Granskningsrapport

Behandlingsregistret

Vård- och omsorgsnämnden

2023-01-27

Dataskyddsombud
Lunds kommun

Security Solution Scandinavia AB
Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

Office +46 31 98 90 00
www.securitysolution.se

Innehåll

Security Solution Scandinavia AB
Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

Office +46 31 98 90 00
www.securitysolution.se

1 Sammanfattning

Målet med granskningen är att säkerställa att kommunens nämnder och styrelser följer dataskyddsförordningens bestämmelser kring ett behandlingsregister som personuppgiftsansvarig. Vidare syftar granskningen till att informera om, och ge rekommendationer och stöd till respektive personuppgiftsansvarig att upprätta och upprätthålla ett processorienterat behandlingsregister.

Dataskyddsombudet noterar att Lunds kommun arbetat med behandlingsregister i olika faser sedan införandet av Dataskyddsförordningen 2018. Bakgrunden till granskningen är att upprättandet av ett behandlingsregister är ett uttryckligt krav i dataskyddsförordningens artikel 30. Registret är också grunden för systematik och kontroll av hur organisationen efterlever dataskyddsförordningen och hur den hanterar personuppgifter på ett lagligt och säkert sätt.

Vård- och omsorgsnämnden har ett behandlingsregister som i vissa fall saknar lagstadgad information om behandling av personuppgifter enligt artikel 30 GDPR. I dataskyddsombudets granskning av vård- och omsorgsnämndens behandlingsregister har det identifierats en del brister där granskningen leder till att rekommendationer ges, t.ex. att nämnden bör förklara och komplettera med ytterligare information för att behandlingsregistret ska bli komplett och tydligare i sin form.

Dataskyddsombudet ser att det kan finnas ett behov att övergå till ett processbaserat behandlingsregister för att kunna tydliggöra/specificera ändamål och rättslig grund med varje behandling. Det kan finnas svårigheter med att avgöra rättslig grund då en personuppgifts-behandling är beskriven utifrån ett specifikt IT-system eller program. Likaså att förklara ändamålet med *behandlingen* och inte med *systemet* eller *applikationen*.

Sammanfattade rekommendationer

- Komplettera registret och tydliggör information om behandlingarna.
- Uppdatera ändamål med behandling så att ändamålet speglar varför det är nödvändigt att behandla personuppgifter på ett visst sätt och i en viss omfattning.
- Komplettera de behandlingar där rättslig grund ej angivits.
- Genomför en översyn av tidsfrister och dokumentera i behandlingsregistret.
- Övergå till ett processbaserat behandlingsregister, använd formuläret ”VOO NY” för att skapa ett processbaserat behandlingsregister.

2 Terminologi

Personuppgiftsansvarig (PUA)	Den organisation (i kommuner ofta nämnd eller styrelse) som bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till. Personuppgiftsansvarig bestämmer mål och medel för behandlingen.
Personuppgiftsbiträde (PUB)	Den organisation/aktör som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvarigas organisation.
Dataskyddsombud (DSO)	Dataskyddsombudets roll är att kontrollera att dataskyddsförordningen följs inom organisationen genom att till exempel utföra kontroller, utbildnings- och informationsinsatser.
Dataskydd	Skyddet för den personliga integriteten vid behandling av personuppgifter.
Behandling	All insamling, hantering, lagring och radering av personuppgifter som helt eller delvis sker på automatisk väg.
Behandlingsregister	Ett register som dokumenterar de behandlingar som PUA eller PUB utför. Behandlingsregister kallades tidigare för registerförteckning.
Artikel 30	Artikeln i dataskyddsförordningen som beskriver att ett register över behandlingar ska föras, samt det obligatoriska innehållet.
Rättslig grund	Innefattar de rättsliga grunder enligt Dataskyddsförordningen art. 6.1 då en behandling anses laglig. Laglig grund används som ett synonymt begrepp.
Mottagare	Enligt Dataskyddsförordningen innefattar ’mottagare’ både personuppgiftsbiträden samt tredje parter.
Tredje part	En fysisk eller juridisk person som inte är den registrerade, den personuppgiftsansvarige, eller personuppgiftsbiträdet utan behandlar personuppgifter för sina egna ändamål
Tredjeland	Samtliga länder som ligger utanför EU/EES-området.
Gallringsfrist	Den tidpunkt då personuppgifter raderas.
Dataskyddsförordningen	Dataskyddsförordningen är den svenska kompletterande lagstiftningen till EU förordningen GDPR. Dataskyddsförordningen och GDPR används synonymt i denna rapport.

3 Bakgrund

Dataskyddsombudet ska enligt artikel 39.1.b dataskyddsförordningen: ”[…]övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av

den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning”.[1]

I Lunds kommun genomför dataskyddsombudet årliga granskningar av olika områden som en del av detta arbete. I tidigare granskningsområden har organisationens mognadsnivå och dess incidenthanteringsprocesser varit föremål för genomlysning. 2022 års granskning vänder sig till samtliga personuppgiftsansvariga nämnder och styrelser i Lunds kommun.

3.1 Granskning av behandlingsregister 2022

Dataskyddsombudets granskning för 2022 innefattar de register över personuppgiftsbehandlingar (vidare kallat för behandlingsregister) som varje nämnd och styrelse i kommunen måste föra enligt lag. Utgångspunkten för dataskyddsombudet är att hjälpa verksamheterna att kunna förvalta detta register långsiktigt, effektivt och med högre kvalitet i efterlevnaden.

3.1.1 Varför ska man ha ett register för personuppgiftsbehandlingar?

Det är ett uttryckligt krav i dataskyddsförordningens artikel 30 och brister i registret kan ge sanktionsavgifter. Registret är också grunden för systematik och kontroll av hur organisationen efterlever dataskyddsförordningen och hur den hanterar personuppgifter på ett lagligt och säkert sätt. Utgångspunkten för transparens gentemot de registrerade finns genom behandlingsregistret. Registret är viktigt för att visa att organisationen uppfyller ansvarsskyldigheten.

3.1.2 Användningsområden för behandlingsregistret

Ett behandlingsregister har flera huvudsakliga användningsområden, exempelvis:

- Lämna ut uppgifter till IMY vid tillsyn, eller vid begäran om allmän handling.
- Vid incidenter kan personuppgiftsansvarig identifiera vilka personuppgiftsbehandlingar och kategorier av registrerade som påverkas av ett systemhaveri eller en dataläcka.
- Vid ett registerutdrag enligt artikel 15 i Dataskyddsförordningen kan personuppgiftsansvarig mer effektivt identifiera vilka IT-system där personuppgifter behandlas.
- Stöd för klassning, riskanalys och konsekvensbedömningar.
- Hjälp vid hantering av personuppgiftsbiträdesavtal.
- Hjälp vid kontroll av leverantörer

[1] Europarlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG. Förordningen benämns i det följande som Dataskyddsförordningen. https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=SV

Ovan uppräkning är inte uteslutande och flera av dessa går in i varandra. Poängen är att utan ett effektivt sätt att hantera behandlingsregistret, är det svårt att ha en god efterlevnad på andra områden som täcks av Dataskyddsförordningen.

3.2 Omvärldsanalys

Integritetsskyddsmyndigheten (IMY) har tillsammans med andra europeiska data-tillsynsmyndigheter kommit med rekommendationer i tillsynsärenden gällande transparens.[2] I rekommendationerna lägger tillsynsmyndigheterna stor vikt vid den personuppgiftsansvariges kännedom om de personuppgiftsbehandlingar som utförs. En förutsättning för bra information och hög dataskyddsmognad kännetecknas av att behandlingsregistret innehåller fullständig information om de personuppgiftsbehandlingar som verksamheten utför. Behandlingsregistret ligger till grund för den personuppgiftsansvariges möjlighet att uppfylla artikel 30 i Dataskyddsförordningen. En tydlig informationsredovisning och systematiskt arbetssätt visar på högre kunskap, större medvetande och en djupare kännedom om de personuppgiftsbehandlingar som utförs.

3.3 Processer eller system

Det finns två huvudsakliga sätt att dokumentera ett behandlingsregister – utifrån system eller processer.

1. **Verksamhetsprocesser**: En struktur av aktiviteter som genererar och använder personuppgifter
2. **System**: Multipla aspekter av applikationer/system (ex moln, geografisk placering) och koppla till risker och säkerhetsåtgärder

Båda delar behöver finnas dokumenterat inom en verksamhet, men utgångspunkten i behandlingsregistret är vilka personuppgifter som hanteras och varför. Därför är det en fördel att utgå från verksamhetsprocesser. Samtidigt behövs också en förteckning av system, eftersom flera aspekter till underleverantörer och säkerhetsåtgärder kopplas till de tillämpningar som används. Kopplingen mellan process och system är att en behandling kan använda flera system, samtidigt som ett system kan förekomma i många processer.

3.3.1 Systemorienterat behandlingsregister

Sedan Dataskyddsförordningen trädde i kraft 2018 har praxis förändrats för hur ett behandlingsregister ska utformas. Vid starten av dataskyddsarbetet var den gängse modellen att utforma behandlingsregistret enligt en systemorienterad modell. Vanligtvis genomfördes kartläggningar av system, listor och applikationer som användes i verksamheterna. De personuppgiftsbehandlingar som påträffades i ett system kunde användas för många olika

[2] IMY, Beslut 2021-03-31 efter tillsyn enligt dataskyddsförordningen – Klarna Bank AB (Dnr: DI-2020-10518) https://www.imy.se/tillsyner/klarna-bank-ab/ samt Datatilsynet, Beslut 2022-07-14 efter tillsyn enligt dataskyddsförordningen – Helsingörs kommun (journalnummer: 2020-431-0061) https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-

ändamål. Resultatet blev ett stort behandlingsregister som var svårhanterligt, med mycket information som behövde upprepas.

Efter omvärldsbevakning av andra kommuner och offentliga aktörer har dataskyddsombudet konstaterat att en stor andel personuppgiftsansvariga fortfarande har ett systemorienterat behandlingsregister. Många gånger är registret inte heller uppdaterat sedan det upprättades. Eftersom system och tjänster byts ut över tid är risken uppenbar att tidiga systemorienterade behandlingsregister blir mindre rättvisande.

3.3.2 Mot processorientering

Dataskyddsombudet ser en nu förändrad praxis på området och de offentliga aktörernas attityd tyder på att ett processorienterat behandlingsregister ger bättre möjligheter till en långsiktig hantering. Verksamheternas processer och ändamål ändras inte i samma takt över tid.

En processorientering är inget nytt. Inom arkivhanteringen har det länge varit en utgångspunkt att kartlägga verksamhetens processer för en bättre klassificering av handlingar. Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet gav 2012 ut en bra vägledning, som visar att användandet av processer underlättar arbetssätt, samt effektiviserar och medför en högre kvalitet i informationshantering i stort.[3]

Utifrån denna bakgrund och ny praxis på området, beslutade dataskyddsombudet att utbilda representanter från kommunen i hur ett processorienterat behandlingsregister tas fram och sedan granska nämnder och styrelsers behandlingsregister för att säkerställa långsiktig lagefterlevnad gentemot artikel 30 i dataskyddsförordningen.

[3]MSB & riksarkivet (2012) *Vägledning för processorienterad informationskartläggning* https://rib.msb.se/filer/pdf/26410.pdf

4 Artikel 30 – register över behandlingar

Enligt dataskyddsförordningen har PUA och PUB olika ansvar för behandlingen och hur utförligt den ska beskrivas i ett register. En nämnd eller styrelse kan inneha bägge roller. Kraven enligt artikel 30.1 avser PUA och 30.2 avser PUB. Tabell 1 Artikel 30 – register över behandlingar visar en översikt över kravställningarna. Kraven är mer omfattande för PUA. En del punkter är inte tillämpliga för PUB. Personuppgiftsbiträdet kan notera dessa punkter i sitt register, men har inget eget ändamål med behandlingen och ska utföra de saknade kraven enligt instruktioner från personuppgiftsansvarig.

Tabell 1 Artikel 30 – register över behandlingar

	Personuppgiftsansvarig (Art 30.1)	**Personuppgiftsbiträde (Art 30.2)**
Förteckning av vad	Behandlingar	Kategorier av behandlingar som utförs på uppdrag av ansvarig
Kontaktinfo	Namn och kontaktuppgifter för: • Ansvariga • Gemensamt ansvariga (i vissa fall) • Ansvariges representant • Dataskyddsombud (DSO)	Namn och kontaktuppgifter för: • Biträdets biträde (Underleverantör) • Varje ansvarig som biträdet agerar på uppdrag av • Ansvarig och biträdes representant (i vissa fall) • Dataskyddsombud (om det finns)
Ändamål	Ändamål med behandlingen (inkl. laglig grund, nödvändighet)	Ej tillämpligt
Registrerade	En beskrivning av kategorier av registrerade	Ej tillämpligt
Personuppgifter	En beskrivning av kategorier av personuppgifter (om skyddsvärda/känsliga gäller även art 9 GDPR)	Ej tillämpligt
Mottagare	Kategorier av mottagare som personuppgifter har eller kommer skickas till (inkl. mottagare i tredjeland eller internationell organisation)	Ej tillämpligt (enligt instruktioner)
Säkerhet	En generell beskrivning av tekniska och organisatoriska säkerhetsåtgärder om möjligt enligt artikel 32.1	En generell beskrivning av tekniska och organisatoriska säkerhetsåtgärder om möjligt enligt artikel 32.1
Gränsöverskridande behandling	Överföringar till tredjeland eller internationella organisationer (om detta finns) Lämpliga skyddsåtgärder enligt art 49.1 vid undantag i särskilda situationer	Överföringar till tredjeland eller internationella organisationer (om detta finns) Lämpliga skyddsåtgärder enligt art 49.1 vid undantag i särskilda situationer
Lagring	Planerade tidsgränser för radering av olika kategorier av uppgifter	Ej tillämpligt (enligt instruktioner)

4.1 Personuppgiftsansvarig (PUA)

Respektive nämnd eller styrelse är personuppgiftsansvarig för sin verksamhets personuppgifts-behandling. Den personuppgiftsansvariga är skyldig att föra ett register över sina behandlingar. Enligt artikel 30 i dataskyddsförordningen ska respektive personuppgiftsansvarig dokumentera varje behandling som utförs under dess ansvar och ska inkludera de obligatoriska uppgifterna som presenteras i artikel 30.1 a-g.

4.2 Personuppgiftsbiträde (PUB)

Den som behandlar personuppgifter för en personuppgiftsansvarigs räkning är personuppgiftsbiträde. Utöver underleverantörer kan PUB förekomma inom kommunen. En del av organisationen kan vara PUB åt en annan del som är PUA. Exempelvis kan ett koncernbolag vara PUB gentemot sina dotterbolag, eller en kommunstyrelse eller servicenämnd kan vara PUB åt andra nämnder. Kraven gällande ett personuppgiftsbiträdes dokumentation i ett register av behandlingar presenteras i artikel 30.2 a-d.

4.3 Dataskyddsombud

Utsett dataskyddsombud ska anges tydligt i registerförteckningen med kontaktuppgifter.

4.4 Artikel 32

Både PUB och PUA är skyldiga att enligt artikel 32 dataskyddsförordningen vidta *lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken* för de personuppgiftsbehandlingar de utför.

5 Syfte

Syftet med granskningen är att säkerställa att personuppgiftsansvarig uppfyller kraven i artikel 30.1 i dataskyddsförordningen på ett effektivt och långsiktigt sätt.

6 Mål med granskningen

Målet med granskningen är att säkerställa att kommunens nämnder och styrelser följer dataskyddsförordningens bestämmelser kring ett behandlingsregister som personuppgiftsansvarig. Vidare syftar granskningen till att informera om, och ge rekommendationer och stöd till respektive personuppgiftsansvarig att upprätta och upprätthålla ett processorienterat behandlingsregister.

6.1 Avgränsningar

Granskningen avser artikel 30.1, som rör det ansvar som Vård- och omsorgsnämnden har som personuppgiftsansvarig. Eventuell personuppgiftsbehandling som personuppgiftsbiträde enligt 30.2 är exkluderat ur denna granskning. Där behandlingar som biträde förekommer i granskade dokument noteras detta, men bedöms ej.

Artikel 32 gäller säkerhet i samband med behandlingen och skall anges i behandlingsregistret. En avgränsning i 2022 års granskning är att detta bara kommenteras översiktligt och utan en genomlysning av angivna säkerhetsåtgärder.

Lämpliga skyddsåtgärder för överföringar till tredjeland eller internationella organisationer (om detta finns), ska anges i behandlingsregistret. Skyddsåtgärder noteras och kommenteras, men en mer utförlig bedömning sker inte i 2022 års granskning. (inkl. förekomst av artikel 49 om undantag i särskilda situationer).

7 Granskningsmetod och målområden

Dataskyddsombudet har genomfört utbildning av hur man hanterar ett behandlingsregister, samt gett rekommendationer för skapandet av processorienterade behandlingsregister. Utbildningen för Lunds kommun genomfördes den 2 juni 2022 där representanter för personuppgiftsansvariga var inbjudna. Dataskyddssamordnare och andra personer medverkade vid utbildningen och uppslutningen var stor. Utbildningen presenterade minimikraven enligt artikel 30 samt hur ett processorienterat behandlingsregister kan tas fram utifrån ett antal bra exempel. Material som presenterades under utbildningen ligger till grund för att organisationen ska kunna skapa en mer processorienterad eller processbaserad modell för sitt behandlingsregister.

Själva granskningen skedde därefter genom att en begäran skickades via e-post till samtliga personuppgiftsansvariga med kopia till respektive dataskyddssamordnare. Begäran skickades ut den 30 september 2022 till samtliga personuppgiftsansvariga i Lunds kommun.

Granskningen utgår från två övergripande målområden som presenteras nedan:

7.1 Målområde 1: Artikel 30.1

Underlaget för granskningen är artikel 30.1 i Dataskyddsförordningen, där det tydligt specificeras minimikrav på vilken typ av information som ska inkluderas för respektive behandling. I 2022 års granskning kontrollerades om samtliga krav fanns med i behandlingsregistret ur ett kvalitativt perspektiv, där innehållet bedömts utifrån respektive minimikrav.

Artikel 30.1-kraven tolkades i bred mening till att omfatta samtliga punkter som inkluderas i artikeln, även de som inleds med *om möjligt*...

Samtliga punkter i artikel 30.1 omfattas. Dessa är:

- Namn och kontaktuppgifter för den personuppgiftsansvarige samt dataskyddsombud
- Ändamålen med behandlingen
- Beskrivning av kategorier av registrerade och kategorier av personuppgifter
- Kategorier av mottagare, inklusive mottagare i tredjeländer
- I tillämpliga fall, överföringar till ett tredjeland samt dokumentation av lämpliga skyddsåtgärder enligt artikel 49.1
- Om möjligt, tidsfrister för radering
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder

7.2 Målområde 2: Processorienterat behandlingsregister

Dataskyddsombudets generella rekommendation är att personuppgiftsansvariga tar fram ett processorienterat register. Fördelarna är flera. En av dessa är att registret blir mer användbart

för verksamheten, en guide till vad verksamheten faktiskt gör som innefattar personuppgifter snarare än enbart var och i vilket system de finns. En processbaserad dokumentation kan även användas för att skapa en tydligare bild över de faktiska behandlingarna man har för att inte av misstag dokumentera för mycket.

Målområdet 2:s inriktning finns inte specificerat i dataskyddsförordningen, men praxis på området pekar på att behandlingsregistret blir mer användbart om det baseras på verksamhetens processer snarare än på de system som verksamheten använder. Forskning på området menar att en processorientering av dataskyddsarbetet ger bättre efterlevnad.[4]

Det är vanligt förekommande att organisationer redan idag har en processbaserad verksamhetsbeskrivning och kanske till och med redan har en dokumenterad processbaserad informationshantering. Processerna hjälper verksamheterna till ett gemensamt arbetssätt, som bland annat beskriver hur information ska hanteras. Det är samtidigt viktigt att man inte helt likställer verksamhetsprocesser med personuppgiftsbehandlingar utan tar hänsyn till att man kan dela upp en process inom verksamheten med flera personuppgiftsbehandlingar.

Målområdet granskas gällande hur väl övergången till ett processorienterat register gjorts och hur långt personuppgiftsansvarig har kommit. Rekommendationer ges om huruvida ändamålen är tillräckligt tydligt beskrivna, om det finns en tydlig och uteslutande rättslig grund samt råd för fortsatt arbete.

[4] Cortina, Stéphane, et al. (2021). *Towards a Process-Based Approach to Compliance with GDPR* https://doi.org/10.1007/978-3-030-85521-5_8

8 Resultat

I följande avsnitt presenteras resultatet av granskningen gällande Vård- och omsorgsnämndens behandlingsregister *VOO system*. I anslutning till varje rubrik beskrivs kriterier för vad registret ska innehålla och i vissa fall vad registret bör innehålla. I anslutning ges ett antal rekommendationer till personuppgiftsansvarig i enlighet med Dataskyddsförordningen. Dataskyddsombudet har uppfyllt sitt åtagande enligt artikel 39.1.b Dataskyddsförordningen genom att genomföra granskning och analysera inlämnat behandlingsregister samt presentera resultat, råd och rekommendationer. Nedan presenteras resultatet av genomförd granskning gällande Vård- och omsorgsnämndens lagefterlevnad av artikel 30 Dataskyddsförordningen.

Skala	Kriterier för bedömning
Saknar information/ ofullständigt	Obligatoriska krav är inte uppfyllda, registret är ofullständigt, saknar t.ex. information i obligatoriska fält. Registret går inte att bedöma.
Förbättringspotential	Registret saknar viss icke-obligatorisk information. Det återstår en del arbete för att t.ex. förtydliga och förenkla. Kravet/kraven är delvis uppfyllda.
Tillfredsställande	Förbättringsmöjligheter finns, men lagefterlevnad anses ändå tillfredsställande.
Lagefterlevnad bedöms god	Kontrollen helt uppfylld. Bedömning är att lagefterlevnaden är god.

8.1 Artikel 30 Dataskyddsförordningen

Kraven i artikel 30 Dataskyddsförordningen ställs i förhållande till inlämnat behandlingsregister:

Artikel 30	Bedömning	Kommentar
Kontaktinformation för personuppgiftsansvarig och dataskyddsombud	Förbättringspotential	Samtliga behandlingar har dokumenterat PUA och DSO, men utan kontaktuppgifter.
Ändamål med behandling	Förbättringspotential	Ändamålsbeskrivning behöver förtydligas utifrån nödvändighet, dvs varför personuppgifter behandlas.
Beskrivning av kategorier av registrerade och kategorier av personuppgifter	Förbättringspotential	Tydliga kategorier av registrerade finns men behov av förtydliganden gällande kategorier av personuppgifter
Rättslig grund	Förbättringspotential	Flera rättsliga grunder har angivits för flera behandlingar.
Kategorier av mottagare vid utlämnande av uppgifter	Förbättringspotential	Angivits för en del av behandlingarna men ytterligare komplettering behövs.
Överföring till tredjeland	Tillfredställande	Dokumenterat i de flesta behandlingar men är i några fall bristfälligt dokumenterad.
Tidsfrist för gallring	Förbättringspotential	Lagringstid och arbetssätt för gallring presenteras i en del av behandlingarna.
Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder	Tillfredställande	Dokumentation är angiven för samtliga men tydliggöranden kan behövas.

8.1.1 Kontaktinformation för personuppgiftsansvarig och dataskyddsombud

Personuppgiftsansvarig ska i behandlingsregistret ange kontaktuppgifter till personuppgiftsansvarig och i förekommande fall kontaktuppgifter till personuppgiftsansvarig vid delat personuppgiftsansvar samt kontaktuppgifter till Dataskyddsombudet om sådant har utsetts.

Uppgift om personuppgiftsansvarig anges i samtliga dokumenterade behandlingar. Utsedd kontaktperson för behandlingen hos personuppgiftsansvarig finns dokumenterat i 15 av de 16 dokumenterade behandlingarna. Vård- och omsorgsnämndens utsedda dataskyddsombud anges för varje behandling. Det återfinns inte kontaktuppgifter till kontaktperson hos den personuppgiftsansvariga eller kontaktuppgifter till det av nämnden utsedda Dataskyddsombudet. Dataskyddsombudet noterar att det efter diskussioner med Lunds kommun framkommit att kontaktuppgifter till personuppgiftsansvarig samt Dataskyddsombud finns inlagt i systemet för behandlingsregistret. Kontaktuppgifterna följde inte med i utdraget och finns därmed inte tillgängligt för Dataskyddsombudet vid granskningen av behandlingsregistret. Dataskyddsombudet ser att Vård- och omsorgsnämnden har inkluderat kontaktuppgifter till såväl personuppgiftsansvarig som Datasskyddsombud, men denna information inte framgår av utdraget av registret. Dataskyddsombudet anser därmed att registret kan vara dokumenterat på ett tydligt och tillfredsställande sätt, men att det finns en förbättringspotential för att säkerställa att kontaktuppgifter inkluderas i utdrag från behandlingsregistret.

Dataskyddsombudet rekommenderar att:

- Vård- och omsorgsnämndens kompletterar behandlingsregistret med kontaktuppgifter till personuppgiftsansvarig samt dataskyddsombud

8.1.2 Ändamålen med behandlingen

Det är obligatoriskt att ange vilket/vilka ändamål som finns med behandlingen. Förklara varför personuppgifter hanteras.

Behandlingsregistret *VOO system* finns beskrivning av ändamål för samtliga behandlingar. Ändamålen med att behandla personuppgifter bör förtydligas mer. Det är inte klart uttryckt varför personuppgifter är nödvändiga att behandla för en viss aktivitet, tjänst, eller ärende. Ett exempel är behandlingen ”Procapita VoO” där ändamålet beskrivs i en punktlista med exempelvis "*Journalhantering, beställning/verkställighet, avvikelsehantering (...)”*. Här förklaras det inte tydligt varför det är nödvändigt att behandla de registrerades personuppgifter. Likaså med behandlingen ”Pascal” där ändamålet är *PASCAL – är ett ordinationsverktyg som vi har tillgång till för patienter som har dosdispenserade läkemedel driftas av INERA.* Det räcker inte att förklara hur systemet fungerar eller vad det innehåller, utan behöver även definiera varför personuppgifter behandlas. Dataskyddsombudet anser att dokumentationen gällande behandlingars ändamål har förbättringspotential.

Dataskyddsombudet rekommenderar att:

- Vård- och omsorgsnämnden uppdaterar ändamål med behandling så att ändamålet speglar varför det är nödvändigt att behandla personuppgifter på ett visst sätt och i en viss omfattning.

8.1.3 Beskrivning av kategorier av registrerade och kategorier av personuppgifter

Uppgiften är obligatorisk att ange vilkas personuppgifter som behandlas, exempelvis kund, leverantör, personal, elever, brukare etc. Ange också vilken typ av personuppgifter som behandlas, exempelvis kontaktuppgifter, identifikationsuppgifter. Om det förekommer känsliga/extra skyddsvärda personuppgifter ska dessa dokumenteras.

Vård- och omsorgsnämndens behandlingsregister *VOO system* innehåller tydliga och konsekventa kategorier av registrerade. Kategorier av registrerade finns dokumenterat för samtliga behandlingar. Här används även ”annat” som kategori där det uppgetts i fyra behandlingar men utan specifikation gällande vad ”annat” innebär. Kategorier av personuppgifter finns dokumenterat i flera kolumner. Kategorier av personuppgifter dokumenteras i tio olika kolumner. Detta ger en otydlig och osammanhängande bild av de personuppgifter som respektive behandling innehar. I ”personuppgifter” skrivs ett fåtal personuppgifter och exempelvis kontaktuppgifter dokumenteras på ett annat ställe. Som helhet finns uppgifter som utgör en personuppgift spridda genom behandlingsregistret och det saknas därmed en sammanhängande och tydlig sammanställning. I tre behandlingar (Appva MCSS, Lifecare Mobilhemtjänst (LMHT) samt Phoniro) uppges det under extra skyddsvärda uppgifter att hälsouppgifter behandlas. Dataskyddsombudet vill poängtera att hälsouppgifter anses enligt Dataskyddsförordningen vara känsliga personuppgifter. Detta dokumenteras ännu en gång under kolumnen ”känsliga personuppgifter”. Dataskyddsombudet anser att kategorier av registrerade är tydligt och tillfredställande men att det i dokumentationen av kategorier av personuppgifter inte är tydlig och tillfredsställande dokumenterat och att en förbättringspotential finns.

Dataskyddsombudet vill uppmärksamma på att om särskilda kategorier av personuppgifter, kallas också extra skyddsvärda eller känsliga personuppgifter, behandlas ska dessa personuppgifter anges i registret. Exempel på extra skyddsvärda-/känsliga uppgifter är bland annat uppgift om personnummer (notera att Sverige har valt att ha ett särskilt skydd för personnummer och samordningsnummer, men Dataskyddsförordningen inte tar upp det som extra skyddsvärd[5]), uppgift gällande barn/minderårig, uppgift om medlemskap i fackförening, hälsouppgifter (exempelvis läkar-/sjukintyg), uppgift om brott eller uppgifter som rör den privata sfären.

Dataskyddsombudet rekommenderar att:

- Vid eventuellt kommande behandlingar dokumenteras tydligt och sammanhållet.
- Säkerställa lagligheten i att behandla personuppgifter gällande extra skyddsvärda-/känsliga personuppgifter enligt kompletterande dataskyddslagstiftning och artikel 9 Dataskyddsförordningen, annars upphöra med behandling.
- Dokumentera samtliga kategorier av personuppgifter i en kolumn.

[5] IMY- Personnummer Personnummer (imy.se)

- Dokumentera samtliga kategorier av registrerade och personuppgifter och komplettera behandlingsregistret där ”annat” inte tydliggörs.

8.1.4 Rättslig grund

Verksamheten bör formulera en rättslig grund för behandling av personuppgifter. Finns ingen rättslig grund, eller lämnat samtycke, samt att berörda är informerade är behandlingen olaglig och får ej utföras. Klarna-fallet har visat på vikten att dokumentera rättslig grund för behandling av personuppgifter. Ett sätt för att påvisa om det finns en *rättslig förpliktelse* för behandlingen är att inventera vilka lagar som styr verksamheten. Exempel på detta är upphandlingslagar, bokföringslag, arbetsmiljölagar etc.

Rättslig grund har angivits för 14 av de 16 dokumenterade behandlingarna. För ett antal behandlingar har flera rättsliga grunder angivits, som exempelvis ”Appva MCSS”, ”i-care online (ICO)” samt ”Phoniro” där bland annat avtal, myndighetsutövning, allmänt intresse samt skydda intressen av grundläggande betydelse angivits som rättsliga grunder. Det saknas dokumentation av rättslig grund för två behandlingar, ”Pascal” samt ”Tandvårdsfönstret”. Dataskyddsombudet ser att det för några behandlingar anges flera rättsliga grunder. I dessa fall bör en bedömning göras huruvida behandlingen ska delas upp eller om det bara råder osäkerhet om vilken rättslig grund som ska anges. För några behandlingar anges ej någon rättslig grund och Dataskyddsombudet rekommenderar att rättslig grund dokumenteras för samtliga behandlingar.

Enligt propositionen till den svenska dataskyddslagen[6] är den rättsliga grunden uppgift av allmänt intresse (art. 6.1.e. GDPR) den grund som vanligen bör tillämpas av (kommunala eller statliga) myndigheter, med anledning av att den verksamhet som en myndighet bedriver inom ramen för sin befogenhet är av ”allmänt intresse” för invånarna i kommunen. Dock behöver den rättsliga grunden vila på att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Om verksamheten har en skyldighet enligt lag att tillhandahålla t.ex. ett stöd eller ett skydd till en person eller ålagts att utföra vissa uppgifter kan den rättsliga grunden tillskrivas en *rättslig förpliktelse*, då det inom området finns lagar som styr, till exempel; Lag (2016:1146) om offentlig upphandling (LOU), Tryckfrihetsförordning (1949:105) ändrad t.om. SFS 2018:1801 och Arkivlag (1990:782). Även lokala föreskrifter kan vid hand borga för en rättslig förpliktelse beroende på vad som statueras i exempelvis reglementen eller likande. I de fall samtycke används som rättslig grund bör det finnas upprättad dokumentation om hur samtycke inhämtas och hur det hanteras vid återtagande.

Om den personuppgiftsansvariga måste behandla personuppgifter för att skydda en registrerad, om denne inte kan lämna samtycke genom exempelvis medvetslöshet kan *Skydda grundläggande intresse* användas som rättslig grund. Vård- och omsorgsnämnden har angett denna rättsliga grund i tre behandlingar. Denna rättsliga grund ska enbart användas om behandlingen är

[6] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

nödvändig för att rädda liv. Denna rättsliga grund ska användas i mycket begränsad omfattning och kan enbart användas om behandlingen är nödvändig.[7] IMY rekommenderar att denna rättsliga grund inte ska användas då den registrerade kan fatta beslut, genom exempelvis planerade vårdbesök. Då bör en annan rättslig grund anges för behandlingen. Dataskyddsombudets bedömning är att registret kan förtydligas och har en förbättringspotential.

Dataskyddsombudet rekommenderar att:

- Vård- och omsorgsnämndens ser över och kompletterar de behandlingar där rättslig grund ej angivits.
- Se över samtliga rättsliga grunder, om det möjligtvis finns en skyldighet enligt lag att bedriva en viss verksamhet, där *en rättslig förpliktelse* skulle kunna ligga till grund för behandling av personuppgifter.
- Se över de behandlingar där flera rättsliga grunder har angivits, dela upp behandlingen så att det endast är en rättslig grund per behandling eller ange endast en rättslig grund.
- Vård- och omsorgsnämnden ser över behandlingar där skydda grundläggande intressen angivits som rättslig grund och utreder om denna är den korrekta rättsliga grunden för behandlingen.
- I de fall samtycke används som rättslig grund hänvisa i Tekniska och organisatoriska säkerhetsåtgärder till upprättad rutin/information om hantering av samtycke.
- Att tydligt dokumentera den rättsliga grunden när det kommer till behandling av känsliga- och extra skyddsvärda personuppgifter.

8.1.5 Kategorier av mottagare vid utlämnande av uppgifter

Ange vilken tredje part som är mottagare av personuppgifter. Exempel på tredje part; Myndigheter (Skatteverket, Försäkringskassan), organisationer, personuppgiftsbiträden, leverantör av supporttjänst, banker, Bolagsverket, tredjepartsrevisor, andra aktörer och intressenter.

Uppgift om mottagare finns angivet för 14 behandlingar där det är aktuellt med en tredjepartsutlämning av personuppgifterna eller ej. För exempelvis behandling ”Phoniro” och ”Procapita VoO” anges att uppgifter lämnas ut till en extern mottagare. Mottagare anges som såväl ”Inom kommunen” som ”till en extern part”. Tydliggörande gällande vilken nämnd inom kommunen samt den externa parten finns. I tre behandlingar dokumenteras att ett utlämnande sker men ingen kompletterande information finns. Av de 16 dokumenterade behandlingarna uppger 15 om ett utlämnande till en tredje part sker eller ej. I fyra behandlingar uppges att en utlämning görs, och det specificeras även till vilken eller vilka mottagare. Det saknas kompletterande information gällande vilken mottagare uppgifter lämnats ut till i tre behandlingar. Att endast uppge ”inom kommunen” eller till ”extern part” som mottagare, kan uppfattas som ofullständigt. Dataskyddsombudets bedömning är att där det har dokumenterats kategorier av mottagare är det tydligt och tillfredställande, men att förbättring finns då uppgifter saknas ett antal behandlingar.

[7] IMY - Skydda grundläggande intressen https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/skydda-grundlaggande-intressen/

Dataskyddsombudet rekommenderar att:

- Vård- och omsorgsnämndens ser över och kompletterar registret för att dokumentera mottagare för samtliga behandlingar.
- I förkommande fall att komplettera behandlingsregistret i syfte att säkerställa att samtliga mottagare finns angivna i fysik eller juridisk person. Tänk på att eventuellt personuppgiftsbiträde också är en mottagare av personuppgifter och bör därmed uppges som mottagare.

8.1.6 Överföringar till tredjeland

Om relevant ska detta anges i behandlingsregistret. Ange vem som är mottagare till personuppgifterna som lämnas/skickas ut. Tänk även på att en molntjänstleverantör kan vara en part i tredjeland. Särskilt viktigt om uppgifter lämnas utanför EU/EES-området. Det kan behövas upprättas ett personuppgiftsbiträdesavtal eller ett datadelningsavtal.

Vård- och omsorgsnämndens behandlingsregister ”*VOO system*” dokumenterar om en tredjelandsöverföring sker i 13 av de 16 behandlingarna. Där om en tredjelandsöverföring sker eller ej har det dokumenterat ett nekande svar på samtliga 13 behandlingar. Vård- och omsorgsnämndens rekommenderas att kontrollera om det sker en tredjelandsöverföring i någon av behandlingarna, och i sådana fall, dokumentera uppgifter om att tredjelandsöverföring sker. Dataskyddsombudets bedömning är att registret har dokumenterat tredjelandsöverföring på ett tillfredsställande sätt men att det finns en viss förbättringspotential finns för att samtliga behandlingar ska dokumenteras.

Dataskyddsombudet rekommenderar att:

- Kontrollera och dokumentera eventuell tredjelandsöverföring i förekommande fall.
- Kontrollera att konsekvensbedömning är gjord i förekommande fall.

8.1.7 Tidsfrister för gallring

Uppgiften fylls i om möjligt att ange hur länge informationen sparas. En hjälp är att titta i er informationshanteringsplan/dokumenthanteringsplan som ger ledning i hur länge riksarkivet, styrelsen/nämnden och kommunarkivet har godkänt lagringstider för olika informationstyper. Om gallringsbeslut finns ska de följas. Klarna-beslutet har visat på att det är viktigt att ange lagringstiden och inte bara hänvisa till dokumenthanteringsplanen eller gallringsbeslutet.

Vård- och omsorgsnämndens behandlingsregister dokumenterar att skriftliga gallringsrutiner finns för sju behandlingar. För sju behandlingar uppges att ingen skriftlig gallringsrutin finns och i fyra behandlingar förekommer ingen dokumentation. Tydliggörande kommentarer för hur gallringen sker finns, där det specificeras om gallring sker samt att det i flera fall hänvisas till nämndens dokumenthanteringsplan. Tydliggörande kommentarer finns inte i samtliga av de behandlingar som uppgett en avsaknad av dokumenterad gallringsrutin. I de fall då en skriftlig gallringsrutin finns refereras det till dokumenthanteringsplanen i ett flertal av behandlingarna, som exempelvis ”Appva MCSS” och ”Castor”. Ett flertal beskrivningar gällande gallringsrutinen syftar mer på att beskriva hur en gallring går till snarare än hur längre personuppgifterna lagras (se exempelvis *Traka32_VoO* och *UMO*). Dataskyddsombudet ser att Vård- och omsorgsnämnden

presenterar hur de arbetar med gallring i ett flertal av behandlingarna. I ett antal behandlingar dokumenteras gallringstiden men konkreta tidsintervall saknas i flertalet behandlingar. Dataskyddsombudet ser ett behov av att tydliggöra och dokumentera konkreta tider för gallring av personuppgifter då angivelse om lagringstid är bristande och registeruppgifterna uppfyller inte kravet enligt Artikel 30 samt praxis från Klarna-fallet. Dataskyddsombudet noterar att Vård- och omsorgsnämndens informationsredovisning tydligt dokumenterat tidsfrister för gallring men att denna information saknas i behandlingsregistret. Dataskyddsombudets bedömning är att registret kan förtydligas och har en förbättringspotential.

Dataskyddsombudet rekommenderar att:

- Vård- och omsorgsnämnden genomför en översyn av tidsfrister och dokumenterar i tydliga gallringsrutiner för samtliga behandlingar.
- Vård- och omsorgsnämnden dokumenterar skriftliga gallringsrutiner där det saknas.

8.1.8 Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder

Om möjligt ska detta inkluderas i personuppgiftsansvariges behandlingsregister. Om uppgifter lämnas utanför EU/ESS så ska registret innehålla uppgifter om tekniska och organisatoriska säkerhetsåtgärder.

Vård- och omsorgsnämndens behandlingsregister dokumenterar säkerhetsåtgärder för samtliga behandlingar. De tekniska och organisatoriska säkerhetsåtgärderna finns presenterade i ett flertal kolumner. Vård- och omsorgsnämnden har utförligt dokumenterat gällande behörigheter och behörighetstilldelning för ett antal behandlingar samt tydliggörande kommentarer finns då det saknas en skriftliga rutiner gällande behörighetstilldelning (exempelvis *UMO* och *Kameratillsyn/Trygghetskamera*). Dokumentation kring allmänna tekniska och organisatoriska säkerhetsåtgärder finns för samtliga angivna behandlingar, detta kombineras med dokumentation av behörigheter och behörighetstilldelning samt säkerhetsåtgärder gällande användarna. Detta sätt att dokumentera kan uppfattas rörigt och otydligt varvid Dataskyddsombudet rekommenderar att dokumentera lämpliga skyddsåtgärder enligt Artikel 44–49 Dataskyddsförordningen.

Dataskyddsombudet rekommenderar att:

- Vård- och omsorgsnämnden dokumenterar allmänna tekniska och organisatoriska säkerhetsåtgärder för samtliga behandlingar, där så är lämpligt.

8.2 Processorienterad förteckning

I anslutning till granskningsresultatet ger Dataskyddsombudet rekommendationer kring utformningen av ett processbaserat register. Rekommendationerna baseras på den utbildning som Lunds kommun erhöll den 2 juni 2022.

Vård- och omsorgsnämnden behandlingsregister *VOO process* och *VOO NY* utgörs av en processorienterad struktur där samtliga behandlingar är presenterade utifrån verksamhetens processer. Behandlingsregistret, *VOO NY*, utgör en bra grundstruktur som uppfyller kraven enligt Artikel 30 i Dataskyddsförordningen.

I arbetet med ett processorienterat behandlingsregister är det nödvändigt att informationsbärare/informationstillgångar, dvs berörda system och applikationer, dokumenteras för respektive behandling. Genom att precisera verksamhetssystem/applikationer möjliggörs att en separat systemlista kan upprättas. Systemlistan kan per se innehålla mer känslig eller verksamhetskritisk information. Namn eller annat identifikationssätt på system eller applikationer utgör bryggan mellan de två dokumenten.

Dataskyddsombudet rekommenderar att:

- Vård- och omsorgsnämnden, om möjligt, övergår till en processbaserad registerförteckning.

9 Avslutningsvis

Granskningen av behandlingsregistret har resulterat i ett antal slutsatser. Man kan konstatera att Vård- och omsorgsnämndens behandlingsregister är ett systemorienterat register. Dataskyddsombudets övergripande bedömning av Vård och omsorgsnämndens behandlingsregister är att det finns en förbättringspotential och behov av komplettering. I vissa fall är det systemstödet (DraftIT) som ställer alltför långtgående frågor som gör att det blir onödigt tidskrävande att registrera behandlingar. Dataskyddsombudet rekommenderar att Vård- och omsorgsnämnden fortsätter arbeta med ett processorienterat register och att komplettera de delar där det anmärkts i granskningsrapporten.

Dataskyddsombudet rekommenderar att nämnden och kommunövergripande dataskydds-organisationen arbetar fram tydliga rutiner för hur registret ska hanteras och ge stöd till de verksamheter, där så krävs, för att upprätta korrekta behandlingsregister. En övergång till ett processbaserat behandlingsregister ses som ett steg på vägen att skapa ett mer tids effektiviserat arbetssätt och ett större användningsområde för den dokumenterade informationen.