Stockholms läns sjukvårdsområde
*Sjukvårdsdirektören*

ANMÄLAN
2021-03-22

SLSO 2021-0217

# Årsrapport GDPR för verksamhetsåret 2020

Årsrapport GDPR för verksamhetsåret 2020 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2021-03-24

SLSO 2021-0217

# Årsrapport GDPR

För verksamhetsåret 2020

## 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 ..... 3
3.2 Åtgärd ..... 4

4. Registerförteckning ..... 4
4.1 Bedömning ..... 4
4.2 Åtgärd ..... 5

5. Medborgares rättigheter ..... 5
5.1 Bedömning ..... 5
5.2 Åtgärd ..... 5

6. Personuppgiftsincidenter ..... 5
6.1 Bedömning ..... 6
6.2 Åtgärd ..... 6

7. Styrdokument ..... 6
7.1 Bedömning ..... 7
7.2 Åtgärd ..... 7

8. Omvärldsbevakning ..... 7
8.1 Bedömning ..... 7
8.2 Åtgärd ..... 8

9. Konklusion ..... 8

# 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 och personuppgiftshantering.

## 2.1 Bedömning

DSO upplever 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. Det arbetet påbörjades av SLSO:s informationssäkerhetssamordnare under 2020 men fick av förklarliga skäl stå tillbaka under pågående pandemi.

## 2.2 Åtgärd

DSO-funktionen stärks under 2021 med en ny jurist vilket förbättrar möjligheter till ett mer proaktivt arbete i frågor gällande dataskydd.

Givet en förhoppning att den ansträngda arbetssituationen under pågående covid-19 pandemi förbättras så behöver DSO driva på arbetet i skapandet av en dataskyddsorganisation tillsammans med SLSO:s informationssäkerhetssamordnare.

# 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.

## 3.1 Bedömning

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.

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.

Exempel på sådana situationer är:

- Initialt då frågan lyftes att SLSO skulle överta IT för den egenägda vården var DSO inte alls varit involverad i arbetet vilket anses vara anmärkningsvärt.
- Forskningsstudier med bristande följsamhet enligt artikel 35 där konsekvensbedömningar inte genomförts i tid vilket inneburit att både artikel 35 och 38 inte efterlevts. Noterbart är att denna bristande följsamhet vid forskningsstudier vid ett tillfälle lett till att en forskare inom SLSO blivit åtalsanmäld.

## 3.2 Åtgärd

I samråd med representanter från verksamhetsområdet FoUU har DSO gjort förenklingar av den mall som används vid konsekvensbedömningar som syftar till att det ska vara till hjälp för verksamheten i syftet att uppfylla och följa de krav som ställs på ansvariga för personuppgiftshanteringar.

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.

I SLSO:s fortsatta arbete med vårdstödjande IT-lösningar för den egenägda vården måste DSO involveras.

# 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 2021. 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.

## 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.

Samtliga enheter inom SLSO behöver årligen uppmanas att se över sina uppgifter om personuppgiftsbehandlingar och vid behov revidera dessa. DSO ansvarar för att påminna om behov av översyn och revidering samt att kontrollera vilka eventuella ändringar som görs av verksamheten.

# 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. Vid den förfrågning gällande rätten till radering som inkom hänvisades medborgaren till Inspektionen för vård och omsorg (IVO) för vidare behandling då journaluppgifter inte får raderas enbart med stöd av dataskyddsförordningen.

## 5.2 Åtgärd

Översyn av befintliga rutiner för att tillgodose de registrerades rättigheter görs kontinuerligt.

# 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 samt 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 låg kunskap beträffande vad en personuppgiftsincident är och att rutinen för SLSO:s hantering av dessa inte är tillräckligt inarbetad.

Majoriteten av inträffade personuppgiftsincidenter 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”.

## 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.

# 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 – riktlinje för SLSO
- Personuppgiftsincident – riktlinje SLSO
- E-postanvändning – övergripande anvisning för SLSO

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 Dokumenta/Platina.

### 7.1 Bedömning

Riktlinjen för personuppgiftshantering fastställdes 2019 och skulle behöva en översyn och eventuell revidering utifrån att det hänt mycket på dataskyddsområdet sedan 2019. Vidare skulle DSO behöva upprätta en rutin för att kontinuerligt se över befintliga styrdokument men även ta fram nya vid behov.

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

Översyn av riktlinjen för personuppgiftshantering och vidareutveckla dokument för ett strategiskt ställningstagande för SLSO:s dataskydd ingår i planen för innevarande år. 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.

Noterbara händelser under 2020 var framför allt IMY:s granskning av åtta vårdgivare däribland SLSO:s vårdgrannar Karolinska Universitetssjukhuset och Capio St:Göran gällande personalens åtkomst till journaluppgifter.

DSO vill även lyfta fram det faktum att den 16 juli 2020 meddelade EU-domstolen dom i det så kallade Schrems II-målet. 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.

Gällande IMY:s granskning i vårdsektorn ansågs bristerna vara så pass allvarliga att de utmynnade i sanktionsavgifter om 4 respektive 30 miljoner kronor för Karolinska respektive Capio S:t Görans sjukhus. DSO följer utvecklingen och aktiviteter som följer av granskningen och eventuella överklaganden.

Beträffande Schrems II-domen måste SLSO göra en inventering av alla sina avtal för att kontrollera att det inte överförs personuppgifter till USA utan rätt lagstöd. Överföringar som baserats på Privacy Shield måste avbrytas omedelbart.
IMY har inlett granskning av sex svenska företag efter Schrems II-domen: Sinovum Media, Modern Women Media, Coop Sverige, Dagens Industri, Tele2 och Cdons finska domän cdon.fi.

## 8.2 Åtgärd

DSO följer utveckling av vårdgivarna för att nå IMY:s beslut och arbetet med att kartlägga SLSO:s avtal är förlagt till portföljkontoret. Detta kommer följas upp under första halvåret 2021.

# 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 2021.

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 har en signifikant påverkan på SLSO:s personuppgiftshantering.

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

Stockholm, mars 2021

Camilla Heise Löwgren
Dataskyddsombud

Henrik Strand
Dataskyddsombud