Stockholms läns sjukvårdsområde
Närsjukvårdsdirektören

ANMÄLAN
2025-03-03

SLSO 2025-1059

Årsrapport GDPR för verksamhetsåret 2024

Årsrapport GDPR för verksamhetsåret 2024 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2025-02-25

Diarienummer
SLSO 2025-1059

Årsrapport GDPR

För verksamhetsåret 2024

Innehållsförteckning

Inledning 4

1. Dataskyddsombudets arbete 4
1.1 Bedömning av dataskyddsombudets resurser 4
1.2 Bedömning riskhantering 4
1.2.1 Åtgärd riskhantering 5
1.3 Mognadsmätningar 5
1.3.1 Åtgärd mognadsmätningar 6
1.4 Smittspårningsmodul 6
1.5 Diabetesmonitorering 6
1.5.1 Åtgärd diabetesmonitorering 6
1.6 VAL-databasen 7
1.6.1 Åtgärd VAL-databasen 7
1.7 IT-önskemål och behovsprocess 7
1.7.1 Åtgärd IT-önskemål och behovsprocess 7

2. Dataskyddsorganisation 8
2.1 Bedömning 8
2.2 Åtgärd dataskyddsorganisation 9

3. Registerförteckning 9
3.1 Bedömning 9
3.2 Åtgärd 9

4. Medborgares rättigheter 10
4.1 Bedömning 10
4.2 Åtgärd 10

5. Personuppgiftsincidenter 11
5.1 Bedömning av personuppgiftsincidenter 11
5.2 Åtgärder av personuppgiftsincidenter 12
5.3 Personuppgifter på extern lagringsyta 12

6. Styrdokument 12
6.1 Bedömning 13
6.2 Åtgärd 13

7. Omvärldsbevakning 14
7.1 Bedömning AI-förordningen 14
7.1.1 Åtgärd AI-förordningen 15

8. Konklusion 15

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 sammanfattar dataskyddsombudens iakttagelser och arbete under det gångna året.

1. Dataskyddsombudets arbete

Enligt art. 39 ska Dataskyddsombudet övervaka och ge råd till den personuppgiftsansvarige så att kraven i GDPR uppfylls. Detta kan ske genom information och utbildning till 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.

1.1 Bedömning av dataskyddsombudets resurser

I teorin består funktionen av två tjänstemän som delar sitt uppdrag som DSO med uppdrag som hälso- och sjukvårdsjuridik och informationssäkerhet. Detta innebär i praktiken att funktionen i dagsläget inte är en fulltidstjänst.

Eftersom funktionen är tillsatt med nuvarande resurser innebär det även att DSO arbetar i praktiken som integritetshandläggare. Funktionen som DSO ska vara opartisk vilket är svårt att upprätthålla då DSO i mångt och mycket gör bedömningar av sitt eget arbete.

1.2 Bedömning riskhantering

Dataskyddsombudet kan konstatera att flertalet verksamheter gjort framsteg i sin förståelse och kunskap om dataskyddsarbetet. Detta är särskilt tydligt i samband med konsekvensbedömningar avseende dataskydd, där DSO i sin granskande roll observerar att material som lämnas in håller allt högre kvalitet.

Trots dessa framsteg kvarstår dock utmaningar inom framför allt riskhanteringen där bedömningen är att det finns brister i både förståelse av konceptet riskhantering och dess genomförande. Riskhantering är en central och systematisk process som innefattar flera steg: identifiering, analys, utvärdering och uppföljning av potentiella risker kopplade till behandling av personuppgifter. Varje steg är avgörande för att skapa en helhetsbild av de

utmaningar som verksamheten står inför och för att säkerställa efterlevnad av GDPR och andra tillämpliga regelverk. Genom att etablera en tydlig process och ansvarsfördelning kan SLSO skapa förutsättningar för ett systematiskt och proaktivt arbetssätt inom dataskyddsområdet. Bedömningen är att det finns svårigheter att genomföra detta systematiska arbete när det inte finns ett systemstöd för riskhantering. Excelfiler och användandet av andra typer av mallar för riskbedömningar riskerar till mångt och mycket att bli pappersprodukter utan ordentlig uppföljning över tid.

1.2.1 Åtgärd riskhantering

Utmaningarna inom riskhanteringen behöver hanteras och ett första steg sker i samband med att Region Stockholm upphandlar ett nytt systemstöd för arbetet inom dataskydd, informationssäkerhet och verksamhetsbaserad informationssredovisning (VIR). Systemstödet ska kunna hantera området för riskhantering, det ska således vara möjligt att genomföra riskanalyser som kan följas upp över tid, ha riskmatris som kan anpassas och finnas i olika versioner beroende på användningsområde samt möjligheten att koppla risker till person (riskägare). Det är av vikt att tidsperspektivet och kopplingen mellan riskägare och risk kan göras i ett IT-stöd i den mening att riskhanteringen inte ska vara en ”pappersprodukt” vilken inte medger någon automatisk uppdatering vid exempelvis avslut av anställning eller angivet tidsperspektiv på åtgärder.

Det kan även tänkas att DSO kan skriva stödjande dokument om området inkluderat till exempel förslag på vanligt förekommande risker inom området. Förhoppningen med en sådan lista eller dokument är att starta och nyansera riskhanteringen. Risken med ett sådant dokument är att dessa förformulerade risker endast klipps in i en riskanalys utan någon signifikant eftertanke.

1.3 Mognadsmätningar

Vidare betonar DSO vikten av att införa ett verktyg eller ett strukturerat arbetssätt för en regelbunden och effektiv utvärdering av dataskyddsarbetet. I dagsläget saknas sådana hjälpmedel vilket gör det svårt att systematiskt och konsekvent bedöma hur väl dataskyddsarbetet fungerar och identifiera områden som behöver förbättras.

Ett sådant hjälpmedel skulle inte bara ge DSO en mer omfattande och djupgående överblick över styrkor och svagheter i det nuvarande dataskyddsarbetet, utan också utgöra en värdefull grund för att analysera och identifiera specifika förbättringsområden. Genom att använda denna metod skulle DSO kunna prioritera insatser och resurser på ett mer strategiskt sätt, vilket i sin tur skulle bidra till att stärka verksamhetens förmåga att hantera personuppgifter i enlighet med både interna riktlinjer och externa regelverk. Detta skulle leda till ett mer proaktivt än reaktivt arbetssätt.

1.3.1 Åtgärd mognadsmätningar

Ett inledande samtal förs mellan Region Stockholms DSO:er för möjligheten att införskaffa alternativt själv skapa ett stöd för mognadsmätningar.

1.4 Smittspårningsmodul

Arbetet med att utveckla en digital smittspårningsmodul har fortsatt under 2024 och smittspårningsmodulen befinner sig nu i en utvecklings- och pilotfas. Denna smittskyddsmodul är frikopplad från de övriga delarna i Alltid öppet, för att kunna dokumentera smittspårningsarbete som bedrivs inom primärvården.

Smittspårning är inte journalföring utan sker för att kunna redogöra över handläggningsprocessen av smittspårningen. Därför är det viktigt att inte blanda ihop den delen av Alltid öppet med smittskyddsdokumentationen.

DSO deltar i utvecklingsarbetet när frågor gällande personuppgiftshanteringen uppkommer och uppfattar att projektdeltagarna har en förståelse för vikten av integritetsskydd och att tänka riskbaserat i utvecklingen.

1.5 Diabetesmonitorering

Under 2023 inledde DSO en konsekvensbedömning tillsammans med regionledningskontoret (RLK) för bedömningen av ett digitalt verktyg som tagits fram av ett amerikanskt bolag som möjliggör för diabetessjuksköterskor och läkare att följa patienternas blodsockervärden i realtid.

Applikationen samlar in patientdata och dessa känsliga personuppgifter hanteras i en molntjänst i servrar som är geografiskt lokaliserade utanför EU/EES. Den geografiska positionen medför en så kallad tredjelandsöverföring och är därmed inte förenlig med offentlighet- och sekretesslagen då patientuppgifter kan anses vara röjda. I samband med arbetet av konsekvensbedömningen konstaterade arbetsgruppen att det är väldigt komplicerat att konstatera vem som är personuppgiftsansvarig för hanteringen av patientuppgifter och någon slutsats i frågan gällande personuppgiftsansvar kunde således inte fastställas. Det något oklara rättsläget bekräftas även av Sveriges Kommuner och Regioner (SKR) i deras laglighetsbedömning[1].

1.5.1 Åtgärd diabetesmonitorering

DSO gjorde en formell framställan till RLK om hjälp för att ta fram säkerhetsanvisningar för att vården ska kunna använda verktyget – det arbetet pågår alltjämt och DSO hoppas att ärendet kan avslutas under 2025.

[1] Promemoria - Laglighetsprövning av FreeStyle Libre CGM-system med avseende på dataskydd och annat integritetsskydd 2022-03-31.

1.6 VAL-databasen

Både DSO från SLSO, Hälso- och sjukvårdsnämnden (HSN) samt Primärvårdsnämnden (PVN) har konstaterat att det finns utmaningar när det gäller tillgången och användningen av data som hämtas från VAL-databasen. Personuppgiftsbehandlingen sker främst inom SLSO:s centrumbildningar och utmaningarna gäller framför allt ansvarsförhållandet av data och uppdragsbeskrivningar som i vissa fall är för ospecifika gällande personuppgiftshanteringen.

Den gemensamma bedömningen är att det behöver tillkomma bättre organisatoriska rutiner inom både HSF och SLSO för att komma till rätta med dessa utmaningar.

1.6.1 Åtgärd VAL-databasen

Gällande VAL-databasen och dess utmaningar så har DSO sammankallat medarbetare från både Hälso- och sjukvårdsförvaltningen (HSF) och SLSO för ett initialt möte i januari där konsensus kunde etableras kring problematik och åtgärder. Nya möten är inbokad och arbetet med åtgärder har således påbörjats.

1.7 IT-önskemål och behovsprocess

En återkommande frågeställning och utmaning som ofta uppstår i samband med nya personuppgiftsbehandlingar infinner sig när verksamheterna önskar köpa in nya (ofta) molntjänstbaserade IT-lösningar. Verksamheternas önskemål avhandlas i IT- säkerhetsforum där SLSO:s IT-chef är sammankallande.

Bedömningsprocessen av nya inköp och/eller upphandling har under 2024 förfinats men det återstår alltjämt utmaningar med att säkerställa att det ställs adekvata krav på skydd av den personliga integriteten i samtliga inköp och upphandlingar som görs av SLSO.

Utan en robust och genomtänkt inköps- och upphandlingsprocess avseende kravställning så finns det risker att det inte ställs några krav på informationssäkerhet eller följsamhet gentemot GDPR när verksamheterna får en godkänd inköpsansökan från upphandlingsenheten. DSO märker av detta i samband med att personuppgiftsbiträdesavtal ska skrivas och det vid kontrollfrågor angående skyddsåtgärder inte finns några initierade svar alternativt att det inte gjorts någon kravställan avseende varken informationssäkerhet eller dataskydd. En otillräcklig kravställning försvårar märkbart SLSO:s förmåga att skydda den personliga integriteten.

1.7.1 Åtgärd IT-önskemål och behovsprocess

SLSO har under andra halvan av 2024 startat ett omfattande IT-säkerhetsprojekt där informationssäkerhetssamordnare tillika dataskyddsombud ingår i projekt- och styrgrupp. Projektet avser att stärka

IT- och informationssäkerhet genom hela livscykelprocessen vilket innebär att genomlysa:

- Styrning IT-tjänst
- Process IT-tjänst
- Förvaltning IT-tjänst

IT-säkerhetsprojektet kommer således adressera frågan om en utvecklad och förbättrad process för att hantera ett IT-stöd från dess att behovet uppstår till en eventuell avveckling av detsamma. Utmaningar med kravställning och skyddsåtgärder i IT-stöd kommer då hanteras effektivare framöver.

2. Dataskyddsorganisation

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 bland annat säkerställa ordning och reda när det gäller dataskydd, personuppgiftshantering och informationssäkerhet

2.1 Bedömning

För att effektivt kunna bedriva ett dataskyddsarbete inom en sådan stor förvaltning som SLSO vore det rimligt att det finns ett nätverk av personer som kan tjäna som kontaktpunkter ute i verksamheterna. Inom ramen för denna dataskyddsorganisation kallas dessa personer för koordinatorer.

Under 2023 startade DSO ett nätverk där representanter ifrån verksamhetsstöd ingår samt kärnverksamhet i form av habilitering. Nätverket har haft fyra sammankomster årligen sedan 2023 och tanken har till början varit att arbeta enligt MSB:s metodstöd för informationssäkerhet. Denna tanke reviderades under 2024 på grund av bland annat tidsbrist och oklar arbetsinsats när det gäller metodstödet. I stället har metodstödet ersatts av stående agendapunkter så som omvärldsbevakning, nytt inom dataskydd och informationssäkerhet samt egna inspel från deltagare.

Bedömningen av årets arbete är att DSO inte till fyllest lyckats vara tydliga i syftet med nätverket och därigenom har de operativa insatserna till stor del uteblivit. Årets avslutande möte fokuserade på frågan kring syfte med nätverket och vad som kunde tänkas begäras av deltagarna. Då kunde gruppen nå samsyn om att eventuella insatser ska bestämmas under 2025 års första möte.

Till dags dato har inte DSO lyckats införliva mer utav kärnverksamheten i nätverket på grund av bland annat primärvårdens och psykiatrins geografiska spridning och storlek på verksamheterna. Bedömningen är att det kommer fortsätta vara en utmaning framöver där DSO inte har någon omedelbar lösning att tillgå.

2.2 Åtgärd dataskyddsorganisation

På deltagarnas uppmaning ska DSO under 2025 vara tydligare i vad det är DSO vill få ut av nätverket. Den initiala tanken är då att nätverket tillsammans ska bli bättre på att tillsammans följa upp genomförandet av obligatoriska utbildningar.

Ytterligare aktivitet som kommit från en deltagare i nätverket är att sända ut ett FAQ-liknande material till SLSO:s verksamhetschefer som kan användas vid exempelvis APT:er i syfte att öka kunskapen kring hantering av information.

3. Registerförteckning

SLSO ska enligt artikel 30 föra ett register över de personuppgiftsbehandlingar som utförs under dess ansvar, en så kallad registerförteckning.

3.1 Bedömning

Personuppgiftsbehandlingar tillkommer och förändras ständigt. Genom den digitala plattformen Draftit så har en avlastning skett för DSO då huvudansvaret för själva anmälningarna läggs på registeransvarig ute i verksamheterna, till exempel så anmäler en forskare sin personuppgiftsbehandling i Drafit vilket sedan granskas av DSO.

Arbetssätten kopplat till Drafit har inom SLSO och förmodligen inom Region Stockholm inte varit så utvecklat som önskat då det inte är integrerat med områdena för informationssäkerhet och informationshantering. I verktyget är det inte heller möjligt att göra till exempel konsekvensbedömningar vilket tillsammans med sitt isolerande tillstånd från angränsande verksamhetsområde gjort verktyget något ineffektivt. Av den anledningen så har DSO tillsammans med en arbetsgrupp från RLK, Regionarkivet och Trafikförvaltningen, sonderat marknaden i ett försök att hitta ett systemstöd som inte bara hantera art. 30 register utan även ett systemstöd som täcker och väver in informationssäkerhet, dataskydd och informationshantering (VIR). Förhoppningen är att ett integrerat systemstöd där mångt fler aktiviteter utförs ska utveckla och förbättra dataskyddsarbetet.

3.2 Åtgärd

Upphandlingen av ett nytt mer omfattande IT-stöd som kommer vara till gagn för funktionerna inom dataskydd, informationssäkerhet och VIR startade 2024 och utvärderingen av anbud slutförs under januari-februari 2025, tilldelningen skedde i februari. Införandet sker successivt med start 2025.

4. 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.

4.1 Bedömning

DSO konstaterar att det finns svårigheter att leverera ett registerutdrag enligt art. 15 via exempelvis 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 till en registrerad.

Sedan början av förra året finns det ett enhetligt tillvägagångssätt för alla vårdgivare inom Region Stockholm för framtagande av så kallade logglistor. Dessa listor redogör behörig eller icke behörig åtkomst till journaluppgifter. De uppdaterade dokumenten som nu ska användas av alla vårdgivare i samband med uttag av logglistor, bygger till stor del på SLSO:s tidigare versioner. DSO har i samband med utlämning av dessa så kallade logglistor noterat att fler och fler verksamhetsrepresentanter kontaktar DSO för praktisk handläggning av utlämnandet av logglistorna.

4.2 Åtgärd

DSO kommer fortsättningsvis skicka tillbaka förfrågningar om utdrag av logglistor från verksamhetsrepresentanter om utdrag av logglistor då det är en uppgift som verksamheterna ska hantera själva.

5. Personuppgiftsincidenter

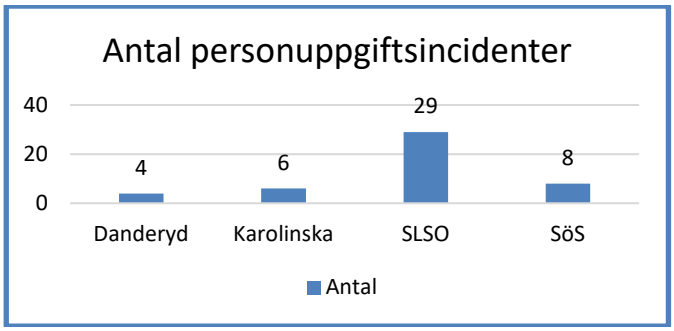
En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt hanterats. En incident ska utan onödigt dröjsmål och, om så är möjligt anmälas till IMY inom 72 timmar efter att verksamheten fått vetskap om den.

5.1 Bedömning av personuppgiftsincidenter

Givet SLSO:s storlek och mängden personuppgifter som hanteras inom vårdgivaren så är DSO av uppfattningen att antalet anmälda personuppgiftsincidenter är fortsatt lågt. För 2024 så anmäldes 29 personuppgiftsincidenter där 83 % av incidenterna berodde på den mänskliga faktorn. Bakom hälften av de incidenter som orsakas av den mänskliga faktorn ligger någon form av felskick, alltså felskickade brev, mejl eller sms.

Beträffande antalet incidenter så är det viktigt att påpeka att det inte nödvändigtvis behöver vara en indikation på bristande säkerhet att en organisation anmäler många personuppgiftsincidenter. Tvärtom kan det ofta tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter. På motsvarande sätt behöver det inte vara en signal om en hög grad av informationssäkerhet när ett område rapporterar få personuppgiftsincidenter. Det kan exempelvis handla om att verksamheter inte rapporterar anmälningspliktiga personuppgiftsincidenter av rädsla för att bli föremål för IMY:s tillsynsverksamhet och eventuella sanktionsavgifter[2].

I samband med bedömningen av antalet incidenter så kontrollerade DSO hur många personuppgiftsincidenter som anmäldes av vårdgrannarna Danderyds Sjukhus, Karolinska Universitetssjukhuset och Södersjukhuset.



I jämförelsen så är det tydligt att antalet anmälda incidenter är högt inom SLSO. DSO tolkar detta som att vårdgrannarna har en ovanligt låg nivå av

[2] https://www.imy.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2022.pdf s.14. Hämtad 2025-02-10

incidenter. Orsaken varför det ser ut på detta sätt kan inte SLSO bedöma, men DSO ser det som positivt att man anmäler incidenter inom SLSO:s verksamheter.

För SLSO:s räkning är antalet inrapporterade incidenter fortfarande lågt med tanke på verksamhetens storlek. 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.

5.2 Åtgärder av personuppgiftsincidenter

DSO har genomfört särskilda informationsinsatser till primärvårdens verksamhetschefer och medicinska sekreterare för att informera om vad som utgör en personuppgiftsincident samt vikten av att göra incidentanmälan till IMY då även underlåtenhet att rapporteraincidenter kan medföra sanktionsavgifter.

Fortsatt informationsspridning sker via intranät, dataskyddsnätverket samt via den så kallade BAS-utbildningen för nya chefer, detta för att bibehålla och öka medvetenhet kring personuppgiftsincidenter och reglerna i GDPR.

5.3 Personuppgifter på extern lagringsyta

I slutet av maj fick SLSO vetskap om att en anställd använt sig av behörigheter från före detta anställda på ett felaktigt sätt. Man fann då också att personuppgifter hade lagrats på den anställdes på Dropboxkonto i strid mot gällande riktlinjer. Tusentals patientuppgifter som tagits fram i samband med förfrågningar för kvalitetsuppföljning och forskning hade lagrats på denna externa lagringsplats utan att SLSO kunde ställa villkor för säker hantering av patientuppgifterna. Anmälning till IMY gjordes omgående och en polisutredning inledes. Ur ett juridiskt perspektiv så fanns det incitament för att uppgifterna kunde anses vara röjda då uppgifterna fanns i en amerikansk molntjänst med risk för att supportpersonalen på Dropbox hade tillgång till uppgifterna. Alla uppgifter som fanns på Dropbox är numera borttagna. Allmänheten informerades via SLSO:s externa hemsida och Alltid öppet om incidenten. Det har också funnits möjlighet för medborgare att höra av sig huruvida uppgifter om en själv fanns på den externa lagringsytan. Rutinerna för behörighetstilldelningen har stramats åt. Polisutredningen är numera nedlagd. Huruvida IMY tänker inleda tillsyn är inte känd.

6. 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.

6.1 Bedömning

Det finns varken inom Region Stockholm eller SLSO någon riktlinje avseende dataskydd vilket även har påpekats av revisorer i samband med en granskning av Karolinska Universitetssjukhuset[3]. DSO håller med revisorernas kritik mot avsaknaden av en riktlinje för dataskyddsarbetet.

I dagsläget sker kommunikation via intranätet och inom dataskyddsorganisationen 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. Under det gånga året har DSO fått återkoppling från dataskyddsnätverket avseende styrdokumenten som kommer att tillvaratas inför den årliga uppdateringen.

6.2 Åtgärd

Arbetet med riktlinjer för dataskydd inom Region Stockholm drivs av RLK och påbörjas i första kvartalet 2025. I stället för ytterligare en riktlinje så är tanken att arbetet för dataskydd ska inkluderas i Riktlinjen för informationssäkerhet[4]. Ett första utkast på uppdaterad riktlinje där dataskydd ingår i riktlinjen för informationssäkerhet förväntas gå på remiss 1/5–2025.

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.

---

[3] Regionrevisorerna, Projektrapport 1/2024 Systematiskt arbete med informationssäkerhet och dataskydd på Karolinska universitetssjukhuset, dnr RK 2023–0108

[4] Riktlinjer för informationssäkerhet, dnr 2020–0148

7. 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.

7.1 Bedömning AI-förordningen

SLSO står inför behovet av att anpassa sig till den snabba tekniska utvecklingen, särskilt inom området artificiell intelligens (AI). Medan AI erbjuder nya möjligheter, innebär det också uppkomsten av nya hot och sårbarheter som måste hanteras proaktivt och sammanhängande från behov till driftsättning.

Förordningen trädde i kraft den 1 augusti 2024 men merparten av bestämmelser ska börja tillämpas 24 månader efter ikraftträdandet, det vill säga den 1 augusti 2026.

Reglerna i AI-förordningen börjar gälla vid olika tidpunkter.

- 2 februari 2025 reglerna om oacceptabel risk (förbjuden AI).
- 2 augusti 2025 reglerna om AI-modeller för allmänna ändamål.
- 2 augusti 2026 samtliga regler börjar gälla (med vissa undantag).

Som kompletterande lagstiftning till GDPR reglerar AI-förordningen hur AI-system får användas, särskilt när de hanterar personuppgifter. Redan befintliga krav inom personuppgiftshantering stramas åt och det är viktigt att SLSO i sin användning av AI följer GDPR:s principer om laglighet, transparens och dataminimering. Det är också viktigt att SLSO som användare av AI kan säkerställa att systemen är rättvisa, pålitliga och förklarliga, vilket stärker individens rättigheter enligt GDPR.

Bedömningen är att verksamheter som avser att använda generativ AI behöver se till att användningen är förenlig med GDPR och kompletterande lagstiftning. Frågor som då behöver besvaras är bland annat följande.

- Är användningen förenlig med de grundläggande dataskyddsrättsliga principerna?
- Vem är personuppgiftsansvarig? Finns det personuppgiftsbiträden?
- Finns det rättslig grund och annat rättsligt stöd för behandlingen av personuppgifter?
- Sker det automatiserat beslutsfattande eller överföring av personuppgifter till tredje land vid användningen och finns i så fall förutsättningar för det?
- Hur ska enskildas rättigheter tillgodoses vid användningen?
- Hur ska lämplig säkerhet uppnås vid användningen?

- Vilka risker från ett dataskyddsperspektiv medför användningen av generativ AI? Vilka åtgärder kan vidtas för att begränsa riskerna[5]?

Projektet ”Ett sammanhållet och strategiskt arbete kring data och artificiell intelligens” drivs som en nyckelaktivitet inom RLK, Strategisk IT och genomförs regionövergripande. Bedömningen är att projektet har syfte och mål som väl överensstämmer med de behov DSO ser inom SLSO gällande frågor kopplat till AI.

Myndigheten för digital förvaltning (DIGG) har tillsammans med IMY tagit fram riktlinjer och förslag på arbetssätt för generativ AI inom den offentliga förvaltningen. Platsen (en hemsida) är för de som vill förstå hur AI kan skapa samhällsnytta – och hur en offentlig organisation går tillväga för att börja använda AI. Webbplatsens innehåll är till nytta de som arbetar med verksamhetsutveckling, digitalisering och innovation, vill öka kunskap eller stilla sin nyfikenhet om AI inom offentlig förvaltning.

7.1.1 Åtgärd AI-förordningen

I enlighet med Region Stockholms rekommendationer så rekommenderas följande åtgärder.

- Inventera om AI-system används i verksamheten utifrån den definition som finns i AI-förordningen.
- Fastställ vilken risknivå som systemet tillhör. Om ett AI-system tillhör kategorin förbjuden AI ska systemet inte användas efter den 2 februari 2025.
- Fastställ om Region Stockholm/SLSO intar rollen som leverantör eller användare av AI-system.
- Identifiera och implementera nödvändiga åtgärder baserat på risknivå och roll[6].

DSO kommer fortsatt att kontrollera så att SLSO har de processer och rutiner på plats som behövs för att säkerställa de grundläggande bestämmelserna i GDPR när det gäller AI. Det regionövergripande projektet kommer även att bevakas för att dra lärdomar och insikter.

8. Konklusion

Med ökad användning av AI ställs SLSO inför nya utmaningar som kan förenkla och effektivisera arbete inom såväl administration som inom hälso- och sjukvården men det får inte ske på bekostnad av den personliga integriteten i sambandet med framtagande eller användningen av AI-applikationen. SLSO kan vara en leverantör när medarbetare tar fram en AI applikation via forskning eller innovation, men framför allt användare av AI-applikationer vilket i båda fall leder till att krav enligt nya AI-förordningen måste tillgodoses, vilket har nämnts tidigare. Såväl DSO, som

[5] https://www.digg.se/ai-for-offentlig-forvaltning/riktlinjer-for-generativ-ai/beakta-dataskyddsregelverket-som-utgangspunkt Hämtad: 2025-02-11
[6] vagledning-om-ai-forordningen.pdf Hämtad: 2025-02-11

handläggare på digitala tjänster följer det regionövergripande AI-projektet men det är i dagsläget oklart vilka rutiner som ska gälla för SLSO:s verksamhet och vem som har ansvaret att utreda och säkerställa följsamheten av AI-förordningen.

Det saknas dock förutsättningar för att bedriva ett systematiskt och fungerande dataskyddsarbete som exempelvis revision av verksamheternas dataskyddsarbete för SLSO:s vidkommande på grund av organisationens komplexitet och brister på resurser.

I dagsläget bedrivs GDPR-arbetet genom två halvtidstjänster i en organisation om ca 12 000 anställda. Under det gångna året har en av DSO:erna varit tvungen att arbeta mindre med övergripande dataskyddsfrågor för att lägga ökad fokus på granskning av forskningsprojekt som ökar stort inom SLSO. Detta medför att möjligheterna minskar ytterligare att bedriva ett arbete med ständiga förbättringar som medför ett lärande för verksamheterna.

Komplexitet av regelverket, ny tillkommen praxis och den tekniska utvecklingen ökar i snabb takt. Konsekvensen av detta blir att DSO:s arbete består i att hantera akuta ärenden vilket är otillfredsställande och leder till att det inte finns tid för uppföljnings- och granskningsverksamhet som DSO ska göra. Med de förutsättningar som råder idag är DSO mer än integritetshandläggare än en oberoende granskande funktion.

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

Stockholm, februari 2025

Camilla Heise Löwgren
Dataskyddsombud

Henrik Strand
Dataskyddsombud