inom Region Stockholm. DSO har inte accepterat metoder från andra bolag och nämnder inom Region Stockholm då dessa ej ansetts svara upp till de krav som ställs på en konsekvensbedömning. Således har de konsekvensbedömningarna varit otillfredsställande utifrån grundläggande kunskap om personuppgiftshanteringen och riskhanteringen vilket SLSO:s DSO inte har accepterat.

Regionledningskontoret har under 2021 tagit fram en regiongemensam metod för konsekvensbedömningar vilken upplevs av DSO som mycket gedigen men något mer tidskrävande än nuvarande metod. Bedömningen är dock att denna metod bättre svarar upp mot de krav som ställs på en konsekvensbedömning enligt dataskyddsförordningen. Ett gemensamt arbetssätt inom Region Stockholm gör att tidskrävande diskussioner och samarbetssvårigheter inte blir lika vanligt förekommande samtidigt som konsekvensbedömningen som sådan ökar i kvalitet. DSO bedömer således att SLSO ska implementera det regiongemensamma arbetssättet gällande konsekvensbedömningar.

Dataskyddsombudet har under verksamhetsåret gett råd och stöd i löpande frågor som inkommit från både medarbetare och allmänheten. Dataskyddsombudet har genomfört utbildnings- och informationsinsatser riktade mot ledningsgrupper, enheter och övriga anställda. Verksamhetsanpassade utbildningar har även genomförts efter beställning från verksamheter. Sedan tidigare har även en generell utbildning gällande dataskyddsförordningen tagits fram och erbjuds via plattformen Lärtorget, utbildningen bör samtliga medarbetare genomföra som ett led i att höja medvetenheten och kunskapen gällande personuppgiftshanteringar och de krav som ställs. Bedömningen är att genomförandegraden av utbildningen är något låg och behöver förbättras.

Det har under året noterats en kunskapsvariation i frågor beträffande dataskydd vilket bland annat inneburit att det förekommit situationer då DSO involverats sent eller inte alls i processen gällande personuppgiftshantering och dess skydd.

3.2 Åtgärd

Den 24 januari 2022 beslutade SLSO:s tf. sjukvårdsdirektör och FoUU direktör att SLSO framgent ska använda den regiongemensamma metoden för konsekvensbedömningar. Beslutet togs på inrådan av dataskyddsombudet. Det nya arbetssättet kommer starta så fort metod och

mall har kvalitetssäkrats av regionledningskontoret och i samband med uppstart gör DSO tillsammans med kommunikationsavdelningen en kommunikationsinsats för att sprida nyheten inom nämnden.

DSO kommer löpande utbilda och informera om metoden för konsekvensbedömningar i lämpliga forum som ”Behovsgruppen” och Kvalitetssäkringsrådet där alla SLSO:s nya behov och ofta personuppgiftshanteringar hanteras.

DSO kommer fortsätta sitt arbete med att medvetandegöra och utbilda inom organisationen och tydliggöra de krav som ställs på personuppgiftshanteringar. Detta sker bland annat inom ramen för SLSO:s kvalitetssäkringsråd.

Dessutom kommer DSO genomföra utbildningsinsatser där det framkommit att enheterna har uppenbara kunskapsbrister i personuppgiftshantering och kraven som ställs på verksamheten. Slutligen så kommer DSO att behöva genomföra en kommunikationsinsats gällande den digitala utbildningen för att öka medvetenheten inom organisationen.

4. Registerförteckning

SLSO ska enligt artikel 30 föra ett register över de personuppgiftsbehandlingar som utförs under dess ansvar, en så kallad registerförteckning. För detta syfte har SLSO tidigare använt ett systemstöd vid namn Personuppgiftshantering (PUH). Registerverktyget PUH skulle ersättas av DraftIT, som är ett regiongemensamt systemstöd, under 2020 men på grund utav administrativa komplikationer så försenades införandet vilket gör att DraftIT införs först under 2022. Under tiden hanteras SLSO:s registerförteckning i Excel.

4.1 Bedömning

Personuppgiftsbehandlingar tillkommer och förändras ständigt. Det är därför viktigt att det inom SLSO finns en systematik för att löpande lägga in nya personuppgiftsbehandlingar i registerförteckningen samt för att se över och uppdatera de personuppgiftsbehandlingar som lagts in i registerförteckningen. Manuel hantering i Excel gör detta arbete tidskrävande och ineffektivt, behovet av ett systemstöd är således stort och systemstödet bedöms vara på plats under 2022.
DSO har under året noterat att det inom en centrumbildning funnits brister i att uppdatera sina personuppgiftshanteringar. Detta då ändamålen med den ursprungliga personuppgiftshantering fått ett nytt ändamål vilket inte resulterat i en ny anmälan till registret för personuppgiftshanteringar vilket är ett krav.

4.2 Åtgärd

Ett nytt användarvänligt systemstöd är en åtgärd för att fortsättningsvis kunna arbeta aktivt med registerförteckningen och se till att behandlingarna kontinuerligt ses över men även att nya läggs in. Systemet tar användaren genom processen steg för steg vid varje ny registrering och ställer relevanta frågor längs vägen, om bland annat syfte, gallringstider, överföringar, samtycke och särskilda kategorier av personuppgifter. Aktivitets- och påminnelsefunktioner i systemet hjälper till att spara tid och att hålla koll på viktiga behandlingar. Fördelar med ett systemstöd är att registerförteckningen hålls uppdaterad på ett snabbt och effektivt sätt.

I tillägg så behöver DSO genomföra en utbildningsinsats på den centrumbildning som brustit i sin bristande uppdatering av personuppgiftsbehandling i nämndens register.

5. Medborgares rättigheter

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade eller att få ut eller flytta sina uppgifter.

5.1 Bedömning

De förfrågningar som inkommit gällande exempelvis rätt till information, rätt till registerutdrag har kunnat tillgodoses tack vare etablerade rutiner.

DSO har hanterat ett antal förfrågningar under året och kan konstatera att det finns tekniska svårigheter att leverera ett komplett och strukturerat registerutdrag via ett it-stöd. 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.

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

Den övergripande anvisning för hantering av registerutdrag har uppdaterats.

6. Personuppgiftsincidenter

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

DSO:s bedömning är att antalet incidenter borde vara högre i en organisation av SLSO:s storlek och med stor sannolikhet uppdagas endast en bråkdel av incidenterna. Detta är en brist, dels för att det strider mot dataskyddsförordningen att inte dokumentera och rapportera incidenter, dels att det försvårar arbetet med att identifiera brister och arbeta förebyggande för att nya personuppgiftsincidenter inte ska inträffa.

Det låga antalet inrapporterade personuppgiftsincidenter beror troligen på bristande kunskap beträffande vad en personuppgiftsincident är och att rutinen för SLSO:s hantering av dessa inte är tillräckligt inarbetad.

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 hade 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”.

Under det gångna året inkom en visselblåsning som handlade om röjande av personuppgifter. DSO har varit delaktig i utredning. En anonym person gjorde DSO uppmärksam på att det fanns flera incidenter där personuppgifter röjts i samband med beställning och leverans av hjälpmedel. Dessa återkommande incidenter hade rapporterats i avvikelsesystemet Händelsevis men ej kommit till DSO:s kännedom och ej heller anmälts till tillsynsmyndigheten. Det kunde konstateras att flertalet av dessa incidenter berodde på systemfel. Incidenterna hade inte tillräckligt analyserats och systemfelet hade ej heller åtgärdats.

6.2 Åtgärd

Arbetet med att informera och synliggöra incidenter måste ske fortlöpande och bedömningen är att detta lämpligast görs via intranät och sedvanliga kommunikationskanaler.

SLSO:s övergripande anvisning för personuppgiftsincidenter har uppdaterats i syfte att påskynda processen att rapportera inom 72 timmar. Detta sker genom att ansvaret för incidentrapportering tillfaller

verksamheten där incidenten skett, inte DSO som tidigare var den som skötte rapporteringen.

Ett ytterligare förslag för att öka antalet rapporterade personuppgiftsincidenter är att uppmana verksamheterna att rapportera alla incidenter i avvikelsesystemet Händelsevis så att man använder sig av samma system som övriga avvikelser inrapporteras in i. Dessutom är rapportering av avvikelser ett inarbetat sätt att hantera händelser som haft en negativ utgång. DSO kommer fortlöpande begära utdrag ur Händelsevis för att upptäcka systemfel och för att medverka att få en lösning på dessa problem som har en gemensam teknisk nämnare.

7. Styrdokument

En grundläggande princip i dataskyddsförordningen 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 dataskyddsförordningen 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.

7.1 Bedömning

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

7.2 Åtgärd

Årlig översyn av riktlinjen 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 det fortsatt råder oklarheter rörande tolkning av både dataskyddsförordningen och avgörande i EU-domstolen som har bäring på SLSO:s hantering av personuppgifter.

Schrems II-målet fortsätter att påverka arbetet med personuppgifts-hanteringen. 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.

8.1 Bedömning

I omvärldsbevakningssyfte har DSO deltagit i nätverksträffar och utbildningar samt bevakat praxis och nyheter och informerat berörda när informationen varit relevant för dem.

8.2 Åtgärd

DSO fortsätter att hålla sig á jour för att arbeta proaktivt med personuppgiftshantering.

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. I vissa avseenden ser DSO allvarligt på att kunskapen inom vissa områden inte är högre än vad den borde vara trots upprepade förmaningar om de krav lagen ställer på personuppgiftshantering. Detta måste DSO fortsatt arbeta med och kommer eskalera dessa problemställningar om ingen förbättring sker under året 2022.

En gemensam metod för konsekvensbedömningar avseende dataskydd inom Region Stockholm blir en kvalitetssäkrande åtgärd vilket höjer kvaliteten på momentet.

Vidare kan DSO konstatera att förseningen av införandet av ett nytt registerverktyg har haft en negativ påverkan på personuppgiftshantering och detta kommer följas upp under året.

Slutligen kan DSO konstatera att Schrems II-domen fortsatt har en signifikant påverkan på SLSO:s personuppgiftshantering.

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

Stockholm, januari 2022

Camilla Heise Löwgren Dataskyddsombud	Henrik Strand Dataskyddsombud	Marcus Carlbrand Dataskyddsombud