

Granskningsrapport

Behandlingsregistret

Miljönämnden

2023-01-27

Dataskyddsbud
Lunds kommun

Innehåll

| | | |
|-----|-----------------------------------------------------------|----|
| 1 | Sammanfattning..... | 3 |
| 2 | Terminologi..... | 4 |
| 3 | Bakgrund..... | 4 |
| 3.1 | Granskning av behandlingsregister 2022 | 5 |
| 3.2 | Omvärldsanalys..... | 6 |
| 3.3 | Processer eller system..... | 6 |
| 4 | Artikel 30 – register över behandlingar | 8 |
| 4.1 | Personuppgiftsansvarig (PUA)..... | 9 |
| 4.2 | Personuppgiftsbiträde (PUB)..... | 9 |
| 4.3 | Dataskyddsombud..... | 9 |
| 4.4 | Artikel 32 | 9 |
| 5 | Syfte | 9 |
| 6 | Mål med granskningen..... | 9 |
| 6.1 | Avgränsningar..... | 9 |
| 7 | Granskningsmetod och målområden..... | 10 |
| 7.1 | Målområde 1: Artikel 30.1 | 10 |
| 7.2 | Målområde 2: Processororienterat behandlingsregister..... | 10 |
| 8 | Resultat..... | 12 |
| 8.1 | Artikel 30 Dataskyddsförordningen..... | 12 |
| 8.2 | Processororienterad förteckning..... | 16 |
| 9 | Avslutningsvis | 17 |

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 processororienterat 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.

Miljönämnden har ett behandlingsregister som i vissa fall saknar lagstadgad information om behandling av personuppgifter enligt artikel 30 GDPR. I dataskyddsombudets granskning av nämndens 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 Miljönämnden har påbörjat ett arbete med att upprätta ett processororienterat behandlingsregister och rekommenderar nämnden att färdigställa detta.

Sammanfattade rekommendationer

- Övergå till ett processbaserat behandlingsregister.
- Säkerställa att samtliga behandlingar omfattas i registret
- Komplettera och tydliggör information om behandlingarna där det anmärkts i granskningsrapporten

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 | Artikel 30 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.
- Hjälps vid hantering av personuppgiftsbiträdesavtal.
- Hjälps vid kontroll av leverantörer

¹ Europaparlamentets 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 uppräknade 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 tillsynsändamålet 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

²IMY, 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 processororientering

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

En processororientering 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 processororienterat behandlingsregister tas fram och sedan granska nämnder och styrelser behandlingsregister för att säkerställa långsiktig lagefterlevnad gentemot artikel 30 i dataskyddsförordningen.

³MSB & riksarkivet (2012) *Vägledning för processororienterad 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: <ul style="list-style-type: none"> • Ansvariga • Gemensamt ansvariga (i vissa fall) • Ansvariges representant • Dataskyddsombud (DSO) | Namn och kontaktuppgifter för: <ul style="list-style-type: none"> • Bitrådets 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 personuppgiftsbehandling. 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 Miljönämnden 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 processororienterade behandlingsregister. Utbildningen för Lunds kommun genomfördes den 2 juni 2022 där nämnder och styrelser var inbjudna. Dataskyddssamordnare och andra personer medverkade vid utbildningen och uppslutningen var stor. Utbildningen presenterade minimikraven enligt artikel 30 samt hur ett processororienterat 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 processororienterad 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 att 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: Processororienterat behandlingsregister

Dataskyddsombudets generella rekommendation är att personuppgiftsansvariga tar fram ett processororienterat 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 processororientering 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 processororienterat 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 Miljönämndens behandlingsregister *MN process*. 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 Miljönämndens 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

Behandlingsregistret *MN process* innehåller totalt 44 behandlingar, varav för 14 finns det ytterligare information om behandlingen och hur den uppfyller kriterierna i artikel 30. Bedömningen i detta avsnitt omfattar därav enbart dessa 14 behandlingar.

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 | Saknar information/ ofullständigt | För de flesta behandlingar görs endast hänvisning till dokumenthanteringsplan |
| Beskrivning av kategorier av registrerade och kategorier av personuppgifter | Förbättringspotential | Dokumentation över kategorier av registrerade och personuppgifter förekommer, men behöver förtydligas. |
| Rättslig grund | Förbättringspotential | Flera rättsliga grunder har angivits för flera behandlingar. |
| Kategorier av mottagare vid utlämnande av uppgifter | Förbättringspotential | Huruvida om mottagare förekommer har angetts, troligtvis har inte alla mottagare angetts |
| Överföring till tredjeland | Saknar information/ ofullständigt | Saknas information för samtliga behandlingar |

Security Solution Scandinavia AB

Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

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

| | | |
|----------------------------------------------------------------------|-----------------------------------|----------------------------------------------------------------------------------------|
| Tidsfrist för gallring | Förbättringspotential | Görs endast hänvisning till dokumenthanteringsplan alternativt informationsredovisning |
| Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder | Saknar information/ ofullständigt | Saknas information för samtliga behandlingar |

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 för de 14 behandlingarna. Det finns även angiven kontaktperson hos den personuppgiftsansvariga samt nämndens utsedda dataskyddsombud. 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. Uppgift om personuppgiftsansvarig, kontaktperson hos personuppgiftsansvarig samt utsett dataskyddsombud anges explicit. Däremot saknas kontaktuppgifter till dataskyddsombudet, så som e-postadress eller ett telefonnummer. Dataskyddsombudet har noterat att det för vissa behandlingar i fältet "Vem kan svara på frågor kring behandlingen/processen?" har angetts "Dataskyddsombud Maria Skogh" vilket troligtvis är en inaktuell uppgift.

Dataskyddsombudet ser att Miljönämnden har inkluderat kontaktuppgifter till såväl Personuppgiftsansvarig som Dataskyddsombud, 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:

- Fyll i uppgift om kontaktinformation på behandlingar som saknar detta

8.1.2 Ändamålen med behandlingen

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

Behandlingsregistret har beskrivning av ändamål med behandling för de 14 behandlingarna. För de flesta av de 14 behandlingar görs enbart en hänvisning till dokumenthanteringsplanen. För tre behandlingar anges en mer utförlig beskrivning, dock inte varför det är nödvändigt att behandla personuppgifter utan mer en beskrivning av en arbetsprocess eller en lagstadgad skyldighet som nämnden har. Det räcker inte att förklara att processen beskrivs i dokumenthanteringsplanen. Det skälet, per se, behöver inte betyda att ni måste behandla personuppgifter. Förklara varför

personuppgifter är nödvändiga att samla in eller hantera och beakta dessutom kravet om uppgiftsminimering.

Dataskyddsombudet rekommenderar att:

- Uppdatera ändamål med behandling så att ändamålet speglar varför det är nödvändigt att behandla personuppgifter på ett visst sätt och i en viss omfattning.
- Fyll i uppgift om ändamål för de behandlingar som saknar detta

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.

Miljönämnden presenterar tydliga och konsekventa kategorier av registrerade. Kategorier av personuppgifter anges i olika fält i behandlingsregistret. Kategorier av personuppgifter dokumenteras i tio olika fält. Detta ger en otydlig och osammanhängande bild av de personuppgifter som respektive behandling innehåller. 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. Dataskyddsombudet anser att kategorier av registrerade och personuppgifter kan förtydligas och har därmed förbättringspotential. Dataskyddsombudet har även noterat att för "Behandling 1.1.1 Politiska beslutsprocessen" har det angivits att extra skyddsvärda uppgifter behandlas, men det har inte tydliggjorts vilka kategorier av extra skyddsvärda uppgifter som menas.

Dataskyddsombudet rekommenderar att:

- Dokumentera samtliga kategorier av personuppgifter i ett fält.
- Fyll i uppgift om kategorier av registrerade och personuppgifter på behandlingar som saknar detta

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, arbetsmiljölager etc.

Rättslig grund har angivits för samtliga behandlingar i registret. För några behandlingar har flera rättsliga grunder angivits. 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. 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; Bokföringslag (1999:1078), 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. Dataskyddsombudets bedömning är att registret kan förtydligas och har en förbättringspotential.

Dataskyddsombudet rekommenderar att:

- 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.
- Fyll i uppgift om rättslig grund på behandlingar som saknar detta

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 huruvida mottagare finns eller ej är angivet för 14 behandlingar. Behandlingsregistret uppger tydligt huruvida mottagare finns eller ej genom att ange "ja" eller "nej". För de behandlingar där mottagare finns har dessa tydliggjorts genom att ange antingen "inom kommunen" eller "till extern part". Följt av dessa finns fälten "beskriv den externa parten" alternativt "vilken/vilka nämnd-er?" där mottagare finns angivet. Dataskyddsombudet bedömer att det kan finnas ytterligare mottagare för dessa 14 behandlingar. Därmed kan registret förtydligas och har en förbättringspotential.

Dataskyddsombudet rekommenderar att:

- I förkommande fall att komplettera behandlingsregistret i syfte att säkerställa att samtliga mottagare finns angivna i fysisk eller juridisk person, där så är möjligt. Tänk på att eventuell personuppgiftsbiträde också är en mottagare av personuppgifter och bör därmed uppges som mottagare.
- Fyll i uppgift om mottagare på behandlingar som saknar detta

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.

Uppgift om behandling med potentiell tredjelandsöverföring är ej angett. Miljönämnden rekommenderas att kontrollera om det sker en tredjelandsöverföring i någon av behandlingarna, och i sådana fall, dokumentera uppgifter om att tredjelandsöverföring sker. I förekommande fall krävs även att en konsekvensbedömning är utförd. Kontrollera att konsekvensbedömning har

gjorts, där så krävs. Dataskyddsombudets bedömning är att registret har en förbättringspotential, att behandling av potentiellt känsliga personuppgifter kontrolleras och dokumenteras mer noggrant.

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.

I Miljönämndens behandlingsregister besvaras frågan "*Finns det skriftliga gallringsrutiner*" (besvaras med ja eller nej) och om ja, görs hänvisning till dokumentationen, men en specifik lagringstid anges inte. För de 14 behandlingarna görs enbart hänvisning till dokumenthanteringsplanen alternativt informationsredovisningen. Det är inte tillräckligt tydligt, den faktiska lagringstiden bör anges. Det återstår en del arbete för att registret kan förtydligas och det har en förbättringspotential.

Dataskyddsombudet rekommenderar att:

- Miljönämnden genomför en översyn av tidsfrister och dokumenterar i behandlingsregistret.

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.

Registret har inget fält/kolumn/fråga för att ange allmänna tekniska och organisatoriska säkerhetsåtgärder. Det anges att konsekvensbedömning har utförts för några behandlingar, övrig dokumentation saknas, varvid Dataskyddsombudet rekommenderar att dokumentera lämpliga skyddsåtgärder enligt Artikel 44–49 Dataskyddsförordningen.

Dataskyddsombudet rekommenderar att:

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

8.2 Processororienterad 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.

Miljönämndens behandlingsregister, *MN process* innehåller 44 behandlingar. Dessa behandlingar kan utgöra en bra grund för att skapa ett fullständigt processbaserat behandlingsregister.

Inom ramen för ett processororienterat behandlingsregister ska det finnas en tydlig ändamålsbegränsning där ändamålen måste vara specifika och konkreta, inte luddiga eller otydliga. När man formulerar en ändamålsbeskrivning ska man kunna börja ändamålet med att "Det är nödvändigt att behandla dessa personuppgifter för att...". Miljönämndens ändamålsbeskrivningar hänvisar till processer i nämndens dokumenthanteringsplan. Detta försvårar förståelsen för personuppgiftsbehandlingen och processens syfte. Nämndens behandlingar illustrerar behovet inom behandlingsregistret att tydliggöra och konkretisera respektive ändamål. Ett klagörande av ändamålen är vitalt för ett processororienterat behandlingsregister då det tydliggör hela behandlingens process.

I arbetet med ett processororienterat 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. Miljönämnden har dokumenterat informationsbärare avseende de 14 behandlingarna.

Dataskyddsombudet rekommenderar att:

- Miljönämnden, om möjligt, övergår till ett processbaserat behandlingsregister.

9 Avslutningsvis

Granskningen av behandlingsregistret har resulterat i ett antal slutsatser. Dataskyddsombudet kan konstatera att Miljönämnden påbörjat arbetet med att upprätta och föra ett processororienterat behandlingsregister och rekommenderar att nämnden fortsätter detta arbete.

Resultatet från granskningen indikerar på vissa svårigheter med att besvara kraven. I vissa fall är det systemstödet (DraftIT) som ställer alltför långtgående frågor som gör att det blir onödigt tidskrävande att registrera behandlingar. I andra fall kan skönjas en begränsad kunskapsnivå hos personuppgiftsansvarig kring vad som ska dokumenteras och hur texterna ska formuleras. Med insikt av detta bör nämnden säkerställa att en konsekvent och korrekt hantering av nämndens behandlingsregister utförs inom den egna förvaltningen.

Dataskyddsombudet rekommenderar att nämnden och kommunövergripande dataskyddsorganisationen 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 effektiviserat arbetssätt och ett större användningsområde för den dokumenterade informationen.