Dataskyddsombudets rapport

Kvartal 2 2023

Diarienummer	Senast uppdaterad	Beslutsinstans	Processägare
20230227:036	2023-06-26	Dataskyddsombud	Dataskyddsombud

Dokumentets syfte

Den personuppgiftsansvariga nämnden har en skyldighet enligt dataskyddsförordningen att ansvara för, och kunna visa på, att dataskyddslagstiftningen efterlevs.[1]

Kvartalsrapporten tas fram av dataskyddsombudet och syftar till att hålla den personuppgiftsansvariga nämnden och kommunledningsgruppen informerad om dataskyddsombudets iakttagelser av kommunens hantering av personuppgifter. Detta som ett led för att nämnden ska kunna ta sitt personuppgiftsansvar och kunna redovisa sin efterlevnad av dataskyddsförordningen.

Dokumentet gäller för

Kvartalsrapporten riktas främst till respektive personuppgiftsansvarig nämnd och ställs till kommunledningen i sin kommunövergripande funktion, men är även aktuell för alla chefer och anställda som direkt eller indirekt arbetar med personuppgifter i kommunen. Rapporterna utgör ett led i kommunens systematiska kvalitetsarbete för att säkra korrekt behandling av personuppgifter.

[1] Art 5.2 dataskyddsförordningen, (hyperlänk i hela dokumentet: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679, 2022-06-29).

DANDERYDS KOMMUN

Innehållsförteckning

1 Inledning

Dataskyddsombudets kvartalsrapport syftar till att hålla de personuppgiftsansvariga nämnderna och kommunledningsgruppen informerade om dataskyddsombudets iakttagelser av kommunens hantering av personuppgifter. Rapporten inleds med dataskyddsombudets berättelse och redovisar därefter statistik om personuppgiftsincidenter, begäran av skadestånd, registerutdrag eller andra rättigheter, tillsyn och sanktionsavgifter samt dataskyddsombudets granskningar av verksamhetens regelefterlevnad.

Det är den personuppgiftsansvariga nämnden som är ansvarig för sin behandling av personuppgifter och bör underrättas om rapportens innehåll i relevanta delar.

För kvartal 2 2023 avses perioden den 1 april - 26 juni 2023. De återstående dagarna i juni får hanteras i rapporten för kvartal 3.

2 Dataskyddsombudets berättelse för kvartal 2 2023

Under denna rubrik redogör dataskyddsombudet för verksamhetens hantering och utveckling, fokusområden, praxis och rättsutveckling samt lämnar aktuell information.

2.1 Behandlingsregistret

Varje personuppgiftsansvarig nämnd ska föra ett register över personuppgiftsbehandlingar som utförs av nämnden, inbegripet förvaltningen.[2] Flera utvecklingsområden har identifierats såsom bristande enhetlighet mellan nämnderna och oklarheter hur kommungemensamma system ska registreras. Huvudkontaktombudet och kontaktombuden arbetar för att få till kommungemensam samsyn och rutiner för hanteringen.

2.2 Dataskyddsombudet om Integritetskyddsmyndighetens rapport om personuppgiftsincidenter år 2022

Integritetsskyddsmyndigheten har i sin personuppgiftsincidentsrapport för år 2022 noterat följande.

- *Den mänskliga faktorn* har de senaste tre åren varit anledningen till cirka 60 procent av alla rapporterade personuppgiftsincidenter.[3]
    - Det medför att verksamheten måste, med tekniska åtgärder som *privacy by design* och ”lätt att göra rätt” i ett säkert system samt organisatoriska åtgärder som framtagande av styrdokument, systemstöd och utbildning – måste fokusera på att *minska riskerna att göra fel* på grund av mänsklig faktor. Skulle man lyckas med detta skulle alltså 3 av 5 personuppgiftsincidenter på generell nivå kunna elimineras.

[2] Jfr. art 30 dataskyddsförordningen.
[3] Rapport om anmälda personuppgiftsincidenter, s. 19, https://www.imy.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2022.pdf (den 14 juni 2023).

- En tillbakagång i *rapporterade personuppgiftsincidenter* på grund av *antagonistiska angrepp*, vilket även kunnat bekräftas utifrån Myndigheten för beredskaps (fortsättningsvis MSB:s) statistik.[4]
    - En möjlig förklaring skulle kunna vara att verksamheter stärkt sina tekniska och organisatoriska åtgärder för att stävja antagonistiska angrepp under krigsåret.
- Det finns indikation på att mörkertalet av personuppgiftsincidenter kan vara tre gånger så många incidenter som för tillfället rapporteras in till Integritetsskyddsmyndigheten.[5]

2.3 Antagonistiska angrepp

En underleverantör av kommunens leverantör av rekryteringssystem har utsatts för ett antagonistiskt angrepp. Detta sker kort efter att trygghetslarmen för äldre utsatts för ett antagonistiskt angrepp vilket skedde i princip samtidigt som kommunens leverantör av transport utsattes för ett antagonistiskt angrepp.

Vad gäller trygghetslarmen har utredningen nu visat att aktören kunnat få obehörig åtkomst till en mycket begränsad mängd uppgifter samt att individer svårligen kunnat identifieras. Personuppgiftsincidenterna gällande rekryteringssystemet och leverantören av transport kommenteras under statistiken om personuppgiftsincidenter.

2.4 Dataskyddsombudets rätt till resurser och oberoende

Det har hänt i några få ärenden att förvaltningschef eller chef, på dataskyddsombudets begäran, inte vill fortsätta utreda granskningar eller incidenter utan hävdar att resurserna ska läggas på annat.

Dataskyddsombudet vill påminna om art 38 p. 2 dataskyddsförordningen stadgar att den personuppgiftsansvarige och personuppgiftsbiträde ska stödja dataskyddsombudet i utförandet av datasskyddsombudets uppgifter genom *att tillhandahålla de resurser som krävs.*

2.5 Överföring mellan löne- och budgetsystem

En tidigare incident i budgetsystemet rörde överföring av en anställds personnummer från lönesystemet till ett budgetsystem. I utredningen till incidenten framkom att hela personnumret regelmässigt fördes över till budgetsystemet. Under utredningen framkom att budgetsystemet behövde få tillgång till födelsedatan för att kunna identifiera storleken på arbetsgivaravgiften, men att de fyra sista siffrorna inte behövde föras över. Sedermera bekräftade verksamheten att man nu fått bukt med detta, så att endast födelsedatan fördes över till budgetsystemet.

---

[4] Rapport om anmälda personuppgiftsincidenter, s. 37, https://www.imy.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2022.pdf (den 14 juni 2023) med vidare hänvisning till MSB:s statistik.
[5] Rapport om anmälda personuppgiftsincidenter, s. 30, https://www.imy.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2022.pdf (den 14 juni 2023).

Vid dataskyddsombudets kontroll hade detta justerats för en typ av rapport, men inte gällande två andra rapporter. Dataskyddsombudet har bett verksamheten att se över detta.

2.6 Flera system på väg fram

Dataskyddsombudet har granskat systemet LifeCare som används av kommun, region och öppen vården, vilket närmare beskrivs under reaktiva granskningar. Dataskyddsombudet vill påtala att flera system över myndighets- och bolagsgränser, som hanterar sekretessbelagda uppgifter samt extra skyddsvärda och känsliga personuppgifter, är på väg fram enligt följande.

- Ungdomsmottagning i app (Storsthlm)
- Sammanhållen vård och omsorgsdokumentation (lagen [2022:913] om sammanhållen vård och omsorgsdokumentation [fortsättningsvis SWOD:en]). (Inera)

Även om i vart fall SWOD:en kompletterar dataskyddsförordningen och personuppgiftsansvaret i vart fall i paragrafform hanteras, identifieras flera liknande obesvarade frågor som vad gäller LifeCare.

2.7 Personuppgiftsbiträdesavtals regleringar om överföring till tredje land

Dataskyddsombudet har vid ett flertal gånger uppmärksammat att kommunen ingått eller planerar att ingå personuppgiftsbiträdesavtal med bestämmelser om överföring till tredje land som denna; ”*datan ska sparas inom EU/EES*” eller liknande.

Dataskyddsombudet vill återigen uppmärksamma att det väsentliga är om leverantören eller dess underleverantörer har *säte i tredje land*, inte var datan är sparad. Har leverantören eller underleverantören säte i tredje land innebär det i regel en otillåten tredjelandsöverföring[6], även om själva datan är sparad inom EU/EES – varför avtalsbestämmelser som den nämnda är otillräckliga för att stävja tredjelandsöverföring.

2.8 Kom ihåg att identifiera och anmäla personuppgiftsincidenter till dataskyddsombudet

Dataskyddsombudet har i årsrapporterna 2022 konstaterat att de nämnder som har många personuppgiftsincidenter också har många granskningar och framför allt vice versa. Huvudkontaktombudet arbetar för att stärka kanaler och utbilda förvaltningarna.

Eftersom det inte finns någon *lägstanivå* för personuppgiftsincidenter bör ett visst antal incidenter kunna förväntas ske varje år, till exempel borttappad mobiltelefon, skickat en e-post till fel mottagare eller att ett

[6] Såvida inte kommunen lyckas uppnå adekvat skyddsnivå för personuppgifterna i det tredje landet. EU-kommissionen har godkänt att vissa länder upprätthåller en sådan skyddsnivå (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en). I övrigt är kraven för att uppnå sådan adekvat skyddsnivå så höga att den är svårt att få till. USA upprätthåller, i dagsläget, inte en adekvat skyddsnivå.

system krånglar på så sätt att verksamheten förlorar tillgången till sina personuppgifter.

2.9 Senaste praxis inom GDPR

- Irlands tillsynsmyndighet har beslutat att tilldela Meta (Facebook) en administrativ sanktionsavgift om ca 14 miljarder SEK. Främst har rättslig grund för överföringen av personuppgifter till tredje land (USA) saknats och standardklausulerna har bedömts inte tillräckliga för att uppnå en adekvat skyddsnivå i det tredje landet. Beslutet har tagits efter en omfattande remissomgång till andra länders tillsynsmyndigheter och European Data Protection Board (EDPB).
- Integritetsskyddsmyndigheten har tilldelat Spotify en administrativ sanktionsavgift om 58 miljoner SEK på grund av att det varit svårt för enskilda att förstå hur deras personuppgifter behandlats och att kontrollera om hanteringen av deras personuppgifter är laglig. Beloppet har bestämts utifrån att allvarlighetsgraden varit *låg*, att Spotify vidtagit flera åtgärder för att tillgodose rättigheterna, antalet registrerade och Spotifys omsättning.

2.10 Fortsätt att bevaka

- Integritetsskyddsmyndigheten granskning av en kommuns användning av Google workspace i skolan.[7]
- Danska tillsynsmyndigheten granskning av Helsingörs kommuns användning av Google workspace i skolan.

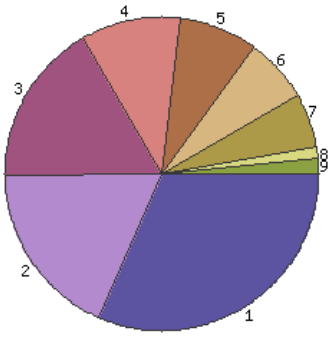
Flera personuppgiftsansvariga nämnder som använder amerikanska molntjänster skulle kunna bli berörda av utgången av besluten ovan.

3 Redovisning av statistik[8]

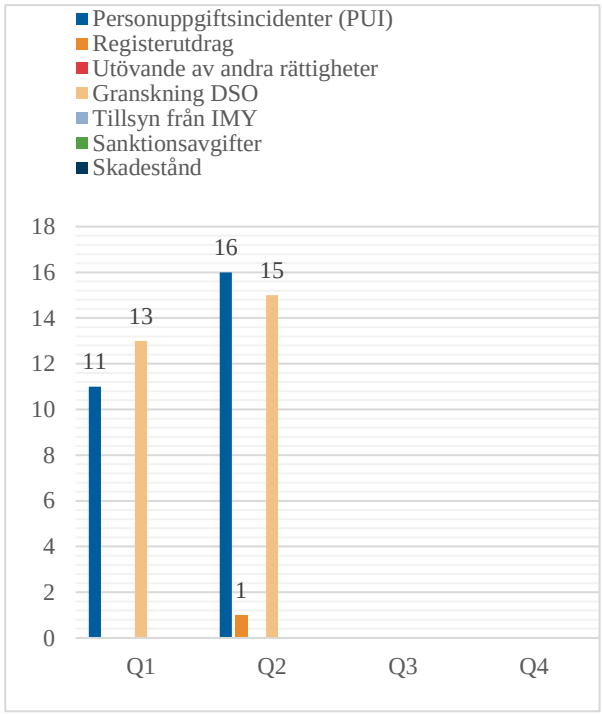
Nedan presenteras statistik för samtliga ärenden som registrerats i systemet för dataskydd under kvartal 2 2023.

[7] IMY-2023-1647

[8] Specificering av kategorier: *Reklam* rör främst erbjudanden om kurser inom dataskydd etc. *Övrigt* rör främst systemuppdateringar. *Underärenden* rör främst en ärendeuppbyggnaden i systemet. Vissa ärenden som skickats in till dataskydd utan ärendekoppling måste ärendekopplas och läggs sen som underärenden för att statistiken ska bli korrekt. *Granskning DSO* rör ärenden där dataskyddsombudet granskar nämndernas efterlevnad av dataskyddslagstiftningen. *PUI* rör personuppgiftsincidenter som anmälts eller kommit till dataskyddsombudet kännedom. *Rådgivning internt* är främst huvudkontaktombudets redskap för intern rådgivning. *IMY* rör främst post eller beslut från Integritetsskyddsmyndigheten gällande anmälda personuppgiftsincidenter. Oftast diarieförs dessa handlingar i verksamhetens system för personuppgiftsincidenten, men ibland skickas de till dataskydd för kännedom. *Rådgivning registrerad* rör främst ärenden där allmänheten ställer frågor till dataskyddsombudet eller huvudkontaktombudet. *Rapporter* rör främst dataskyddsombudets kvartals- och årsrapporter.



	Objekt	Antal ärenden	Antal ärenden (procent)
1	Reklam - Dataskydd	28	31.8
2	PUI	16	18.2
3	Granskning DSO	15	17.0
4	Underärenden	9	10.2
5	Informationssäkerhet	7	8.0
6	Övrigt - Dataskydd	6	6.8
7	Rådgivning internt	5	5.7
8	Reklam och nyhetsbrev	1	1.1
9	Registerutdrag	1	1.1
	Summa	88	100%



3.1 Hur identifieras ett ärende?

Ärenden identifieras genom till exempel anmälningar från leverantör, frågor och anmälningar verksamheten ställt till dataskyddsombudet eller som dataskyddsombudet själv upptäckt i kontakt med verksamheten genom till exempel granskningar, personuppgiftsincidenter och konsekvensbedömningar.

3.2 Personuppgiftsincidenter

En personuppgiftsincident är en incident som leder till *oavsiktlig* eller *olaglig förstöring*, *förlust* eller *ändring* eller till *obehörigt röjande av* eller *obehörig åtkomst till* de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Personuppgiftsincidenten ska anmälas till Integritetsskyddsmyndigheten inom 72 timmar, *såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter*. Personuppgiftsincidenter ska registreras i respektive nämnds diarium.

Under kvartal 2 2023 har 16 personuppgiftsincidenter kommit till dataskyddsombudets kännedom, varav dataskyddsombudet har rekommenderat anmälan till Integritetsskyddsmyndigheten i 8 fall. Vad dataskyddsombudet känner till har rekommendationerna hörsammats i samtliga dessa fall. Av dessa 8 rörde en handfull incidenter en och samma leverantör för transport.

Nedan nämns några personuppgiftsincidenter enligt följande.

- Under slutet av april 2023 inträffade en driftsstörning i kommunens system för rekrytering där också rekryteringshandlingar bevarades i tre år. Några dagar senare framkom att det var fråga om ett antagonistiskt angrepp hos en underleverantör till leverantören.

Angriparna hade lagt en kryptering på servern, vilket medförde att underleverantören stängde av portalen och verksamheten kom därefter inte åt sina personuppgifter (rekryteringshandlingar med mera). Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten, vilket verksamheten ombesörjde.

    - Under slutet av maj 2023 publicerade leverantören en rapport som visade att ett antagonistiskt angrepp skett, att antagonisten navigerat sig runt mellan servrar med full administratörsbehörighet, att det inte finns bevis för att något laddats ned eller kopierats, men att det inte kan uteslutas. Några andra utomstående organ underrättade sina registrerade (arbetssökande) via e-post. Dataskyddsombudet rekommenderade att underrättelse skulle ske på grund av en sannolik hög risk för röjande och en sannolik risk för att uppgifter läckts samt påtalade att en av de grundläggande rättigheterna är att den registrerade ska få information. Verksamheten publicerade en kort informationstext på hemsidan under ”lediga jobb”, vilket får bedömas utgöra mininivå. Verksamheten arbetar fortsatt med ärendet.

- En handläggare hade glömt en genomförandeplan avseende ett barn som placerats på HVB-hem i en av kommunens poolbilar. Handlingen hittades av en anställd i en annan förvaltning. Ingen hade använt bilen under tiden handlingen legat där. Dataskyddsombudet bedömde att händelsen inte behövde anmälas till Integritetsskyddsmyndigheten men påminde verksamheten att se över och informera om rutiner för manuell hantering av handlingar utanför kontoret.

- I samband med hanteringen av en kränkning på en skola har en anställd mejlat elevers vårdnadshavare med information om att namngivna sex elever kränkt en elev. Vårdnadshavarnas e-postadresser har varit synliga för varandra och e-posten har lett till fortsatt mejltråd mellan vårdnadshavare och den anställde, samt även av vårdnadshavare tillagda vårdnadshavare till andra barn. Hanteringen har inte varit konfidentiell eller säker.[9] Det var varken nödvändigt eller relevant att uppge samtliga barns namn, till samtliga barns vårdnadshavare, eller att synliggöra vårdnadshavarnas e-postadresser för varandra. Uppgifterna hade fått oönskad spridning och incidenten är pågående genom fortsatta mejltrådar. Dataskyddsombudet rekommenderade verksamheten att se över sina rutiner för hantering av kränkningar utifrån ett personuppgiftsperspektiv, inbegripet att se till att hanteringen av kränkningen, inte leder till ytterligare kränkningar utifrån berörda elevers fri- och rättigheter. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten, vilket verksamheten ombesörjde.

[9] Jfr. art 5 dataskyddsförordningen.

- Vid kommunens utskick via e-post av infoblad till de som anmält intresse i ett stadsutvecklingsprojekt har ca hundra mottagare fått del av varandras mejladresser, vilket skett av misstag. Dataskyddsombudet bedömde vidare att kommunikationen inte varit konfidentiell eller säker[10] då den skett utanför kommunens miljö men att anmälan till Integritetsskyddsmyndigheten inte behövde göras. Vidare rekommenderade dataskyddsombudet att information om byggnadsprojekt främst borde ske i kommunens egna kanaler, samt att den befintliga e-posthanteringen – även med användandet av dold kopia – innebär en risk för fler personuppgiftsincidenter, då liknande incident även skett vid ett tidigare tillfälle av en annan handläggare.
- Trots att en leverantör av elevhälsans system informerat om att strukna journalanteckningar inte skulle lagras i elevhälsans system, har strukna anteckningar lagrats dolt under perioden den 8 december 2021 – 14 april 2023. Det rör sig totalt om 28 av kommunen skickade (till 15 huvudmän, inbegripet fristående skolor) och 32 av kommunen mottagna strukna journalanteckningar. Danderyds kommuns huvudadministratör ansågs vara betrodd men i och med att kommunen inte har rådighet över andra huvudmäns hantering, rekommenderade dataskyddsombudet att incidenten behövde anmälas till Integritetsskyddsmyndigheten.
- Två av kommunens nämnder använder en och samma leverantör av transport. Efter ett antagonistiskt angrepp under kvartal 1 hos ett av leverantörens underbiträden har verksamheten under kort period anmält över en handfull incidenter vad gäller leverantören. Det handlar om känsliga personuppgifter (hälsa, transport till särskola, korttidsboenden, korttidsvistelser, funktionshinder och särskilda behov vid transport) och extra skyddsvärda personuppgifter (uppgifter om barn, personnummer) som på olika sätt hanterats bristfälligt. Dataskyddsombudet vill understryka att kommunen alltjämt har det yttersta ansvaret i de delar där kommunen är personuppgiftsansvarig för biträdets behandling.

  Incidenterna har huvudsakligen avsett följande.

  - Obehörig åtkomst genom att anställd på kommunen såg ca 40 fler resenärer än hen borde.
  - *Obehörig åtkomst* av personuppgifter vid fakturering dels att resenärer som inte var kommunens fanns med i faktureringsunderlaget, dels att lista med socialnämndens resenärer mejlades till utbildningsnämnden utan kryptering samt parallellt *obehörigt röjande* av socialnämndens personuppgifter på listan.
  - Obehörig åtkomst genom att anställd på kommunen såg ca 500 resenärer fler än hen borde.

[10] Jfr. art 5 dataskyddsförordningen.

- Ytterligare obehörigt röjande vid fakturering.
- Obehörig ändring, förlust och röjande av personuppgifter gällande en resenär.

Dataskyddsombudet har rekommenderat anmälan till Integritetsskyddsmyndigheten för samtliga incidenter. Verksamheten har satt in riktade arbetsträffar (uppdelat i legala- och systemförutsättningar) och utökat dialogen med leverantören för att få till en korrekt hantering. Arbetet har lett till att delar som behörighetskontroll, styrning och gallring bedöms inom kort kunna vara tillgodosedda, medan faktureringsbristerna kräver fortsatt arbete.

3.3 Skadestånd

Den som lidit materiell eller immateriell skada till följd av en överträdelse av dataskyddsförordningen kan begära skadestånd för överträdelsen.

Det har inte kommit till dataskyddsombudets kännedom att något krav på skadestånd riktats mot kommunen under kvartalet.

3.4 Registerutdrag

Den registrerade har rätt att begära ut ett registerutdrag med information om kommunen behandlar personuppgifter om denne och i så fall varför.

Det har kommit in en begäran att få ut kommunens hela behandlingsregister, som får nämnas här. Det har inte kommit till dataskyddsombudets kännedom att någon registrerad begärt ut registerutdrag under kvartalet.

3.5 Andra rättigheter

Utöver de allmänna rättigheterna som till exempel rätt till privatliv, rätt till skydd för personuppgifter, rätt till korrespondens, rätt till effektivt rättsmedel och rättvis rättegång innehåller dataskyddsförordningen flera specifika rättigheter som till exempel rätt till radering, rättelse, invändning och information gällande personuppgifter.

Det har inte kommit till dataskyddsombudets kännedom att någon begäran utifrån registrerades rättigheter inkommit till kommunen.

3.6 Tillsyn och sanktioner av tillsynsmyndighet

Det har inte kommit till dataskyddsombudets kännedom att Integritetsskyddsmyndigheten har genomfört eller annonserat någon kommande tillsyn mot kommunen. Kommunen har inte ålagts att betala någon administrativ sanktionsavgift.

3.7 Påbörjade och planerade granskningar

- Dataskyddsombudet har påbörjat en stor granskning av personuppgiftshanteringen i systemen som används i utbildningsverksamheten. Dataskyddsombudet har fått en kort redogörelse för de system som används. Dataskyddsombudet har ställt verksamheten femton frågor angående tekniska och organisatoriska åtgärder, med svarsfrist den 30 juni 2023. Rapporten

från granskningen beräknas att vara klar under kvartal 3, 2023, såvida underlaget inte behöver kompletteras.

- Dataskyddsombudet planerar på sikt följa upp användningen av samtycke för de nämnder som redovisat brister i behandlingen av personuppgifter med samtycke som rättslig grund vid dataskyddsombudets granskning år 2020.

3.8 Reaktiva granskningar

Dataskyddsombudet övervakar efterlevnaden av dataskyddslagstiftningen och kommunens strategi för skydd av personuppgifter genom granskningar.[11] En granskning kan initieras till exempel genom att verksamheten ställer frågor till dataskyddsombudet om en pågående eller tilltänkt behandling av personuppgifter, att dataskyddsombudet själv uppmärksammar något som bör granskas närmare eller i samband med personuppgiftsincidenter.

Dataskyddsombudet har genomfört 15 reaktiva granskningar under kvartalet bland annat enligt följande.

- I samband med lanseringen av kommunens onboardingportal (utbildningsportal) identifierades en risk för tredjelandsöverföring (som nämndes på leverantörens hemsida, trots att den inte var avsedd enligt pub-avtalet) och att det fanns en möjlighet för anställda att knyta sin utbildningsportal till sina privata sociala medier. Den senare funktionaliteten har tagits bort och support i tredje land har valts bort. Risken för övrig tredjelandsöverföring utreds fortfarande.
- Dataskyddsombudet har gjort en granskning huruvida verksamheten följer den konsekvensbedömning om medarbetare på film och bild på sociala medier, som ledningsgruppen tagit fram. Omfattande dialog har hållits med leverantören av videolösningar för att förstå om publicering av film delas med tredje land eller inte. Slutligen har leverantören tydliggjort att publicering av film *med länk* på sociala medier inte innebär att det sociala mediet får tillgång till innehållet i filmen (mer än själva länken då), medan publicering av film *utan länk eller genom export* av filmen innebär att innehållet delas med det sociala mediet.

  På kommunens sociala medier kunde båda formerna för publicering identifieras och dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten för en film som gällde främst en anställds personuppgifter, samt rekommenderade att den säkrare typen av hantering borde användas för all uppladdning av film på sociala medier. Vid dataskyddsombudets kontroll låg den nämnda filmen utan länk kvar på det sociala mediet nio dagar efter att dataskyddsombudet lämnat rekommendationen att filmen skulle tas bort och anmälas. Dataskyddsombudet har inte fått någon bekräftelse på att personuppgiftsincidenten anmälts till

[11] Art 39.1b dataskyddsförordningen.

Integritetsskyddsmyndigheten, eller att delegationsbeslut om att ej anmäla till Integritetsskyddsmyndigheten har tagits av verksamheten.

- Av lagen (2017:612) om samverkan vid utskrivning från sluten hälso- och sjukvård (fortsättningsvis LUS:en, men kallas även samverkanslagen) framgår att sluten vården, socialtjänsten, kommunalt finansierad hälso- och sjukvård och den regionfinansierade öppna vården ska samverka kring patienter som skrivs ut från sluten vården. Av ett samverkansavtal[12] som ingåtts framgår att samverkan ska ske i ett välfungerade informationssystem/IT-stöd – LifeCare – som tillhandahålls av Region Stockholm. Dataskyddsombudet har granskat hanteringen och noterar bland annat följande.
    - Konsekvensbedömning, utifrån ett kommunperspektiv, saknas och flera dataskyddsfrågor och sekretessfrågor bedöms inte vara tillräckligt utredda eller beslutade. Verksamhetsnyttan har fått visst företräde framför efterlevnaden av bestämmelserna.
    - Enligt information så har kommun och region inte tidigare kunnat komma överens om ett personuppgiftsbiträdesavtal. I det förslag på personuppgiftsbiträdesavtal som regionen genom hälso- och sjukvårdsförvaltningen tagit fram synes regionen utgå ifrån att kommunen huvudsakligen är vårdgivare och därför personuppgiftsansvarig för personuppgiftsbehandlingen i LifeCare. Kommunen är endast vårdgivare i mindre omfattning, till exempel på särskilda boenden i kommunens regi. Eftersom kommunen varken har möjligheter att kontrollera sluten vården eller instruera dem om deras hantering, borde inte kommunen kunna hållas personuppgiftsansvarig för den behandlingen. Kommunen skulle kunna vara personuppgiftsbiträde till slutenvården, eller möjligen någon form att reglerat gemensamt ansvar utifrån samverkanslagen och samverkansavtalet.
    - Systemet möjliggör och förutsätter att kommunen ska skicka anhöriguppgifter i vissa fall samt ange om och vilka insatser[13] patienten har i ett fritextfält i LifeCare. Enligt LUS:en är det dock tillräckligt att *socialnämnden börjar planering av de insatser som är nödvändiga* för utskrivning av patienten[14] – inte att information om vilka insatser som beslutats dessutom ska tillkännages regionen. Detta får effekter för om den tilltänkta personuppgiftshanteringen har en rättslig grund och respekterar principerna, vilket inte verkar ha utretts i tillräcklig omfattning.

[12] Regional överenskommelse om samverkan vid utskrivning från sluten hälso- och sjukvård i Stockholms län, https://vardgivarguiden.se/globalassets/avtal/samverkansomraden/lagen-om-samverkan-vid-utskrivning/om-lag-overenskommelse-riktlinje/regionalovernskommelse2020_samverkan-utskrivning.pdf

[13] enligt socialtjänstlagen (2001:453) eller lagen (1993:387) om stöd och service till vissa funktionshindrade (LSS).

[14] 2 kap. 6 § lagen (2017:612) om samverkan vid utskrivning från sluten hälso- och sjukvård

Uppgifterna om insatser är också sekretessbelagda och en utredning om någon sekretessbrytande bestämmelse kan aktualiseras synes inte ha gjorts.

- Gallringstiden har bestämts till fem år. Systemet är inget journalsystem, utan endast ett informationssystem. Ärendet i LifeCare borde kunna gallras vid inaktualitet eftersom regionen och kommunen har sina egna verksamhetssystem där uppgifterna registreras. Dataskyddsombudet har inte fått svar på frågan hur gallringstiden har bedömts.
- I LifeCare i en senare etapp planeras även att samordnad individuell planering (SIP) ska hanteras och dokumenteras i LifeCare med stöd i 4 kap LUS:en (på öppen vårdens initiativ), men även på kommunens initiativ, mellan region, kommunens hälso- och sjukvård, socialtjänst och öppen vården. Detta komplicerar frågeställningarna ytterligare eftersom öppen vården i dessa fall initierar och torde ansvara för den behandlingen; samt även att LifeCare kan komma att bli ett *gemensamt ärendehanteringssystem* gällande SIP för Region Stockholm, kommuner och ca 3 000 vårdgivare inom öppen vården i länet. Troligtvis krävs identifierade personuppgiftsansvariga för de olika dataflödena.

- Det är obligatoriskt för alla anställda att göra brandskyddsföreningens utbildning. Dataskyddsombudet gjorde år 2022 en granskning av brandskyddsföreningens integritetspolicy, där verksamheten slutligen meddelade att integritetspolicyn inte gällde för kommunens anställda. När utbildningen återigen initierades år 2023 uppmärksammade dataskyddsombudet att de flesta bristerna kvarstod och inledde granskning igen, bland annat med fråga vilka åtgärder verksamheten vidtagit efter granskningen år 2022 för att säkra en korrekt personuppgiftshanteringen. Granskningen beräknas att kunna avslutas under kvartal 3, 2023, såvida verksamhetens svar inte behöver kompletteras.
- Verksamheten har tagit in en funktion för att skicka säker e-post med kryptering. Funktionen har, inte använts av verksamheten och verksamheten anser att kostnaden för tjänsten därför inte är proportionerlig. Verksamheten överväger nu att ta bort funktionen. För socialnämnden ska en annan lösning tas fram och på sikt planeras säker kommunikation på annat sätt för resten av verksamheten.

  Dataskyddsombudet bedömer initialt att i det fall funktionen inte används idag, torde verksamheten i stället vidta ansträngningar för att få verksamheten att använda den säkra funktionen, inte ta bort den. Dataskyddsombudet anser att kommunen måste ha möjligheter att skicka säker e-post. Detta gäller framför allt uppgifter som extra skyddsvärda och känsliga personuppgifter och sekretessbelagda uppgifter på ett säkert sätt. Dataskyddsombudet ser positiv på den på sikt planerade säkra kommunikationen, men bedömer att det finns risker under den period ingen säker kommunikation finns i

kommunen, annat än för socialnämnden. Granskningen beräknas kunna avslutas under kvartal 3, 2023, såvida verksamhetens svar inte behöver kompletteras.

- Den nya hanteringen där lönesystemet ska hämta personuppgifter direkt från Skatteverket har indirekt lett till att anställda, för vilka de själva eller deras föräldrar, inte angett en markering för tilltalsnamn hos Skatteverket kan få ändrade e-postadresser; såsom *AnnaMargaretaKristina.KarlssonSvensson@danderyd.se* samt *Margareta.KarlssonSvensson@danderyd.se* för den som tagit ett mellannamn till exempel efter giftermål. Dataskyddsombudet har inlett granskning av hanteringen, då e-postadresserna framför allt med samtliga namn blir nästintill jämförbara med att ange personnummer i e-postadressen. Granskningen beräknas att kunna avslutas under kvartal 3, 2023.
- Dataskyddsombudet har inlett granskning efter att en ny tjänst för e-böcker på biblioteken visat sig innehålla både profilering, har underbiträden i tredje land samt hanterar sekretessbelagda uppgifter. Granskningen fortsätter.