Stockholms läns sjukvårdsområde
Sjukvårdsdirektören

ANMÄLAN
2020-05-11

SLSO 20-904

Granskningsrapport GDPR för verksamhetsåret 2019

Granskningsrapport GDPR för verksamhetsåret 2019 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2020-04-01

Diarienr 20-904

Granskningsrapport GDPR

För verksamhetsåret 2019

Innehållsförteckning

1. Inledning 3

2. SLSO:s registerförteckning 3

3. Information till de registrerade....3

4. De registrerades rätt till registerutdrag 4

5. Personuppgiftsincidenter.... 4

6. SLSO:s arbete med IT-säkerhet kring personuppgiftsbehandlingar 5

7. Behörighetsstyrning och loggning 5

8. Säker kommunikationslösning 6

9. Hur har SLSO arbetat med personuppgiftsbiträdesavtal (PuB)? 7

10. Utbildning 7

11. Konklusion 7

1. Inledning

Enligt artikel 24 i dataskyddsförordningen/GDPR har nämnden det yttersta ansvaret för verksamhetens personuppgiftshantering. Dataskyddsombuden ska med stöd av artikel 29 gruppen (som är en expert-grupp kring tolkningen av dataskyddsförordningen) årligen informera nämnden om det gånga årets arbete med personuppgiftshanteringen som bedrivits inom verksamheten.

2. SLSO:s registerförteckning

SLSO ska enligt artikel 30 i dataskyddsförordningen föra ett register över de personuppgiftsbehandlingar som utförs under dess ansvar, för detta syfte använder SLSO ett systemstöd vid namn Personuppgiftshantering (PUH). Registerverktyget PUH har några inneboende brister som försvårar uppföljningen av SLSO:s personuppgiftsbehandlingar gällande registerägare och kontaktpersoner vid t.ex. byte av tjänst eller pensionsavgång vilket resulterar i att somliga behandlingar möjligen har inaktuell information gällande just registerägare och kontaktperson.

På grund av registerverktygets ålderdomlighet så anges fel lagrum vid godkännande av behandlingar, detta korrigeras manuellt av dataskyddsombuden så att behandlingen får hänvisning till rätt lagrum vid godkänd behandling.

Nuvarande brister i SLSO:s registerverktyg kommer helt avhjälpas under hösten och vintern 2020 då PUH ersätts av ett nytt registerverktyg (DraftIT) vilket kommer underlätta arbetet med registrering av behandlingar. Detta verktyg kommer att implementeras inom hela Region Stockholm.

3. Information till de registrerade

SLSO har ansvar enligt dataskyddsförordningen att informera om den personuppgiftsbehandling som sker inom myndigheten. Ett steg i att uppfylla informationsplikten gentemot de registrerade har varit att förmedla övergripande information om integritet och behandling av personuppgifter inom SLSO på websidan (SLSO.sll.se). SLSO förmedlar där sina skyldigheter att värna om de registrerades integritet samt de registrerades rättigheter i förhållande till SLSO som myndighet. Informationen till de registrerade går att ladda ner och skriva ut samt öppna upp i ett program för uppläsning.

Informationsmaterial och affischer är framtagna till SLSO:s verksamheter och finns tillgängligt på intranätet.

Intern kommunikation till SLSO:s anställda har skett både genom utbildningsinsatser samt användning av intranätet. SLSO:s jurister har skrivit ett PM vilket utgör en översikt för regelverket enligt dataskyddsförordningen som är till för att ge vägledning och råd till förvaltningens anställda.

SLSO:s dataskyddsombud har tagit fram ett särskilt avsnitt som finns på intranätet, där sjukvårdsområdets anställda kan få svar på frekvent återkommande frågor kring personuppgiftshanteringen. På intranätet finns även en länk till Lärtorget som leder till e-utbildningen om GDPR som dataskyddsombuden tagit fram.

4. De registrerades rätt till registerutdrag

Registrerade har enligt artikel 13 i dataskyddsförordningen rätt att vända sig till SLSO för att få veta vilka personuppgifter som SLSO hanterar om personen i fråga. För att säkerställa de registrerades rättigheter och SLSO:s skyldighet att ta fram ett så kallat registerutdrag om enskild begär det, har därför en rutin skapats.
Under 2019 var det två personer som begärde registerutdrag vilket kunde tillhandahållas.

5. Personuppgiftsincidenter

Under 2019 har SLSO:s dataskyddsombud rapporterat tio personuppgiftsincidenter till Datainspektionen varav tre incidenter involverade andra vårdgivare inom Region Stockholm.

De tre regionövergripande incidenterna var primärt tekniska incidenter där den ena incidenten röjde känsliga personuppgifter via adressfältet till 1177:s webbplats. Den andra och tredje incidenten var en brist i åtkomst- och behörighetsstrukturen i ett avvikelsehanteringssystem vilket resulterade i att obehörig personal kunde få tillgång till sekretessbelagda uppgifter. Anmälan till Datainspektionen för de tre incidenterna gjordes medan avvikelserna korrigerades av respektive systemägare. Varje drabbad vårdgivare har därefter analyserat materialet som hör samman med incidenterna för att säkerställa att ingen patient som sökt vård hos respektive vårdgivare fått sin integritet kränkt.

Tre utav de sju interna personuppgiftsincidenterna var handhavandefel av SLSO:s personal i överföringen av personuppgifter vilket resulterat att de skickats till fel mottagare.

Vidare inträffade tre incidenter med ID-kapning då personer har använt sig av en annan persons ID för att få vård vilket förutom anmälan till Datainspektionen också ledde till polisanmälan. Berörda patienter har informerats om det inträffade. SLSO har en riktlinje för identitetskontroll som ska följas i syfte att bland annat undvika situationer av detta slag. Slutligen gjorde en vårdpersonal medvetna dataintrång genom att dokumentera patientbesök som aldrig ägt rum i syfte att skapa sig mer fritid. Personalen är numera uppsagd och polisanmäld för dataintrång.

Slutligen har en rutin vid incidenthantering tagits fram då SLSO har en skyldighet att rapportera alla personuppgiftsincidenter inom 72 timmar.

6. SLSO:s arbete med IT-säkerhet kring personuppgiftsbehandlingar

SLSO har som målsättning att förbättra sin projekthantering genom att bli bättra på att registrera, bereda & kvalitetssäkra, prioritera & besluta samt följa upp alla utvecklingsprojekt med en IT-koppling. Ett led i denna förbättring var uppstarten av ett kvalitetssäkringsråd. Målet med detta råd är att fatta kloka och tydliga beslut, transparens och ökad förståelse samt identifiering av risker och brister kopplat till utveckling och införande av IT-tjänster samt idéer och innovation inom SLSO.

För att säkerställa god kvalitet och samlad bild inom kvalitetssäkringsrådet samverkar funktioner från arkitektur, informations- och patientsäkerhet, dataskydd, juridik och informatik.

En förbättrad projekthantering och etableringen av ett kvalitetssäkringsråd både ökar och förbättrar IT-säkerheten kring personuppgiftshanteringarna.

Regelefterlevnadskontroller enligt Region Stockholms krav för informationssäkerhet samt kravställning utifrån dataskyddsförordningen pågår kontinuerligt och följer handlingsplanen för informationssäkerhet.

7. Behörighetsstyrning och loggning

Det finns en ansvarig kontobeställare (benämnd som behörig kontobeställare) på varje enhet inom SLSO. Denne ansvarar för beställning av e-tjänstekort, datorkonto och journalsystemskonto till ny personal. Dessutom meddelar och reviderar kontobeställaren förändringar i

personalens anställningsförhållanden i syfte att säkerställa en god behörighetsstruktur inom varje enhet. Det vill säga att behörighet och åtkomst ska vid varje tillfälle avgränsas till användarens aktuella behov utifrån arbetsuppgifter och organisatorisk tillhörighet.

Varje verksamhet granskar tilldelade behörigheter regelbundet. Vanligtvis är behörig kontobeställare en verksamhets- eller enhetschef men uppdraget kan tilldelas annan personal.

Granskningar av journalöppningar från journalsystemet TakeCare sker regelbundet med IT-hjälpmedlet SALA. På varje vårdenhet väljs då automatiskt ett antal användare ut slumpmässigt. De journalöppningar som dessa användare har gjort under föregående månad körs sedan mot en rad kriterier, t ex om de patienter vars journal användaren har öppnat har en vårdkontakt med den aktuella enheten och om användaren har fört journal på patienten. För varje användare granskas upp till 150 patientjournaler.

De resultat som framkommer av körningen mot kriterierna presenteras i en webapplikation där loggranskaren på ett överskådligt sätt kan se om journalöppningarna förefaller relevant eller behöver granskas närmare. Posterna signeras av en person som har utsetts för uppgiften och därefter ska en kontrasignerare göra sin bedömning av samma poster och kontrasignera dem. Eventuella överträdelser som upptäcks anmäls till HR-avdelningen för vidare handläggning. Målet är att samtliga användare i TakeCare ska granskas minst en gång per år enligt gällande rutin.

8. Säker kommunikationslösning

Arbetet med att etablera säkra kommunikationslösningar har resulterat i att kommunikationen mellan SLSO och Förvaltningsrätten nu helt frångått telefaxen och ersatt den med en säker kommunikationslösning. En liknande digital lösning har påbörjats även för kommunikationen mellan SLSO och Socialtjänsten, i första hand gäller det internationella häktningsorder vilket är på Socialstyrelsens direktiv men SLSO arbetar för att säkerställa att det ska gälla samtliga ärenden myndigheterna emellan.

Det finns ett stort behov både internt och externt av enkla och säkra kommunikationslösningar med tanke på de känsliga personuppgifter som hanteras inom nämnden och det som behöver delges andra myndigheter.

Ineras projekt, Säker digital kommunikation (SDK) tillfredsställer SLSO:s behov av säker och enkel kommunikation både intern och externt över myndighetsgränser inom offentlig sektor. SLSO:s dataskyddsombud följer utvecklingen av projektet som nu är inne på sitt tredje år och det har gjorts tester med goda resultat inom kommunal och statlig verksamhet.

Efter granskning av tillgängligt material från pilotstudier och övrigt projektmaterial inom projektet så är SLSO:s bedömning att en eventuell implementation av SDK inte är något som ligger inom överskådlig framtid.

9. Hur har SLSO arbetat med personuppgiftsbiträdesavtal (PuB)?

Mallar för PuB-avtal är framtagna. Dessa används när verksamheterna skriver avtal med externa leverantörer.

Under 2019 har en checklista tagits fram i samarbete med upphandlingsenheten för när PuB behöver skrivas och dataskyddsombuden granskar PuB-avtalen inför signering. Det är inte ovanligt att leverantörer kräver att deras avtalsmallar för PuB-avtal används vilket kan ställa till en del problem som kräver avtalsanpassningar. Förutom upphandlingsenheten så genererade även flera forskningsprojekt PuB-avtal under 2019.

Tanken för 2020 är att skapa ett samverkansavtal med tillhörande PuB-avtal med Karolinska institutet (KI) för att underlätta för forskare när dessa använder sig av patientuppgifter från SLSO:s verksamheter.

10. Utbildning

SLSO har i dagsläget ca 12 000 anställda och det är svårt att nå ut till alla anställda för att informera om dataskyddsförordningen och om vad som gäller när man hanterar personuppgifter inom hälso- och sjukvården. För att täcka utbildningsbehovet och underlätta för vården har en digital utbildning tagits fram som nås via Lärtorget. SLSO har varit en av initiativtagarna till utbildningen tillsammans med hälso- och sjukvårdsförvaltningen och trafikförvaltningen. Den elektroniska utbildningen får användas av alla ingående förvaltningar och bolag inom Region Stockholm.

Under det gångna året har en Riktlinje för hantering av personuppgifter tagits fram i samarbete med dataskyddsombuden från hälso- och sjukvårdsförvaltningen.

11. Konklusion

Arbetet med att säkerställa de registrerades fri- och rättigheter enligt dataskyddsförordningen har fortskridit med ett fokus på att öka kunskapen inom organisationen genom både fysiska och digitala utbildningsinsatser

samt upprättande av nya rutiner. Dessa utbildningsinsatser och rutiner har inneburit goda resultat inom upphandlingsenheten då SLSO nu är mer följsamma gällande t.ex. tecknande av PuB-avtal.

Ett nytt systemstöd för registerförteckning har upphandlats via regionledningskontoret vilket kommer implementeras under 2020. Det nya systemstödet kommer hjälpa SLSO att svara upp mot de krav som ställs på en registerförteckning.

Slutligen ska det nämnas att det systematiska arbetet med att säkerställa ett adekvat skydd för de registrerades integritet stärktes genom inrättande av ett kvalitetssäkringsråd vilket möjliggör att på ett systematiskt sätt bereda och kvalitetssäkra, prioritera och besluta alla nya projekt och innovationer inom SLSO.

Samverkan med verksamhetsområdet patientsäkerhet rörande avvikelsesystemet Händelsevis har initierats och kommer att fortsätta under 2020 för att fånga upp eventuella personuppgiftsincidenter som rapporteras i Händelsevis men inte når dataskyddsombuden. Det är viktigt att uppmärksamma vårdpersonalen att personuppgiftsincidenter kan ske även på andra sätt än enbart digital hantering.

Stockholm, april 2020

Camilla Heise Löwgren
Dataskyddsombud

Henrik Strand
Dataskyddsombud