Stockholms läns sjukvårdsområde
Närsjukvårdsdirektören

ANMÄLAN
2026-03-05

SLSO 2026-1190

Årsrapport GDPR för verksamhetsåret 2025

Årsrapport GDPR för verksamhetsåret 2025 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2026-03-06

Diarienummer
SLSO 2026-1190

Årsrapport GDPR

För verksamhetsåret 2025

Innehållsförteckning

Inledning 3

1. Dataskyddsombudets arbete 3
1.1 Bedömning av dataskyddsombudets resurser 3
1.2 Bedömning riskhantering 3
1.2.1 Åtgärd riskhantering 4
1.3 Princess 4
1.3.1 Åtgärd Princess 4
1.4 Smittspårningsmodul 5
1.5 Läkemedelsbolag kräver PUB-avtal 5
1.5.1 Åtgärd 5
1.6 VAL-databasen 5
1.6.1 Åtgärd VAL-databasen 6
1.7 IT-önskemål och behovsprocess 6
1.7.1 Åtgärd IT-önskemål och behovsprocess 6

2. Dataskyddsorganisation 7
2.1 Bedömning 7
2.2 Åtgärd dataskyddsorganisation 7

3. Registerförteckning 7
3.1 Bedömning 7
3.2 Åtgärd 8

4. Medborgares rättigheter 8
4.1 Bedömning 8

5. Personuppgiftsincidenter 8
5.1 Bedömning av personuppgiftsincidenter 9
5.2 Åtgärder av personuppgiftsincidenter 10

6. Styrdokument 10
6.1 Ny regionövergripande riktlinje 11

7. Omvärldsbevakning 11
7.1 Bedömning AI-förordningen 11
7.2 ”Omnibus- förordningen” 12

8. Konklusion 12

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

Funktionen består av två tjänstemän som delar sitt uppdrag som DSO med uppdrag som hälso- och sjukvårdsjuridik och informationssäkerhet. Det kan vara en trång sektor med tanke på organisationens storlek och mängd av personuppgiftsbehandling.

DSO arbetar i praktiken som integritetsskyddshandläggare och då funktionen som DSO ska vara opartisk kan det vara 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 anmälan av personuppgiftsincidenter där det är tydligt att verksamheterna inom vården förstår vad som utgör en incident och också anmäler den

Trots dessa framsteg kvarstår dock utmaningar inom framför allt riskhanteringen som görs i samband med konsekvensbedömningar. I en riskanalys kartläggs vilka risker som finns i samband med hanteringen av känsliga personuppgifter. Detta är särskilt viktig när patientuppgifter hanteras.

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.

1.2.1 Åtgärd riskhantering

Det nya registerverktyget IRIS kan förhoppningsvis utgöra ett verktyg framgent för att förenkla arbetet med riskanalyser. Det är dock ännu svårt att avgöra på vilket sätt med tanke på att Informationssäkerhet och verksamhetsbaserad informationsredovisning (VIR) också kommer att inkorporeras i samma system under våren 2026, dock i separata delar utan korrelation till GDPR-delen.

1.3 Princess

Från och med 1 januari 2026 tillhör Sjukvårdsrådgivning per telefon SLSO. Sjukvårdsrådgivningen har tidigare utförts av MedHelp Sjukvårdsrådgivning AB (MedHelp) på uppdrag av Region Stockholm.

Inför övergången från MedHelp till SLSO så har ett beslut tagits fram som undertecknats av närsjukvårdsdirektören om att ta över MedHelp:s egenutvecklade IT-applikation Princess. Som villkor inför övertagande av IT-applikationen ställdes bland annat att en risk- och konsekvensanalys utifrån dataskydd skulle genomföras.

Denna analys genomfördes under hösten 2025. I analysgruppen fanns företrädare för MedHelp, SLSO:s DSO, medarbetare från verksamhetsstöd Digitala tjänster, SLSO:s informationssäkerhetssamordnare och SLSO:s arkivarie. Mycket information som framkom i konsekvensanalysen kunde även återanvändas när samrådet med Regionarkivet skulle tas fram. Ändamålet med personuppgiftshanteringen som sker i Princess är att dokumentera handläggningen av sjukvårdsrådgivning per telefon. Princess anses vara ett ärendehandläggningssystem med koppling till journalsystemet Take Care. Som sammanfattning av konsekvensanalysen kan nämnas att personuppgiftshanteringen har rättslig grund då den sker som en rättslig förpliktelse enligt patientdatalagen då bedömningar och råd som ges inom hälso- och sjukvården ska dokumenteras. Dock har det varit svårt att kartlägga informationssäkerheten kring ärendehanteringsdelen.

1.3.1 Åtgärd Princess

DSO har gett rekommendationen att inventera objektsförvaltning och support av Princess för eventuell flytt till Region Stockholm för att få bättre kontroll över informationssäkerheten och avtal. Det är viktigt att få följsamhet till Region Stockholms regler och avtal.

1.4 Smittspårningsmodul

Arbetet med att utveckla en digital smittspårningsmodul har fortsatt under hela 2025 och fortsätter även under 2026. Smittspårning avseende sexuellt överförbara sjukdomar har redan införlivats i reguljär vårdverksamhet. För närvarande pågår en pilot för smittspårning av hepatit.

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 som rör hälso- och sjukvård med smittskyddsdokumentationen.

DSO fortsätter att delta 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 Läkemedelsbolag kräver PUB-avtal

Under våren 2025 kontaktades DSO av en verksamhetschef inom SLSO där denne fått en uppmaning av ett läkemedelsbolag att skriva på ett PUB-avtal. Läkemedelsbolaget har upphandlats centralt med villkor att läkemedelsbolaget tillhandahåller blodprovstester för att upptäckta allvarliga biverkningar som ett specifikt läkemedel kan ge vid användning av detsamma.
Bolaget hade gett ett laboratorium i Rumänien i uppdrag att dels ta fram en IT-applikation för att dokumentera handläggningen av blodprovssvaren och att genomföra själva analysen. Enligt svensk rätt anses laboratorier som självständiga personuppgiftsansvariga. Läkemedelsbolaget själv ansåg sig som ett personuppgiftsbiträde och krävde att SLSO och andra vårdgivare inom Region Stockholm som förskriver detta specifika läkemedel skulle ta ansvar för hela personuppgiftshanteringsfrågan.

1.5.1 Åtgärd

Ärendet ledde till att DSO kontaktade andra regiondrivna vårdgivares DSO:er som samarbetade i kontakten med Läkemedelsbolaget och bolagets advokater. Även upphandlande enheter har kontaktats för att uppmärksamma dem om händelsen. SLSO har i skrivande stund inte skrivit på något biträdesavtal med läkemedelsbolaget.

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 hälso- och sjukvårdsförvaltningen (HSF) och SLSO för att komma till rätta med dessa utmaningar.

1.6.1 Åtgärd VAL-databasen

Nya möten är inbokade och arbetet fortsätter även under 2026 för att sätta upp regler och rutiner sinsemellan förvaltningar för att säkerställa att hanteringen av personuppgifter från VAL hanteras i enligt med GDPR. HSF är sammankallande.

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 molntjänstbaserade IT-lösningar. Verksamheternas önskemål avhandlas i IT- säkerhetsforum där SLSO:s IT-direktör 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 vare sig informationssäkerhet eller dataskydd. En otillräcklig kravställning försvårar märkbart SLSO:s förmåga att skydda den personliga integriteten.

1.7.1 Åtgärd IT-önskemål och behovsprocess

IT-säkerhetsprojektet som startades av SLSO under 2024 har under 2025 fortgått med informationssäkerhetssamordnaren tillika dataskyddsombud i projektgruppen. Projektet som syftar till att stärka IT och Informationssäkerhetsarbetet genom att skapa tydliga processer för införande, förvaltning och avveckling av IT-tjänster och system börjar nu implementeras enligt plan.

Projektet har även resulterat i att flera tidigare okända IT-system identifierats. Dessa kommer löpande att inventeras, kvalitetssäkras och integreras i den fortsatta förvaltningen.

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.

Nätverket där representanter ifrån verksamhetsstöd samt verksamhetsområde Hjälpmedel ingår, har haft möten både under vår och höstterminen 2025. I stället för MSB:s metodstöd som tidigare använts för att ge ett slags ramverk för koordinatörsnätverket har detta ersatts av stående agendapunkter så som omvärldsbevakning, nytt inom dataskydd och informationssäkerhet samt egna inspel från deltagare.

Det gångna året har APT-material kring GDPR och informationssäkerhet tagits fram tillsammans med några koordinatorer från nätverket där tanken är att chefer uti verksamheterna ska presentera detta material för sina anställda på APT.

2.2 Åtgärd dataskyddsorganisation

DSO arbetar under kommande år med att få med representanter från verksamhetsområde Psykiatri och Habilitering till koordinatorsnätverket.

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. Den gågna hösten har den digitala plattformen Draftit ersatts med en ny digital plattform som kallas för IRIS. Denna är centralt upphandlad. De personuppgiftsregistreringar som fanns i Draftit har flyttats över till nya IRIS.

Förhoppningen är att det nya systemet IRIS ska ge synergieffekter då samma system även ska användas inom informationshantering och informationssäkerhet, men alla delar har ännu inte tagits i bruk.

3.2 Åtgärd

DSO kommer att följa upp huruvida dessa önskade synergieffekter uppnås då informationshantering, dataskydd och informationshantering har nära kopplingar med varandra och ett integrerat arbetssätt är mycket önskvärt, som ovan nämnts.

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.
Hälften av Sveriges befolkning har 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, logglistor redovisande journalåtkomst och e-post med enkelhet tillhandahållas till en registrerad.

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.

5. Personuppgiftsincidenter

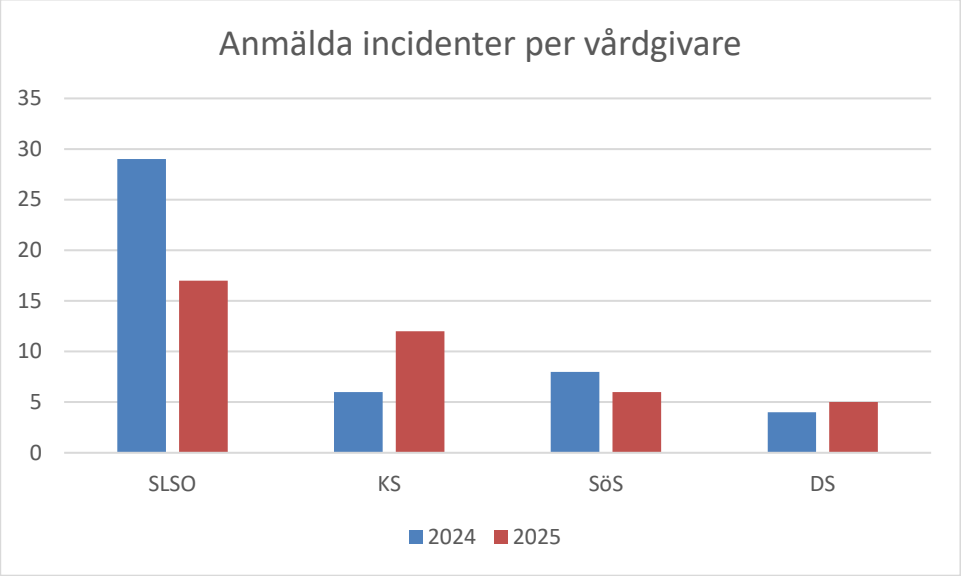
En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt hanterats. En incident ska utan onödigt dröjsmål och, om 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 mycket lågt. Antalet anmälda incidenter har dessutom sjunkit i jämförelse med år 2024.
Under 2025 anmäldes 17 personuppgiftsincidenter där övervägande delar av incidenter berodde på den mänskliga faktorn. Det vill säga någon form av felskick, dvs brev, mejl eller sms.

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 egenupptäckta, anmälda incidenter är fortsatt högre inom SLSO även i jämförelse med den största vårdgrannen KS. Orsaken varför det ser ut på detta sätt kan inte DSO bedöma.

Beträffande antalet incidenter så är det viktigt att påpeka att det inte nödvändigtvis behöver vara en indikation på bristande säkerhet att en organisation anmäler 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.

För SLSO:s räkning är antalet inrapporterade incidenter mycket 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 och tagit fram APT-material för chefer för att informera om vad som utgör en personuppgiftsincident samt vikten av att göra incidentanmälan till IMY då även underlåtenhet att rapportera kända incidenter 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.

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.

I dagsläget sker kommunikation via intranätet och inom dataskyddsorganisationen. Det 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.

6.1 Ny regionövergripande riktlinje

Under hösten har nämnder och bolag inom Region Stockholm haft möjlighet att lämna remissvar för en ny regionövergripande riktlinje kring informationssäkerhet som även omfattar dataskydd. Uppdateringar har gjorts på det ursprungliga förslaget efter avslutat remissrunda. Den nya riktlinjen för informationssäkerhet och dataskydd gäller från och med den 15 januari 2026.

7. Omvärldsbevakning

En noggrann och omfattande omvärldsbevakning som är en del i DSO:s arbete 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 som bland annat innehåller regler om förbjudna AI-system har börjat gälla. Resterande delen av AI-förordningen träder i kraft den 1 augusti 2026.

SLSO har under det gångna året tittat på olika AI-lösningar som förenklar vårdens krav på dokumentation i patientjournaler. Läkare dikterar eller spelar in samtal samtidigt som denne träffar patienten och AI skriver texten som sedan hamnar i patientens journal efter att läkaren slutgranskat AI-resultatet.
Dessa AI-lösningar använder sig av företrädesvis amerikanska molntjänster som i sin tur använder sig av supporttjänster som är sprida över jordklotet. För SLSO är det omöjligt att kontrollera i vilket land som supporten utförs. Det går inte heller att säkerställa att ingen utländsk support har åtkomst till ljudinspelning av en patient eller information som kan kopplas till en levande patient.

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.

7.2 ”Omnibus- förordningen”

EU-kommissionen presenterade i november 2025 ett förslag på omfattande ändringar i dataskyddsförordningen (GDPR), den så kallade digitala omnibus-förordningen. Förslaget bottnar i ett avgörande från EU-domstolen[1] där domstolen kom fram till att pseudonymiserad data inte alltid kan anses vara personuppgifter. Avgörandet och de föreslagna ändringarna i art 4 .1 GDPR har stor inverkan på huruvida tredje part till vilken data överförts, kan identifiera pseudonymiserad (kodade) personuppgifter.
Det finns å ena sidan en risk för att domstolsavgörandet ger en signal om att alla pseudonymiserade personuppgifter kan anses vara oidentifierbara, det vill säga inte utgöra personuppgifter, och därmed så är det fritt fram att föra över patientuppgifter i kodad form.
Det finns dock en å andra sidan en risk för att utredningsansvaret ökar för att en personuppgiftsansvarig behöver säkerställa att tredje part verkligen inte kan identifiera pseudonymiserade personuppgifter beroende på vad EU-kommissionen senare bestämmer efter genomförd remissrunda.

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.
Som beskrivits så använder många AI-tjänster amerikanska molntjänster där risken finns att patientinformation blir åtkomlig för företag eller individer i tredje länder som ska utföra support. Patientuppgifterna anses då vara röjda. DSO har ett ansvar för att påpeka en sådan risk men är medveten om att kraven på effektivisering och förbättrad arbetsmiljö eventuellt prioriteras med en risk om att information inte hanteras så säkert som GDPR kräver.

DSO önskar förstärka det systematiska dataskyddsarbetet som exempelvis revision av verksamheternas dataskyddsarbete.

Komplexitet av regelverket, ny tillkommen praxis och den tekniska utvecklingen ökar i snabb takt. Idag består DSO:s arbete främst i att hantera akuta ärenden, där uppföljnings- och granskningsverksamhet behöver ses över så att DSO kan fungera som oberoende granskande funktion.

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

[1] (EDPS v SRB (C-413/23 P))

Stockholm, mars 2026

Camilla Heise Löwgren
Dataskyddsombud

John Jacobson
Dataskyddsombud