Dataskyddsombudets rapport

Kvartal 3 2023

Diarienummer	Senast uppdaterad	Beslutsinstans	Processägare
20230227:036	2023-10-04	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).

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 ska underrättas om rapportens innehåll i relevanta delar.

Kvartal 3 2023 avser perioden den 27 juni – 30 september 2023.

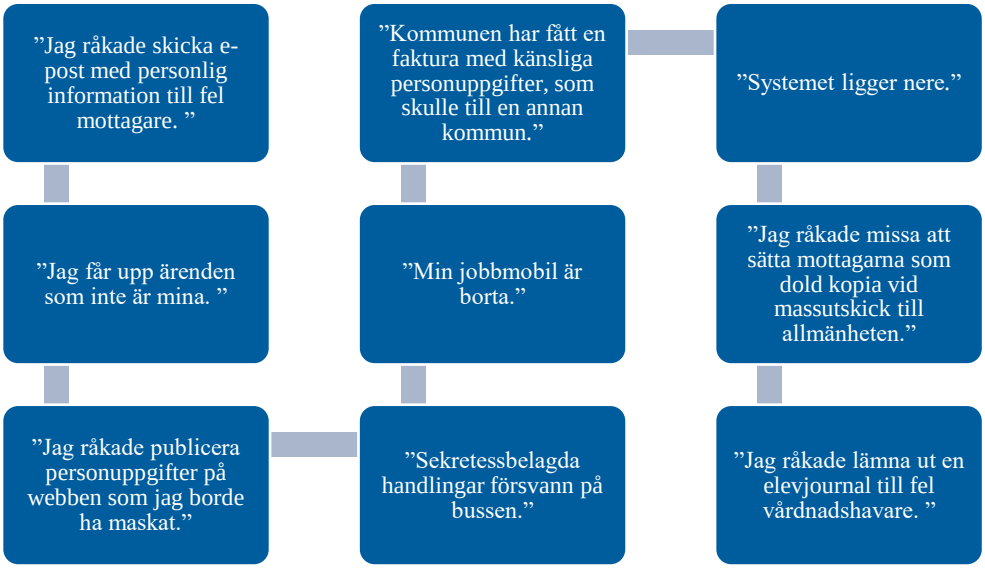
2 Dataskyddsombudets berättelse

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

2.1 Kom ihåg att identifiera och anmäla personuppgiftsincidenter

Kom ihåg att identifiera och anmäla personuppgiftsincidenter till dataskyddsombudet.

Här nedan lämnas exempel på personuppgiftsincidenter som bör anmälas.



Dataskyddsombudet lämnar, efter utredning, rekommendation om incidenten ska anmälas till Integritetsskyddsmyndigheten, och/eller om andra åtgärder bör vidtas.

2.2 *Ramverket* mellan EU och USA

Den 10 juli 2023 har EU-kommissionen antagit ett beslut om adekvat skydd för personuppgifter mellan EU och USA, kallat ”EU-US Data Privacy

Framework", fortsättningsvis *Ramverket*.[2] *Ramverket* ersätter *Safe harbour* och *Privacy shield* som tidigare har upphävts av EU-domstolen.

Dataskyddsombudet har, utifrån *Ramverke*t, tagit fram en promemoria med rekommendationer till verksamheten. Promemorian läggs som bilaga till denna kvartalsrapport, bilaga 2. *Ramverket* har överklagats och kommer att prövas rättsligt.

Dataskyddsombudet rekommenderar återhållsamhet att använda amerikanska molntjänster, trots *Ramverket*, i och med att grundproblematiken med underrättelseinhämtning huvudsakligen består. Kommunen bör fortsätta göra konsekvensbedömningar, försöka undvika att låsa in sig i långa avtal med svårigheter att träda ur, samt att i övrigt följa rekommendationerna i promemorian, bilaga 2.

2.3 Bristande återkoppling från molntjänstleverantör

I två ärenden har dataskyddsombudet genom media fått kännedom om antagonistiska angrepp i Microsofts miljö, varav aktören fått tag på en nyckel vid ett av angreppen. Dataskyddsombudet har haft svårt att få svar på huruvida kommunen drabbats av personuppgiftsincidenter – alltså om kommunens personuppgifter har förstörts, förlorats, ändrats, obehörigen röjts eller kommits åt i samband med detta. Verksamheten har bedömt låg risk för att kommunens personuppgifter har berörts.

- Personuppgiftsbiträdet ska enligt dataskyddsförordningen underrätta de personuppgiftsansvarige (nämnderna) om en personuppgiftsincident har skett utan onödigt dröjsmål.[3] Det är *inte* förenligt med dataskyddsförordningen om biträdet varken kan, eller vill, bekräfta eller dementera om kommunens personuppgifter är berörda, ens på rak fråga. Det är inte heller tillräckligt att hänvisa till generell information på hemsidan.

- I debatten om användningen av amerikanska molntjänster ställs ofta molntjänsternas *gedigna* säkerhet mot de GDPR-bristerna som uppstår med att använda amerikanska molntjänster. Dataskyddsombudet bedömer, något krasst, att ska kommunen använda amerikanska molntjänster, med de GDPR-risker det innebär, med stöd i att molntjänsterna bedöms vara "säkra", så ska de också vara "säkra".

2.4 Uppföljning av incidenter som anmälts till Integritetsskyddsmyndigheten

2.4.1 Läckta personuppgifter från en läroplattform

Elevers personuppgifter från läroplattformen Vklass, som används inom utbildningsverksamheten, hade publicerats på en internetsida i

[2] https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf; läs mer här; https://ec.europa.eu/commission/presscorner/detail/sv/qanda_23_3752, https://ec.europa.eu/commission/presscorner/detail/sv/ip_23_3721, https://ec.europa.eu/commission/presscorner/detail/en/fs_23_3754, den 5 september 2023.
[3] Art 33.2 dataskyddsförordningen.

utpressningssyfte att elever skulle betala för att få sina personuppgifter raderade, vilket vårdnadshavare på annan kommun uppmärksammade i september 2022. Danderyd var en av många kommuner som anmälde incidenten till Integritetsskyddsmyndigheten.

Integritetsskyddsmyndigheten inledde tillsyn mot Vklass och fann att Vklass inte vidtagit lämpliga *tekniska* och *organisatoriska åtgärder* för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Vklass hade inte skyddat personuppgifterna mot obehörigt röjande och obehörig åtkomst samt haft bristande loggningsrutiner.[4] Integritetsskyddsmyndigheten tilldelade Vklass (förvånande nog bara) en reprimand och Vklass förelades att vidta lämpliga *tekniska* och *organisatoriska åtgärder* för att kunna identifiera avvikande händelser och ha spårbarhet i syfte att kunna upptäcka och fastställa incidenters omfattning.[5]

Dataskyddsombudet vill återigen framhålla vikten av att verksamheten vidtar *tekniska åtgärder* som *privacy by design* och *lätt att göra rätt* i säkra system, samt *organisatoriska åtgärder* som framtagande av styrdokument, systemstöd och utbildning.[6]

2.4.2 Antagonistiskt angrepp i rekryteringssystem

En underleverantör av kommunens leverantör av rekryteringssystem Visma Recruit utsattes för ett antagonistiskt angrepp våren 2023. Danderyds kommun med flera anmälde incidenten till Integritetsskyddsmyndigheten.

Integritetsskyddsmyndigheten har beslutat att inte inleda tillsyn av Visma Recruit, men understryker att detta inte innebär att myndigheten har tagit ställning till om företaget brustit i sin hantering av personuppgifter.[7]

Visma har förvärvat Vklass i september 2023.[8]

2.5 Behandlingsregistret

Varje personuppgiftsansvarig nämnd ska föra ett register över personuppgiftsbehandlingar som utförs av nämnden, inbegripet förvaltningen.[9] Huvudkontaktombudet och kontaktombuden har haft en workshop för att få till kommungemensam samsyn och rutiner för hanteringen.

2.6 Kommunens behov av säker och konfidentiell kommunikation

Dataskyddsombudet har noterat att flera personuppgiftsincidenter har haft koppling till e-posthantering under senare tid. Till exempel

---

[4] Jfr. art 32 dataskyddsförordningen.
[5] Integritetskyddsmyndighetens beslut den 24 augusti 2023 i ärende IMY-2022-9092 https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-vklass.pdf.
[6] Jfr. Den mänskliga faktorn har de senaste tre åren varit anledningen till cirka 60 procent av alla rapporterade personuppgiftsincidenter; Rapport om anmälda personuppgiftsincidenter, s. 19, https://www.imy.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2022.pdf, den 14 juni 2023.
[7] https://www.imy.se/nyheter/ingen-granskning-av-visma-recruit/, den 5 september 2023.
[8] https://www.visma.se/nyheter/visma-tar-steget-in-i-den-svenska-skolvarlden---forvarvar-larplattformen-vklass/, den 3 oktober 2023.
[9] Jfr. art 30 dataskyddsförordningen.

- *att* skolor mejlat in information om personer med skyddade personuppgifter till kommunen vid två tillfällen,
- *att* e-postadresser till vårdnadshavare varit synliga vid kommunens mejlutskick rörande ett kränkningsärende på en skola,
- *att* e-postadresser till allmänheten varit synliga vid kommunens massutskick till ca 100 personer,
- *att* kommunen anger e-post som en kontaktväg med klienter med följd att det mejlas in känslig och sekretessbelagd information till kommunen,
- *att* en e-post mellan två handläggare där en klient nämndes med namn och kontaktuppgifter, skickades oavsiktligen till en av kommunens elever, och
- *att* e-postadresser till vårdnadshavare varit synliga vid kommunens mejlutskick inom samma modersmål, vilket indirekt avslöjat etniskt ursprung som utgör en känslig personuppgift.

Detta sammanfaller olyckligt med att kommunen tagit bort funktionen för säker kommunikation. Läs mer på s. 13.

Dataskyddsombudet kan bara understryka att kommunen bör kunna erbjuda allmänheten, klienter och andra aktörer kommunikation och information i säkra och konfidentiella kanaler, och att bristen på detta leder till identifierade personuppgiftsincidenter. Dataskyddsombudet sammanfattar följande.

- E-posthantering i kombination med okunskap, misstag, stress och att förslag på mottagare kommer upp automatiskt i outlook, leder till identifierade personuppgiftsincidenter.
- Särskilt allvarligt är det när e-posten innehåller *sekretessbelagda uppgifter* (till exempel hälsa), *känsliga* (till exempel hälsa, etniskt ursprung) eller *extra skyddsvärda personuppgifter* (till exempel barn, personnummer, integritetskränkande uppgifter).
- En bättre lösning vore om information till allmänheten kunde hanteras i kommunens IT-miljö, hemsida, via e-tjänst eller mina sidor med säker logg in. Korrespondens mellan kommunen, skolor, vårdnadshavare och sinsemellan kommunens verksamheter borde kunna ske i aktuellt och lämpligt system eller i e-tjänst.

2.7 Överföring mellan löne- och budgetsystem

En tidigare incident i budgetsystemet rörde överföring av personnummer från lönesystemet till ett budgetsystem. Brister i överföringen mellan löne- och budgetsystem har huvudsakligen åtgärdats, men fortfarande förekommer hela personnumret i en process. Verksamheten ser över detta.

2.8 På väg mot samsyn vad gäller gemensamt system med regionen…?

Dataskyddsombudet har granskat systemet LifeCare som används av kommun och region (sluten- och öppen vården) för utskrivning av patienter

från sluten vården. Vissa brister har identifierats som det redogjorts för i kvartalsrapport 2 2023.

Positivt är att regionen nu synes tillmötesgå att kommunen enbart är personuppgiftsansvarig för bekräftelse av in- och utskrivningsmeddelande, uppgivande av insatser i LifeCare och kontaktuppgifter. Den större delen av samtliga behandlingar i LifeCare torde därmed sluten- och öppenvården ansvara för. I samverkan med annan kommun och Storsthlm har ett förslag på instruktion lagts fram till regionen.

2.9 Senaste nytt inom GDPR

2.9.1 Profilering

- Integritetsskyddsmyndigheten har utfärdat en administrativ sanktionsavgift mot Bonnier på 13 miljoner kronor, för att koncernen har *profilerat* sina kunder och webbesökare utan deras samtycke. Profileringen har rört sig om att sammanställa köp- och surfbeteenden – som i vissa fall samkörts med kundens kön, bilägande, postnummer, bostadsområde (inbegripet livsfas, köpkraft, boendeform) med mera. Den rättsliga grunden intresseavvägning bedömdes inte hålla för en sådan hantering, varför rättslig grund för behandlingen saknades. I bedömningen av sanktionsavgiftens storlek vägdes in att Bonnier vidtagit omfattande åtgärder för att begränsa intrånget i de registrerades personliga integritet[10].

2.9.2 *Google Analytics*

- Integritetsskyddsmyndigheten har granskat hur Tele 2, CDON, Coop och Dagens industri använt Google Analytics (tredjelandsöverföring med stöd i standardavtalsklausuler) för besöksstatistik på webbsidor. Integritetsskyddsmyndigheten bedömde att inga av bolagens tekniska skyddsåtgärder varit tillräckliga. Ett av bolagen slutade på eget initiativ använda Google Analytics, medan Integritetsskyddsmyndigheten förelade övriga tre att sluta använda Google Analytics. Integritetsskyddsmyndigheten utfärdade en sanktionsavgift på 12 miljoner kronor mot Tele 2 och 300 000 kr mot CDON, vilka vidtagit mindre omfattande skyddsåtgärder än Coop och Dagens industri.[11]

2.9.3 Uppgifter om 650 000 personers hälsa fanns på öppna länkar

- På en offertsida som tillhandahölls av före detta Moderna försäkringar, numera Trygg-Hansa, gick det genom att enbart byta ut

[10] Integritetsskyddsmyndighetens beslut den 26 juni 2023 i ärende DI-2019-11737 https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-bonnier-news.pdf
[11] https://www.imy.se/nyheter/fyra-bolag-maste-sluta-anvanda-google-analytics/; Integritetsskyddsmyndighetens beslut den 30 juni 2023 i ärende DI-2020-11373 https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-ga-tele2.pdf, Integritetsskyddsmyndighetens beslut den 30 juni 2023 i ärende DI-2020-11370 https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-ga-dagens-industri.pdf, Integritetsskyddsmyndighetens beslut den 30 juni 2023 i ärende DI-2020-11368 https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-ga-coop.pdf och Integritetsskyddsmyndighetens beslut den 30 juni 2023 i ärende DI-2020-11397 https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-ga-cdon.pdf.

några siffror i länken, att komma åt 650 000 personers hälsouppgifter. Integritetsskyddsmyndigheten utfärdade en sanktionsavgift på 35 miljoner kronor mot Trygg-Hansa.[12]

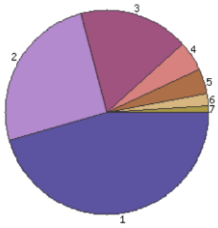
2.10 Fortsätt att bevaka

- Integritetsskyddsmyndigheten granskning av en kommuns användning av Google Workspace i skolan.[13]
- Danska tillsynsmyndigheten granskning av Helsingörs kommuns användning av Google Workspace i skolan.

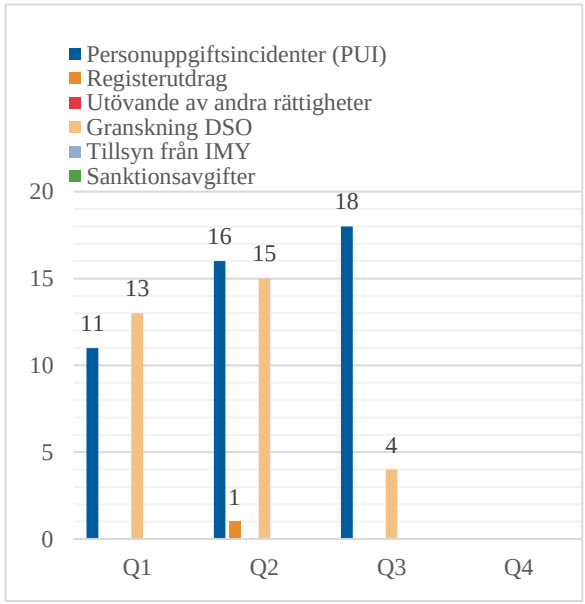
Flera personuppgiftsansvariga nämnder som använder amerikanska molntjänster skulle kunna bli berörda av utgången av besluten ovan. Hur det nyligen antagna *Ramverket* kommer appliceras på satta tillsynsfrågeställningar blir oerhört intressant att följa.

3 Redovisning av statistik[14]

Nedan presenteras statistik för samtliga ärenden som *registrerats* i systemet för dataskydd under kvartal 3 2023. Även ärenden som registrerats vid en tidigare tidpunkt, kan ha avslutats under kvartalet.



	Objekt	Antal ärenden	Antal ärenden (procent)
1	Reklam - Dataskydd	47	45.6
2	Underärenden	26	25.2
3	PUI	18	17.5
4	Övrigt - Dataskydd	5	4.9
5	Granskning DSO	4	3.9
6	Rådgivning registrerad	2	1.9
7	Rådgivning internt	1	1.0
	Summa	103	100%



[12] Integritetsskyddsmyndighetens beslut den 28 augusti 2023 i ärende DI-2021-1905 https://www.imy.se/contentassets/c3ee6b30e5084c598ff5545cd4912055/beslut-efter-tillsyn-enligt-dataskyddsforordningen---trygg-hansa-forsakring-filial.pdf

[13] IMY-2023-1647

[14] 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.

3.1 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.
- Ärenden identifieras genom till exempel personuppgiftsincidents-anmälan 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).

Under kvartal 3 2023 har 18 personuppgiftsincidenter registrerats och kommit till dataskyddsombudets kännedom under kvartalet, varav dataskyddsombudet har rekommenderat anmälan till Integritetsskyddsmyndigheten i 12 fall. Vad dataskyddsombudet känner till har rekommendationerna hörsammats i samtliga dessa fall.

Nedan nämns några personuppgiftsincidenter enligt följande.

- Fortsatta incidenter sker vad gäller obehörig åtkomst och röjande eller ändring av elevers personuppgifter, hos kommunens leverantör för transport, trots att verksamheten har lagt ned mycket arbete för att komma till rätta med problemen. I ett fall meddelade leverantören att felet var löst, trots att personuppgiftsincidenten var pågående. Dataskyddsombudet har lämnat rekommendation om anmälan till Integritetsskyddsmyndigheten i samtliga fall.
- En anställd hade av misstag angett fel kontaktuppgifter till en klient med följd att uppgifter om klientens hälsa och insats mejlades till en privatperson, som svarade att mejlet kommit fel.
    - Oavsett misstaget ovan påtalade dataskyddsombudet att det varken är konfidentiellt eller säkert att mejla uppgifter om hälsa eller insatser, men att klienter olyckligt får den uppfattningen när kommunen anger e-post som en möjlig kontaktväg. Dataskyddsombudet rekommenderade att kommunikation med enskilda för den här typen av uppgifter borde ske i en säkrare miljö än via extern e-post.
- En incident på en förvaltning föranledde att förvaltningen gick upp i stabsläge. Utredning pågår. Aktuell nämnd är underrättad.
- Vid avslut av insats skickades i två ärenden ett meddelande, avsett för aktuell utförare, ut till totalt ca 14 obehöriga kommunanställda och privata utförare i systemet. Personerna behövde logga in i systemet för att få del av uppgifterna. Dataskyddsombudet

rekommenderade anmälan till Integritetsskyddsmyndigheten och att prioritera felsökning och riskminimering.

  - Vad gällde de kommunanställda personerna som fått del av meddelandet är de betrodda handläggare och omfattas av offentlighets- och sekretesslagens bestämmelser, men i och med att de inte haft någon koppling till brukaren borde meddelandet inte ha skickats till dem.
  - Vad gällde de få privata utövare som fått del av meddelandet ska de givetvis inte tillsändas information om brukare som de inte har någon anknytning till, och särskilt inte som rör sekretessbelagda uppgifter.

- Genom intern förebyggande kontroll identifierades att ca 440 av kommunens anställda eller tidigare anställdas e-postadresser och lösenord funnits delvis tillgängliggjorda, med möjlighet till fullt tillgängliggörande digitalt. Verksamheten bytte omgående lösenord för samtliga användare.

  Dataskyddsombudet påtalade

  - *att* omständigheterna kring röjandet och kommande angrepp måste utredas,
  - *att* risker finns för den enskildes fri- och rättigheter när dennes e-post (i tjänsten) och lösenord finns delvis tillgängliga, med möjlighet till fullt tillgängliggörande digitalt, utan att kommunen har kontroll över hanteringen eller kan tillgodose den enskildes rättigheter, till exempel för radering, och
  - *att* anmälan till Integritetsskyddsmyndigheten rekommenderades, att registrerade borde underrättas för att kunna tillvarata sina intressen samt att en påminnelse om att säker lösenordshantering borde skickas ut.

  Verksamheten ombesörjde rekommendationerna.

- I ett system i utbildningsverksamheten lades de nya förskoleklasseleverna in två dagar innan de började förskoleklass, vilket ledde till att befintliga elever kunde ta del av både befintliga och kommande elevers personuppgifter. Incidenten upptäcktes relativt omgående och personuppgifterna för de nya eleverna raderades. Dataskyddsombudet bedömde att incidenten var kortvarig och rekommenderade att rutiner skulle ses över.

- Det uppdagades att medicinska underlag (känsliga personuppgifter) i ärenden om ansökan om handikapparkering inte har sekretessmarkerats i systemet sedan 1,5 år tillbaka. Felet åtgärdades i samband med upptäckt. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten.

- En e-post mellan två handläggare där en klient nämndes med namn och kontaktuppgifter, skickades oavsiktligen till en av kommunens elever. Mejlet återkallades direkt och det bedömdes inte finnas en

sannolik risk för den registrerades rättigheter, varför händelsen inte behövde anmälas till Integritetsskyddsmyndigheten. Dataskyddsombudet rekommenderade två separata AD för elever *kontra* kommunanställda och mottagare på e-post ska skrivas in manuellt, inte komma upp automatiskt.

- En medarbetare har skickat ut information till en grupp vårdnadshavare inom samma modersmål, utan att dölja deras mejladresser för varandra. Genom att den gemensamma nämnaren för vårdnadshavarna var deras barns modersmålsundervisning, finns en risk att kommunen indirekt röjt etniskt ursprung för eleverna och vårdnadshavarna, vilket utgör en känslig personuppgift. Dataskyddsombudet rekommenderade därför en anmälan till Integritetsskyddsmyndigheten, även om förseelsen i övrigt var av lägre allvarlighetsgrad.
- En nyanställd medarbetare kom åt en tidigare anställds löne- och personaluppgifter, när denne loggade in i löne- och personalsystemet. Detta skedde på grund av kommunens beslut att återanvända användar-ID. I och med att den nyanställde ansågs vara betrodd, bedömdes det inte finnas en sannolik risk för den tidigare anställdes fri- och rättigheter och därför krävdes ingen anmälan till Integritetsskyddsmyndigheten. Dataskyddsombudet rekommenderade att gallringsrutiner och beslutet om att återanvända ID behövde ses över.

3.2 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.

3.3 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 inte kommit till dataskyddsombudets kännedom att någon registrerad begärt ut registerutdrag under kvartalet.

3.4 Andra rättigheter

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

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

3.5 Tillsyn och sanktioner av tillsynsmyndighet

Integritetsskyddsmyndigheten kan inleda tillsyn av kommunens personuppgiftshantering, vilket i sin tur kan leda till sanktioner, förelägganden, reprimander med mera.

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.

3.6 Dataskyddsombudets granskningar

Dataskyddsombudet övervakar efterlevnaden av dataskyddslagstiftningen och kommunens strategi för skydd av personuppgifter genom granskningar.[15] 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.

3.6.1 Planerade granskningar

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

I och med den översyn huvudkontaktombud och kontaktombuden gör av behandlingsregistret, bedöms ovan granskning inte behöva göras, i det fall inga eller ytterst få behandlingar med samtycke som rättslig grund kvarstår efter revideringen.

3.6.2 Reaktiva granskningar

Dataskyddsombudet har arbetat vidare med några sedan tidigare registrerade granskningar och har registrerat 4 nya reaktiva granskningar under kvartalet. Två av granskningarna under kvartalet har varit omfattande; promemorian om *Ramverket* (bilaga 2) och granskning av personuppgiftshanteringen i utbildningsverksamhetens system. Nedan nämns några granskningar enligt följande.

- Dataskyddsombudet är i slutskedet av nästan ett års omfattande granskning av personuppgiftshanteringen i utbildnings-verksamhetens system. Nämnden granskas särskilt utifrån personuppgifternas natur, valda systemlösningar, skolors möjligheter till individuella avsteg, bristande gallringsrutiner samt att flera integritetsmyndigheter har inlett tillsyn i utbildningsverksamheten, för vilkas beslut, nämnden måste bevaka och stå rustade inför.

  Granskningen beräknas vara klar inom den närmsta tiden och kommer tillställas den nämnd den berör.

[15] Jfr. art 39.1b dataskyddsförordningen.

- Genom en ny funktion, där lönesystemet kopplar upp till Skatteverket, planerades att initialt 500, sedermera 360 anställda, vars föräldrar inte valt tilltalsnamn för dem hos Skatteverket, eller hade ett mellannamn, skulle få nya e-postadresser hos kommunen innehållande samtliga för-, mellan- och efternamn exempel *AnnaMargaretaKristina.KarlssonSvensson@danderyd.se*.
    - Dataskyddsombudet inledde granskning utifrån ett integritetsperspektiv och noterade att kommunens säkerställande av korrekta personuppgifter, inte borde behöva påverka e-postadressernas typiska utformning. En e-postadress som *ak1@danderyd.se* räckte egentligen för att uppnå ändamålet, digital kommunikation.
    - Vidare borde det vara personliga skäl som föranleder namnändringar hos Skatteverket. Verksamheten ser över hanteringen.
- Dataskyddsombudet har granskat en konsekvensbedömning om videoinspelning av handläggare vid klientsamtal inom familjeterapi – för målgruppen familjer med barn elva till arton år vilka visar ett utagerande beteende, bråkar, har begått brott, skolkar eller missbrukar – i utbildningssyfte. Familjerna kan tacka ja eller nej till ljudupptagningen.

  Dataskyddsombud såg ingen oförenlighet med dataskyddsförordningen att filma handläggaren med ljud och bild under de premisser med förvaring, lösenord och radering som lagts fram samt uppspelning av densamma i grupp med handläggare i andra kommuner i utbildningssyfte.

  Däremot avrådde dataskyddsombudet för ljudupptagning av klienters (inbegripets barns) autentiska berättelse om privat- och familjeliv, missbruk, diagnoser, brott, psykiskt och fysiskt mående etcetera, samt uppspelning i grupp med handläggare i andra kommuner. Behandlingen ansågs inte nödvändig, och dessutom avsåg behandlingen *känsliga personuppgifter* (hälsa, diagnoser, missbruk) och *extra skyddsvärda personuppgifter* (barn, brott, integritetskänsliga uppgifter).

  Barn, fram för allt i dessa fall, bedöms särskilt sårbara och har, utifrån sina förutsättningar, ännu mindre möjligheter att hävda och värna sin integritet. Dataskyddsombudet identifierade också en risk för att sekretesskyddade uppgifter skulle kunna röjas till handläggare i andra kommuner.[16]
- Verksamheten har tagit bort en funktion för att skicka säker e-post med kryptering, då kostnaden inte funnits proportionerlig i och med att ytterst få använt funktionen. Borttagandet skedde mot dataskyddsombudets rekommendationer. Dataskyddsombudet anser att kommunen måste ha möjligheter att skicka säker e-post, och att kommunen i stället borde arbetat med implementering av

[16] 21 kap. 1 § offentlighets- och sekretesslagen (2009:400).

funktionen. Se avsnitt 2.6. Granskning pågår och ärendet har behövt kompletteras av verksamheten.

- Dataskyddsombudet har inlett granskning efter att en ny tjänst för e-böcker på biblioteken visat sig innehålla profilering, har underbiträden i tredjeland samt hanterar sekretessbelagda uppgifter. Se avsnitt 2.9.1 om sanktionsavgiften mot Bonnier för profilering. Dataskyddsombudet väntar på svar från verksamheten.

Bilagor
1. Dataskyddsombudets kvartalsrapport 3 2023 (denna)
2. Dataskyddsombudets PM med rekommendationer efter adekvansbeslutet *EU-US Data Privacy Framework*