Dataskyddsombudets årsrapport 2024 för Danderyds kommun

Diarienr.	Senast	Beslut	Processägare
20240516:098	*2025-02-27*	*Dataskyddsombud*	*Dataskyddsombud*

Dokumentets syfte

Denna rapport har tagits fram av Danderyds kommuns dataskyddsombud för år 2024. Rapporten tas fram för att respektive nämnd ska kunna ta sitt personuppgiftsansvar och redovisa sin efterlevnad av dataskyddsförordningen, vilket dataskyddsförordningen kräver.[1]

Dokumentet gäller för

Rapporten riktas främst till de personuppgiftsansvariga nämnderna, kommunledningen och verksamheterna, inbegripet alla chefer och anställda som direkt eller indirekt arbetar med personuppgifter i kommunen.

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

Innehållsförteckning

1. Inledning

Dataskyddsombudet (jag) vill inleda med att tacka Danderyds kommun för ett fint år och för allt utfört GDPR-arbete.

Dataskyddsförordningen (GDPR)[2] sätter ramarna för hur kommunen får behandla personuppgifter, utifrån de fri- och rättigheter personen har. Denna rapport syftar till att vara ett stöd för att de personuppgiftsansvariga nämnderna, för att de ska kunna ta sitt personuppgiftsansvar och redovisa sin efterlevnad av dataskyddsförordningen, vilket är vad dataskyddsförordningen kräver (*ansvarsskyldigheten*).[3] Av dataskyddsförordningen framgår att nämnderna ska säkerställa att dataskyddsombudet inte tar emot instruktioner, avsätts eller utsätts för sanktioner, för att ha utfört sina uppgifter.[4]

I denna årsrapport redovisas information om statistik och omvärlds-bevakning för år 2024. Rekommendationer lämnas löpande. Årsrapporten avser perioden den 1 januari – 31 december 2024.

2. Vilka regler gäller för dataskydd

I kommunen är nämnderna personuppgiftsansvariga för sin behandling av personuppgifter. Den personuppgiftsansvarige nämnden bestämmer *ändamål* och *medel* för behandling av personuppgifter och kan tilldelas administrativa sanktionsavgifter vid bristande regelefterlevnad.[5] I detta avsnitt ges en kort introduktion av gällande rätt.

- Behandlingen av personuppgifter är endast laglig och tillåten om det finns en *rättslig grund* för behandlingen. Personuppgiftshanteringen måste ha någon av följande rättsliga grunder.[6]
    - Samtycke (ska i regel inte användas av kommun[7])
    - Avtal
    - Rättslig förpliktelse
    - Skydda grundläggande intressen (ska i regel inte användas av kommun[8], kan möjligen vara aktuellt i de fall där kommunen är vårdgivare)
    - Myndighetsutövning och uppgift av allmänt intresse
    - Intresseavvägning (ska i regel inte användas av kommun[9])

[2] Begreppet dataskyddslagstiftningen kan också användas, och avser då dessutom annan lagstiftning som avhandlar hanteringen av personuppgifter.
[3] Art. 5.2 och art. 38.3 dataskyddsförordningen.
[4] Art. 38.3 dataskyddsförordningen.
[5] Jfr. art. 4.7 och 83 dataskyddsförordningen.
[6] Art. 6 dataskyddsförordningen.
[7] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/samtycke/, bevittnat den 30 april 2024.
[8] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/skydda-grundlaggande-intressen/, bevittnat den 30 april 2024.
[9] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/intresseavvagning/, bevittnat den 30 april 2024.

- Vidare ska personuppgiftshantering ske enligt *principerna* i dataskyddsförordningen. Principerna innebär att personuppgifter ska hanteras enligt följande.[10]
    - Behandlas på ett lagligt, korrekt och transparent sätt
    - Samlas in för ett angivet ändamål
    - Ska vara relevanta och så få som möjligt
    - Ska vara korrekta
    - Får inte möjliggöra identifiering längre än nödvändigt
    - Ska behandlas på ett säkert och konfidentiellt sätt, med beaktande av integritet
- Medborgare inom Sverige och EU är tillerkända flera *fri- och rättigheter*, vissa av dem grundlagsstadgade, vilka måste följas vid behandling av personuppgifter, till exempel följande.
    - All maktutövning ska vara grundad på lag eller föreskrift, se 1 kap. 1 § 3 st. regeringsformen. Den offentliga makten ska utövas med respekt för alla *människors lika värde* och för den enskilda *människans frihet och värdighet*, jfr. 1 kap. 2 § 1 st. regeringsformen. Det allmänna ska *värna* den enskildes privatliv och familjeliv enligt 1 kap. 2 § 4 st. regeringsformen.
    - Av 2 kap. 6 § 2 st. regeringsformen följer att var och en gentemot det allmänna är skyddad mot *betydande intrång i den personliga integriteten* som sker utan samtycke, och som innebär *övervakning* eller *kartläggning av den enskildes personliga förhållanden*. För att kommunen ska få vidta sådana åtgärder krävs lagstöd enligt 2 kap. 20 § regeringsformen.
    - Grundlagsstadgade friheter som yttrandefrihet, fri åsiktsbildning, religionsfrihet, informationsfrihet, föreningsfrihet och mötesfrihet.[11]
    - Respekt för privat- och familjeliv (kommunikation), fri rörlighet, skydd av personuppgifter och rätt till effektivt rättsmedel och rättvis rättegång.[12]
- Den person vars personuppgifter behandlas tillerkänns flera specifika rättigheter i dataskyddsförordningen vilka alltid måste beaktas vid behandling av personuppgifter, till exempel rätten enligt följande.[13]

---

[10] Jfr. art. 5 dataskyddsförordningen.
[11] Jfr. 2 kap. 1 § regeringsformen.
[12] Jfr. bl.a. art. 6, 8 och 13 lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna och art. 7, 8 och 47 Europeiska unionens stadga om de grundläggande rättigheterna, https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:12012P/TXT, bevittnat den 30 april 2024.
[13] Kapitel 3, avsnitt 3-4 dataskyddsförordningen.

- *Att* begära rättelse.
- *Att* få ta del av sina uppgifter.
- *Att* få information.
- *Att* begära begränsning av hur personuppgifterna sprids.
- *Att* få invända mot hur personuppgifterna behandlas.
- *Att* få sina personuppgifter flyttade (portabilitet) i vissa fall.

En *personuppgiftsincident* innebär en oavsiktlig eller olaglig händelse som leder till *förstöring, förlust, ändring, obehörigt röjande eller obehörig åtkomst av personuppgifter*.[14] Vid en personuppgiftsincident *ska* den personuppgiftsansvarige utan onödigt dröjsmål och i regel inom 72 timmar, *anmäla* incidenten till tillsynsmyndigheten, om det *inte* är *osannolikt* att personuppgiftsincidenten medför *risk* för *personers fri- och rättigheter*.[15] Faktisk skada krävs inte.

3. Dataskyddsombudets årsberättelse

År 2024 har varit ett innehållsrikt år, där antagonistiska angrepp fortsätter öka, och artificiell intelligens (AI) fortsätter att utvecklas, vilka båda, har sina respektive utmaningar.

3.1 Antagonistiskt hot

Statistik visar att cyberattacker ökat med 75 procent globalt och med 165 procent i Sverige, i jämförelse med motsvarande kvartal senaste året. Särskilt utsatta branscher är utbildning, forskning, myndigheter, militär och hälso- och sjukvård.[16] Myndigheten för samhällsskydd och beredskap (MSB) har varnat för att det pågår en nätfiskekampanj mot kommuner och skolor. [17] Mejlen kan vara välformulerade, se ut att komma från en chef eller medarbetare och även ha relevant innehåll för chefens/medarbetarens eller ens egna arbetsuppgifter, men innehåller infekterade länkar och filer. Det som riskerar att ske är att antagonisten kommer över information som kan användas för bedrägerier, cyberbrottslighet, utpressning mot bolag och individer. MSB rekommenderar att motringa när en kollega delat en fil samt att varna andra om man drabbas. Se *länk i fotnot* för generella råd och snabbkurser.[18]

Flera kommuner, till exempel Kumla kommun[19] har utsatts för antagonistiskt angrepp år 2024, blivit utpressade och fått sin data publicerad

[14] Jfr. art. 4.12 dataskyddsförordningen.
[15] Art. 33 dataskyddsförordningen.
[16] https://www.aktuellsakerhet.se/rapport-cyberattacker-i-sverige-okar-med-165-procent/, bevittnat den 5 december 2024.
[17] https://www.cert.se/2024/06/pagaende-natfiskekampanj-riktad-mot-kommuner-och-skolor.html, bevittnat den 11 december 2024.
[18] Generella råd här: https://www.cert.se/tema/natfiske. Snabbkurser finns här: https://internetkunskap.se/snabbkurser/.
[19] https://www.kumla.se/kommun-och-politik/nyheter/viktigt-meddelande/2024-11-04-kumla-kommun-utsatt-for-cyberangrepp.html och https://www.aftonbladet.se/nyheter/a/yE9Exa/kommun-pressas-pa-pengar-efter-cyberattack bevittnat den 5 december 2024.

på dark web. Kumla kommun har på ett till synes transparent sätt, redovisat sina åtgärder och utmaningar, se *länk i fotnot*.[20]

Trots allt detta, noterar jag, att anmälda personuppgiftsincidenter som skett i samband med antagonistiska angrepp, under året, endast varit någon enstaka i Danderyds kommun. Förhoppningsvis rör det sig om att verksamheten och dess leverantörer har kunnat upprätthålla en hög säkerhetsnivå. Ett febrilt sådant arbete pågår hos många av de stora leverantörerna och kommunerna. I värsta fall, kan finnas ett mörkertal av antagonistiska angrepp eller obehörigt röjande, som varken upptäckts eller anmälts. Här vill jag skicka med att nämnderna måste fortsätta att vara observanta, arbeta förebyggande och hålla en hög skyddsnivå. Ett sätt att hålla en hög skyddsnivå är att upphandla samt teckna personuppgiftbiträdesavtal på ett GDPR-smart sätt.

3.2 Identifiera sårbarheter

Jag fortsätter på temat med att identifiera sårbarheter, där FBI varnat för att använda SMS (som utgör okrypterade textmeddelanden) eftersom det kan leda till identitetsstöld, ekonomiska förluster och utpressning, om uppgifterna koms över.[21] Under hashtagen *#Stravaleaks*, har rapporterats att Joe Biden, Donald Trump och Emanuel Macron kan ha kartlagts via sina livvakters träningsapp, som alltså identifierat var livvakterna, och därmed också skyddspersonen, uppehållit sig.[22] En före detta Apple-chef har stämt Apple för att övervaka anställda på arbetsplatsen och *hemmakontoret*. Medarbetarnas sökhistorik och data från andra enheter som varit kopplade till samma Apple-ID, oavsett om enheten används av den anställde eller en familjemedlem, hämtades in av arbetsgivaren.[23] Det har också rapporterats att ca 100 000 akter årligen, ibland på hundra sidor per akt, laddats ned från Lantmäteriets öppna arkiv, utan att sekretessprövning gjorts.[24] I en tid där allt ska lösas snabbt eller via ett fåtal *klick*, vill jag understryka att det gäller att inte jäkta fram, utan att verkligen se till att ha den juridiska analysen

---

[20] Länk till att Kumla kommun har på ett till synes transparent sätt, redovisat sina åtgärder och utmaningar https://www.kumla.se/kommun-och-politik/nyheter/viktigt-meddelande/2024-11-04-kumla-kommun-utsatt-for-cyberangrepp.html.

[21] https://www.dagensps.se/privatekonomi/sakerhet/fbi-darfor-ska-du-sluta-skicka-sms/, bevittnat den 9 december 2024.

[22] https://omni.se/biden-och-trump-kan-ha-kartlagts-via-traningsapp/a/Av09Ex och https://www.lemonde.fr/societe/article/2024/10/27/comment-suivre-a-la-trace-emmanuel-macron-decouvrez-le-premier-episode-de-notre-enquete-stravaleaks_6361677_3224.html, 3 avsnitt, bevittnat den 5 december 2024.

[23] https://finance.yahoo.com/news/current-apple-employee-suing-company-191704182.html?guccounter=1&guce_referrer=aHR0cHM6Ly9vbW5pLnNlLw&guce_referrer_sig=AQAAAAfSAacPJwAaDPeM6h-XiwnWBZOkJh3l5Jq30LTvXEREpGce_jKW59V0bCzP6KE_HYOOOKN7R2xx52T7bckCkirgTIzuzUm1nMKDjnnJuEbvD8PoeawMxkzcGowVGNnnyu8Pa_apMH64PHb0WiipFz5AxjCIa-oRgtLb0KjjR-Ac och https://omni.se/ny-stamning-mot-apple-overvakar-anstallda/a/jQgLXo, bevittnat den 5 december 2024.

[24] Expressens granskning. https://www.expressen.se/nyheter/sverige/chefen-stoppade-inte-lacka-trots-larm-om-forsvarshemligheter/, bevittnat den 9 december 2024. Läs mer här: Lantmäteriets egen information: https://www.lantmateriet.se/sv/om-lantmateriet/press/nyheter/lantmateriet-begransar-tillgangen-till-viss-information-i-ett-antal-digitala-tjanster-pa-grund-av-sakerhetsskal/.

gjord och dokumentationen på plats. Tumma inte på de rättsliga kraven. Erbjuds en tjänst eller app gratis, har den sannolikt *ett pris*.

En svensk forskare har fått internationell uppmärksamhet, för att ha påtalat att våra digitala rättigheter endast gäller så länge vi lever, och att *den första digitala generationen* på omkring två miljarder människor inom trettio år kommer att dö. *Den* som kommer ha kontrollen över deras personuppgifter (vårt kollektiva digitala förflutna, våra *öden*) kommer få stor politisk makt, vilket behöver bemötas med ekonomiska och tekniska system, utöver det monetära värdet av de digitala resterna, menar författaren.[25] Med detta vill jag förmedla, att var medveten om att personuppgifter har ett värde, nu och senare, på individuell och övergripande nivå.

3.3 Artificiell intelligens

På temat att vara vaksam och medveten har AI-förordningen[26] börjat gälla den 1 augusti 2024 och träder ikraft allteftersom. Läs mer om AI i avsnitt 4.

Trots all *hajp* kring AI, visar en riksomfattande undersökning att andelen positiva till AI är på fortsatt rekordlåg nivå i Sverige. Varannan person oroar sig för att AI ska ta felaktiga beslut. Fyra av tio oroas av att AI ska göra intrång i den personliga integriteten. Endast hälften ser arbetsmöjligheter med AI och sex procent känner sig hotade av att bli ersatta av AI.[27]

Det finns tendenser att begränsa AI, till exempel har det amerikanska representanthuset beslutat att förbjuda användningen av *Copilot* eftersom *Copilot* kan läcka data till molntjänster. Användningen av *ChatGPT* var där sedan tidigare begränsad.[28] Det finns också alarmerande berättelser om hur så kallade *AI-vänner* mordhotat tonåringar och förespråkat självskadebeteende.[29] Ett AI-resultat utgör ett resultat av den data som AI:en tränats på. Ju mer kvalitativ, omfattande och korrekt datan är, desto bättre blir AI:ens slutprodukt. Ju sämre, missvisande eller oviktad datan är,

---

[25] Carl Öhman, *The Afterlife of Data: What Happens to Your Information When You Die and Why You Should Care*, och https://www.unt.se/kultur/litteratur/artikel/uppsalaforskaren-skrev-en-av-arets-mest-omtalade-bocker-/ly4qvezl.

[26] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens); https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202401689&qid=1733995100656 (hyperlänk i hela dokumentet).

[27] https://www.imy.se/nyheter/allt-fler-oroas-over-att-ai-gor-intrang-i-den-personliga-integriteten/, bevittnat den 5 december 2024.

[28] https://techlaw.se/varlden-usas-kongress-forbjuder-microsoft-copilot-pa-grund-av-cybersakerhetsrisker/.

[29] https://www.tv4.se/artikel/4L8ZeZNWEOvXO4n61Xi4G6/se-den-fullstaendiga-chatten-med-ai-vaennen, bevittnat den 5 december 2024 och https://www.bbc.com/news/articles/cd605e48q1vo och https://www.npr.org/2024/12/10/nx-s1-5222574/kids-character-ai-lawsuit, bevittnat den 12 december 2024.

desto större risk för brister i slutprodukten. Det är ofta i dessa senare sammanhang som det identifieras brister i AI:ns slutprodukt.

Vi ser också andra konsekvenser av AI. En bedragare lyckades, utifrån en tidigare inspelad videokonferens, skapa artificiella karaktärer (*deepfakes*) av en medarbetares chefer och lurade medarbetaren att betala ut 25 miljoner dollar.[30] AI förändrar även vårt språk. Användningen av vissa sällsynta engelska ord, som *delve, intricate, tapestry och leverage*, har ökat med 200-300 procent i uppsatser vid svenska och utländska universitet. Detta då arbetskraft i Nigeria (där de sällsynta engelska orden förekommer mer frekvent) tränar AI-funktionen.[31] Regeringen har gett Mediemyndigheten i uppdrag att stärka medborgarnas kunskap mot AI-driven desinformation och förmåga att vara källkritiska.[32] Å andra sidan, har *Integritetsskydds-myndighetens regulatoriska sandlåda* utrett möjligheten att automatisera processen för utlämnandet av allmänna handlingar och funnit att AI kan bistå med maskning under vissa förutsättningar. Vikten av mänsklig kontroll och kvalitetssäkring (*a human in the loop*) betonas.[33] Med detta vill jag säga att AI är ett effektivt och användbart hjälpmedel. Men det är just det, ett *hjälpmedel*. Det gäller att inte ha en *övertro* till AI:ns intelligens och förmåga. Slutprodukten måste faktagranskas och kvalitetssäkras av en faktisk person. Användningen av AI:n måste också följa samtliga gällande lagar och regler samt behöver säkras utifrån AI-förordningen och dataskyddsförordningen. En vanlig missuppfattning tycks också vara att användningen av AI kommer minska kommunens personalkostnader, när det egentligen kan krävas att kommunen behöver anställa svårrekryterad AI-, IT- och IT-juridiskt kunnig personal som klargör ramarna för AI:n och håller AI:n i schack.

Med denna ingress, vill jag tacka för ett fint år 2024 och jag ser med spänning fram emot år 2025.

---

[30] https://techlaw.se/varlden-medarbetare-luras-pa-25-miljoner-dollar-av-ai-fejkade-kollegor-i-videosamtal/.

[31] https://www.sydsvenskan.se/2024-12-02/sydsvenskan-avslojar-robotar-hjalper-studenter-att-skriva-uppsatser/; bevittnat den 9 december 2024. https://www.theguardian.com/technology/2024/apr/16/techscape-ai-gadgest-humane-ai-pin-chatgpt och https://omni.se/ai-forandrar-spraket-pa-svenska-universitet/a/nyBw4B, bevittnade den 2 december 2024.

[32] https://www.regeringen.se/pressmeddelanden/2024/03/mediemyndigheten-ges-i-uppdrag-att-genomfora-nationell-satsning-for-starkt-medie--och-informationskunnighet-inom-ai-driven-desinformation/.

[33] Integritetsskyddsmyndighetens rapport *Utlämnande av allmän handling med hjälp av AI*, ärende IMY-2024-5156, den 7 november 2024; https://www.imy.se/globalassets/dokument/rapporter/utlamnande-av-allmanna-handlingar-med-hjalp-av-ai.pdf och https://www.imy.se/nyheter/ai-kan-forenkla-sekretessbedomningar-av-allmanna-handlingar/. // Helhetslösningen visade sig innehålla tekniska och juridiska hinder, varför projektet begränsad till att tjänsten ska identifiera och ge förslag på uppgifter som ska maskeras i en allmän handling.

4. Mer om AI

Syftet med AI-förordningen är att skapa en trygg och etisk hållbar miljö för AI-innovation, samtidigt som personers fri- och rättigheter skyddas.[34] En AI klassificeras baserat på systemets risker för samhället och personers fri- och rättigheter, enligt följande.

AI med oacceptabel risk. Typexempel är AI som manipulerar människors beteende och utnyttjar människors sårbarheter. Denna typ av AI är förbjuden.[35]

AI med hög risk. Typexempel är AI som utför ansiktsigenkänning på distans och utvärderar kandidater för rekrytering, krediter eller liv- och sjukförsäkring samt AI-system kopplade till rättskipning, brottsbekämpning, kritisk infrastruktur och migration. AI-förordningen ställer här en mängd strikta krav.[36]

AI med systemrisk och begränsad risk. Typexempel är AI som interagerar med människor, ChatGPT, chatbotar och AI som genererar texter och bilder (*deepfake*). AI-förordningen ställer vissa krav. Transparens krävs.[37]

AI med minimal risk. Typexempel är spel. Dessa system omfattas inte av AI-förordningen, men måste hållas under kontroll.[38]

Dataskyddsförordningen gäller parallellt med AI-förordningen. Även offentlighets- och sekretesslagen (2009:400), arkivlagen (1990:782), cybersäkerhetslagen, förvaltningslagen (2017:900) och kommunallagen (2017:725) och andra aktuella regelverk gäller. Vid utveckling av AI gäller det alltså att ha tillräcklig kunskap om de juridiska ramarna för vad som är tillåtet.

Vid utvecklingen av AI gäller det att definiera i vilken AI-kategori kommunen befinner sig, vilka regler som då gäller samt att följa reglerna och följa upp.

Glöm inte, att personuppgifter endast får behandlas för ett bestämt ändamål och om rättslig grund finns.[39] Att personuppgifter i ett sammanhang används (för ett ändamål), innebär alltså inte att samma uppgifter automatiskt får användas för att träna en AI. Se till att ha tillräckligt med kompetens (personal), resurser, digitala förutsättningar och kvalitativa data, för att utveckla och använda en AI. Dokumentera juridiska, säkerhetsmässiga och etiska överväganden och vidta tekniska, organisatoriska och riskminimerande åtgärder.

[34] Art. 1 AI-förordningen.
[35] Art. 5 AI-förordningen.
[36] Art. 6, bilaga 1 och 3 AI-förordningen.
[37] Art. 50-55 AI-förordningen.
[38] Art. 95 AI-förordningen.
[39] Jfr. art. 5-6 dataskyddsförordningen.

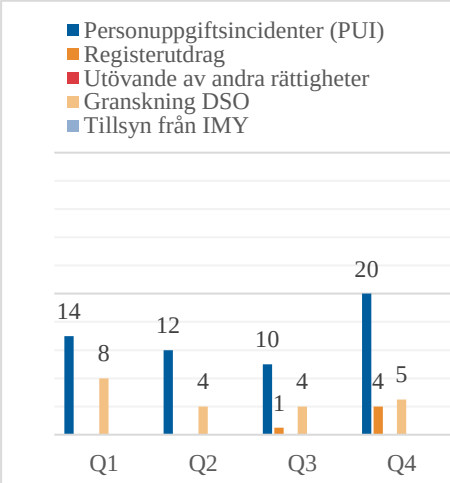
5. Statistik år 2024

Under detta avsnitt presenteras statistik för Danderyds kommun år 2024.

Kategorierna innebär följande.

- *Reklam* rör främst erbjudanden om kurser inom dataskydd etc. Ärendena diarieförs på kommunstyrelsen.
- *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.
- *Övrigt* rör sådana mejl som inte hör hemma under någon annan kategori. Positiv återkoppling på information om personuppgiftshanteringen på webben placeras här och politiska beslut som skickas in till dataskyddsombud för kännedom, men som inte genererar ett eget ärende.
- *Rådgivning internt* är främst dataskyddssamordnarens kategori för intern rådgivning. Intern rådgivning sker framförallt i det löpande dataskyddsarbetet, utanför detta system.
- *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	215	56.3
2	PUI	56	14.7
3	Övrigt - Dataskydd	40	10.5
4	Underärenden	27	7.1
5	Granskning DSO	21	5.5
6	Rådgivning internt	12	3.1
7	Registerutdrag	5	1.3
8	Återkoppling på hemsida	3	0.8
9	Rådgivning registrerad	2	0.5
10	Rapporter	1	0.3
	Summa	382	100%



5.1 Behandlingsregistret

Av art. 30 dataskyddsförordningen framgår att varje personuppgiftsansvarig nämnd *ska föra ett register över sina personuppgiftsbehandlingar*. Ett exempel på en personuppgiftsbehandling kan vara rekrytering och bokföring.

Av skäl (82) dataskyddsförordningen framgår att registret ska tjäna som en kontrollpunkt för tillsynsmyndigheten.

Danderyds kommun har 677 registrerade behandlingar av personuppgifter, varav 128 utgör *kommungemensamma behandlingar*, 167 rör *kommunstyrelsen*, 68 rör *utbildningsnämnden*, 31 rör *kultur- och fritidsnämnden*, 33 rör *tekniska nämnden*, 182 rör *socialnämnden*, 8 rör *valnämnden*, 13 rör *överförmyndarnämnden* och 47 rör *miljö- och stadsbyggnadsnämnden*. Därutöver finns 13 registrerade behandlingar som

rör *byggnadsnämnden*, vilka kommer arkiveras i samband med byte av system.

Detta kan jämföras med tidigare uppgifter enligt följande.

- Danderyds kommun hade 587 registrerade behandlingar av personuppgifter år 2023, och,
- 666 registrerade behandlingar i juni 2024.

Framförallt har *kommunstyrelsens* registrerade behandlingar renodlats och kommungemensamma behandlingar registreras idag för sig, vilket lett till en sammantagen ökning av antalet registrerade behandlingar. Under senare halvåret 2024 är det främst *tekniska nämnden* som registrerat nya behandlingar.

En rättsakt i form av ett reglemente, som ska fastställa nämndernas inbördes förhållanden vid gemensamt personuppgiftsansvar, och interna biträdesrelationer, har arbetats fram under året, och avses att beslutas under våren 2025. Ett nytt system för registrering av behandling av personuppgifter har upphandlats under året.

5.2 Granskningar

Dataskyddsombudet övervakar efterlevnaden av dataskyddslagstiftningen och kommunens strategi för skydd av personuppgifter genom *granskning*.[40]

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 inträffade personuppgifts-incidenter.

Dataskyddsombudet har under året utfört 21 granskningar och lämnat rekommendationer.

Detta kan jämföras med tidigare års granskningar enligt följande.

	Svarsalternativ	Antal ärenden	Antal ärenden (procent)
1	Kommunstyrelsen	12	57.1
2	Utbildningsnämnden	7	33.3
3	Socialnämnden	2	9.5
	Summa	21	100%

- 40 granskningar år 2023
- 44 granskningar år 2022

Nämnder som inte nämns har haft *0* granskningar.

Antalet granskningar har halverats i jämförelse med tidigare år. Som redan påtalats i halvårsrapporten 2024 gäller då att kommunen har en tillräckligt bemannad dataskyddsorganisation med kontaktombud på samtliga förvaltningar, avdelningar och enheter. Kontaktombuden behöver också få tillräckligt med insyn, utbildning och tid för att mäkta med GDPR-arbetet.

Om så säkras upp, flyttas också fokus från ett omfattande reaktivt förfarande (dataskyddsombudets tillsyn) till ett proaktivt förfarande (GDPR-arbetet

[40] Jfr. art 39.1b dataskyddsförordningen.

hanteras proaktivt och löpande på förvaltningsnivå), vilket egentligen är att föredra. Se avsnitt 5.3 s. 13 för planerad granskning.

5.2.1. Några granskningar

Under detta avsnitt redovisas några av dataskyddsombudets granskningar. Avsikten är att utfallet av granskningarna ska vara lärande – inte läxande.

- Några av dataskyddsombudets granskningar har rört till exempel kommunens nya passerkort, rutiner för att avsluta anställdas IT-konton och huruvida kommunen använt system (vilka utsatts för antagonistiska angrepp). I flera fall har granskningarna avslutats utan kritik, då GDPR-arbetet hade gjorts eller kommunen inte varit berörda, vilket givetvis är positivt.
- *Kommunstyrelsen*: Granskning av kommunstyrelsens delegationsordning där anmälan av personuppgiftsincidenter till Integritetsskyddsmyndigheten bedömdes utgöra *verkställighet*. Oavsett om dataskyddsombudets rekommendation följs eller inte, är inrymmer bedömningen sådana komplicerade *överväganden* och *bedömningar*, att det inte borde kunna hanteras som verkställighet,[41] utan borde delegeras till förvaltningschef. Under hösten 2024 ändrades delegationen till viss del.
- *Utbildningsnämnden*: Under hösten 2023 avslutade jag en stor granskning av utbildningsnämndens skolplattformar. Under vintern 2023/24 följde jag upp hur rapporten hade hanterats av bildningsförvaltningen. I det skedet hade rapporten inte tagits upp i utbildningsnämnden och ingen tidsplan eller process hade tagits fram. I juni 2024 följder jag återigen upp status, och vissa åtgärder hade då vidtagits och planerats.

  Den 25 oktober 2024 har utbildningsnämnden *på eget initiativ* återkopplat vidtagna och planerade åtgärder i anledning av granskningen (men även innehållande vissa förvaltningsrättsliga utvecklingsområden). Jag har gått igenom åtgärderna med verksamheten, och bedömer att verksamheten – genom att förstärka med en resurs och utöka samarbetet med andra förvaltningar – arbetar med GDPR-utmaningarna på ett mer strategiskt sätt och i högre tempo, än tidigare.
- *Kommunstyrelsen* med flera: Fortfarande uppmärksammas inte driftsstörningar och buggar i verksamhetssystem, webb och intranät, som leder till *ändring* eller *tillfällig förlust* av *personuppgifter* som en personuppgiftsincident i tillräcklig utsträckning.

5.3 Personuppgiftsincidenter

En personuppgiftsincident är en incident som leder till *oavsiktlig* eller *olaglig förstöring*, *förlust* eller *ändring* eller till *obehörigt röjande av* eller

[41] Jfr. prop. 2016/17:171 s. 382.

obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.[42]

Incidenten ska anmälas till Integritetsskyddsmyndigheten inom 72 timmar, såvida det *inte är osannolikt* att incidenten medför en *risk för personers fri- och rättigheter*.[43] Dataskyddsombudet lämnar verksamheten en rekommendation. Nämnden (delegaten) beslutar huruvida incidenten ska anmälas till Integritetsskyddsmyndigheten. Nämnden ska därefter informeras om beslutet och incidenten diarieföras.

Det bör finnas *ett visst flöde* av rapporterade personuppgiftsincidenter. Att en nämnd har många *rapporterade personuppgiftsincidenter* talar *inte* nödvändigtvis för en sämre hantering av personuppgifter, utan kan istället visa på att personuppgiftsincidenter identifieras och anmäls på ett korrekt sätt. Om en nämnd har *få eller inga personuppgiftsincidenter* talar det inte nödvändigtvis för en bättre hantering av personuppgifter, utan kan visa på att personuppgiftsincidenter inte identifieras och anmäls i tillräcklig utsträckning. Det är mindre troligt att ingen incident inträffat under ett år, utan då antas finnas ett mörkertal.

Danderyds kommun har haft 56 personuppgiftsincidenter år 2024. Detta kan jämföras med tidigare år, enligt följande.

- 57 incidenter år 2023
- 54 incidenter år 2022
- 38 incidenter år 2021

Sammantaget ligger inträffade incidenter på jämn nivå sedan tre år tillbaka, med drygt en rapporterad personuppgiftsincident i veckan på kommun-övergripande nivå.

De rapporterade incidenterna år 2024 är fördelade enligt följande.

	Svarsalternativ	Antal ärenden	Antal ärenden (procent)
1	Socialnämnden	16	28.6
2	Utbildningsnämnden	14	25.0
3	Kommunstyrelsen	11	19.6
4	Miljö- och stadsbyggnadsnämnden	11	19.6
5	Kultur- och fritidsnämnden	2	3.6
6	Tekniska nämnden	1	1.8
7	Överförmyndarnämnden	1	1.8
	Summa	56	100%

De flesta incidenter är av mindre allvarligt slag. Notera att en personuppgiftsincident som rör flera nämnder, endast statistiskt redovisas som *en* incident för *en* nämnd.

Nämnder som inte nämns har haft 0 personuppgiftsincidenter, vilket dessa nämnder har att analysera.

I samband med inträffade personuppgiftsincidenter brukar jag rekommendera att generella eller specifika tekniska eller organisatoriska åtgärder vidtas för att stävja liknande incidenter. Jag avser att på sikt följa upp, genom granskning, om verksamheten har vidtagit tillräckliga åtgärder för att stävja nya incidenter.

[42] Jfr. art. 4 dataskyddsförordningen.
[43] Art. 33 dataskyddsförordningen.

5.3.1. Några personuppgiftsincidenter

Några i Danderyds kommun inträffade personuppgiftsincidenter nämns kort nedan. Avsikten är att exemplen ska vara lärande – inte läxande.

- *Kommunstyrelsen*: Två incidenter har rört *förväxling* av profiler i Microsofts miljö. En medarbetare har mottagit chefens kalender-notiser på sin arbetstelefon samt en medarbetare har mottagit kollegans bokningar i sin kalender.
- *Kommunstyrelsen*: I en upphandlingsportal som används för att avropa avtal kunde kommunens upphandlare *se* andra kommuners upphandlares profiler, och avropa från deras avtal. Rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Miljö- och stadsbyggnadsnämnden*: Flera personuppgiftsincidenter har inträffat vid hanteringen av bygglovsärenden, genom systembrister i kombination med mänsklig faktor i vissa fall. Det har också framkommit att verksamhetssystemet inte inrymmer möjlighet att gallra i enlighet med dokumenthanteringsplanen. Anmälningar till Integritetsskyddsmyndigheten har rekommenderats i flera fall och verksamheten arbetar aktivt med att stävja incidenterna.
    - Samma leverantör har för ett kartsystem larmat om att tjänsten innehållit *allvarliga säkerhetsbrister*, och att fortsatt användning skulle ske på egen risk. Det var anmärkningsvärt att leverantören ville att kommunen skulle stå kostnaden för att kunna tillhandahålla en säker tjänst. Sammanfattningsvis rörde det sig om två incidenter, en rörde säkerhetsbristen och en rörde fortsatt användning av kartsystemet, trots att säkerhetsbristen varit känd. Rekommenderade anmälan till Integritetsskyddsmyndigheten.
    - Även ett annat kartsystem fick stängas ner efter identifierade säkerhetsbrister, varpå översyn av kartsystemen rekommenderades.
- Både *kommunstyrelsen* och *socialnämnden* har under året råkat ut för *ändring* av personuppgifter i bedrägerisyfte. Anmälan till Integritetsskyddsmyndigheten har rekommenderats i båda fallen.
- *Utbildningsnämnden*: Flera fall av *obehörigt röjande* och *obehörig åtkomst* har skett hos leverantören för skolskjuts, under året. Rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Utbildningsnämnden*: Några incidenter har rört *obehörigt röjande* i form av att information om en kränkning skickats till flera vårdnadshavare, information om en konflikt skickats till samtliga vårdnadshavare i klassen och ett mejl om en elevs svagheter skickats till fel vårdnadshavare. Rekommenderade anmälan till Integritetsskyddsmyndigheten i samtliga nämnda fall.
- *Kommunstyrelsen*: Några incidenter har rört driftsstörningar som inloggningssvårigheter, buggar och brister i funktion, vilket utgör

tillfällig *förlust* av personuppgifter. Rekommenderade organisatoriska och tekniska åtgärder.

- *Socialnämnden*: Information om en anhörigträff, mejlades ut utan att använda dold kopia. Rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Socialnämnden*: Några incidenter har rör *obehörigt röjande* och *obehörig åtkomst* genom samverkan i familjerätten och socialjouren. Rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Utbildningsnämnden*: En allvarligare incident rörde att en lista med 700-800 elevers namn, deras vårdnadshavares namn, personals namn, elevers personnummer, hemkommun, utbildningskod och programpeng skickades ut av misstag till skolans samtliga 1 300 elever. Rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Kultur- och fritidsnämnden*: *Obehörigt röjande* har inträffat dels genom användningen av gemensam brevlåda med andra föreningar, och *obehörig åtkomst* genom att en skrivare i öppet bibliotek skrivit ut papper med namn.
- *Socialnämnden*: I samband med en utredning om ett familjehem gjorde handläggaren sökningar på personuppgifter i den rättsdatabas som kommunen har licens för, men som inte är avsedd för att användas för bakgrundskontroller. Hanteringen avvek också från rutiner. Rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Socialnämnden*: I samband med att IT-enheten arbetade med flytt av data, identifierades att uppgifter från socialnämndens verkssystem mellanlagrats inför att föras över till kommunstyrelsens system för fakturering, utan att mellanlagringen varit tillräckligt säker och haft behörighetsinställningar. Rekommenderade anmälan till Integritetsskyddsmyndigheten.

5.4 Skadestånd

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

Vad jag fått kännedom om, har ingen begäran om skadestånd på grund av dataskyddsöverträdelser inkommit under året.

5.5 Registerutdrag

En person har rätt att begära ut ett registerutdrag, vilket är en redogörelse för i vilka sammanhang kommunen hanterar dennes personuppgifter.

Statistiken visar att två nämnder har berörts av begäran om registerutdrag under år 2024, enligt följande.

	Svarsalternativ	Antal ärenden	Antal ärenden (procent)
1	Kommunstyrelsen	3	60.0
2	Socialnämnden	2	40.0
	Summa	5	100%

5.6 Andra rättigheter

Personer har enligt dataskyddsförordningen flera specifika rättigheter som till exempel rätt att begära radering, rättelse, invändning, begränsning och få information.

Vad jag fått kännedom om, har ingen begäran om åberopande av rättigheterna inkommit under året.

5.7 Integritetsskyddsmyndighetens tillsyn och sanktionsavgifter

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

Vad jag fått kännedom om, har Integritetsskyddsmyndigheten inte genomfört eller annonserat någon kommande tillsyn, eller ålagt kommunen att betala någon administrativ sanktionsavgift under året.

6. Omvärldsbevakning

Under detta avsnitt kommer jag redogöra för vägledande och kunskapshöjande omvärldsbevakning. Avsikten är att informationen ska vara lärande – inte läxande.

6.1 Integritetsskyddsmyndigheten: Reprimand för att inte haft tillräcklig spårbarhet (loggning)

Integritetsskyddsmyndigheten har granskat Verisure Sverige AB:s hantering av bildmaterial från kunders hem. Granskningen visade att logguppgifter från kamerorna endast sparades i tre månader, vilket bedömdes otillräckligt ur kontrollsynpunkt. Bolaget meddelades en reprimand.[44]

6.2 Integritetsskyddsmyndigheten: Sanktionsavgifter för överföring till Facebook/Meta

- Avanza hade aktiverat ett analysverktyg för marknadsföring på sin webbplats, Meta-pixeln, vilket kom att innebära att en halv till en miljon kunders uppgifter om värdepappersinnehav, lånebelopp, kontonummer och personnummer överfördes till Meta, i okrypterat format. Integritetsskyddsmyndigheten meddelade Avanza en sanktionsavgift på 15 miljoner kronor.[45]

[44] Integritetsskyddsmyndighetens beslut i ärende IMY-2022-1558, den 27 november 2024; https://www.imy.se/globalassets/dokument/beslut/2024/tillsynsbeslut-verisure-sverige-ab.pdf.
[45] Integritetsskyddsmyndighetens beslut i ärende DI-2021-5544 den 24 juni 2024; https://www.imy.se/globalassets/dokument/beslut/2024/beslut-tillsyn-avanza.pdf.

- Även Apoteket AB och Apohem AB hade aktiverat Meta-pixeln. Kunders namn, adresser och vilka produkter de köpt (receptfria läkemedel, intimprodukter, självtester) hade överförts till Meta, i krypterat format. Integritetsskyddsmyndigheten meddelade administrativ sanktionsavgift till Apoteket på 37 miljoner kronor, och till Apohem på 8 miljoner kronor.[46]

6.3 Integritetsskyddsmyndigheten: Reprimand för att dataskyddsombudet inte fått tillräckliga resurser

Socialnämnden i Örebro har ålagts en reprimand för att nämnden *inte* säkerställt att dataskyddsombudet fått tillräckligt med resurser och blivit involverad i god tid. Vidare har den personuppgiftsansvariga inte säkerställt att dataskyddsombudet rapporterat till högsta förvaltningsnivå.[47]

6.4 Dagens juridik, debatt: Integritetsskyddsmyndigheten sviker dataskyddsombuden och personers fri- och rättigheter

I debattformat riktar några dataskyddsombud kritik mot Integritetsskydds-myndigheten för att inte agera när dataskyddsombud utsatts för repressalier eller avsätts för att de utfört sina arbetsuppgifter.[48] Debattörerna menar att detta i förlängningen får negativa effekter för personers fri- och rättigheter.[49]

———

[46] Integritetsskyddsmyndighetens beslut i ärende IMY-2022-3270 den 30 augusti 2024, https://www.imy.se/globalassets/dokument/beslut/2024/beslut-tillsyn-apoteket-ab.pdf och Integritetsskyddsmyndighetens beslut i ärende IMY-2022-3272 den 29 augusti 2024, https://www.imy.se/globalassets/dokument/beslut/2024/beslut-tillsyn-apohem.pdf.
[47] Integritetsskyddsmyndighetens beslut i ärende IMY-2023-7963; https://www.imy.se/globalassets/dokument/beslut/2024/tillsynsbeslut-socialnamnden-i-orebro-kommun.pdf
[48] Vilket inte är förenligt med art. 38.3 dataskyddsförordningen.
[49] https://www.dagensjuridik.se/opinion/imy-sviker-dataskyddsombuden-och-darmed-alla-svenska-medborgare/, bevittnat den 10 december 2024.