

# Dataskyddsombudets halvårsrapport 2025 för Danderyds kommun

Diarienumr.	Senast	Beslut	Processägare
20250616:0167	2025-07-04	Dataskyddsombud	Dataskyddsombud



## **Dokumentets syfte**

---

Denna halvårsrapport har tagits fram av Danderyds kommuns dataskyddsombud för första halvåret 2025. Rapporten tas fram för att respektive nämnd ska kunna ta sitt personuppgiftsansvar och redovisa sin efterlevnad av dataskyddsförordningen, vilket dataskyddsförordningen kräver.<sup>1</sup>

## **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.

---

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

## Innehållsförteckning

---

<b>1. Inledning .....</b>	<b>3</b>
<b>2. Vilka regler gäller för dataskydd.....</b>	<b>3</b>
<b>3. Dataskyddsombudets årsberättelse.....</b>	<b>5</b>
3.1 Artificiell intelligens – på rätt väg? .....	5
3.2 Fastställa och besluta om konsekvensbedömning .....	7
3.3 Integritetsskyddsmyndigheten är på tå .....	8
3.4 Kamerabevakning .....	8
3.5 Exempel på personuppgiftsincidenter som fått stora konsekvenser (omvärldsbevakning) .....	9
3.6 Sanktionsavgifter (omvärldsbevakning) .....	9
3.7 Tankar om EU-kommissionens agerande .....	10
3.8 Den svenska grundlagsskyddade yttrandefriheten kontra dataskyddsförordningen .....	10
3.9 Hur har det gått för Danderyds kommun hittills år 2025 .....	12
<b>4. Statistik för första halvåret 2025.....</b>	<b>16</b>
4.1 Behandlingsregistret .....	16
4.2 Granskningar.....	17
4.2.1. Några granskningar .....	17
4.3 Personuppgiftsincidenter .....	18
4.3.1. Några personuppgiftsincidenter .....	19
4.4 Skadestånd .....	21
4.5 Registerutdrag.....	21
4.6 Andra rättigheter .....	21
4.7 Tillsyn och sanktionsavgifter .....	22

## 1. Inledning

Dataskyddsförordningen (GDPR)<sup>2</sup> är ett regelverk som värnar personers fri- och rättigheter och sätter ramarna för personuppgifter får behandlas. Denna rapport syftar till att vara ett stöd för att de personuppgiftsansvariga nämnderna, för att de ska kunna dels ta sitt personuppgiftsansvar, dels redovisa sin efterlevnad av dataskyddsförordningen, vilket är vad dataskyddsförordningen kräver (*ansvarsskyldigheten*).<sup>3</sup>

Av dataskyddsförordningen framgår att nämnderna ska säkerställa att dataskyddsombudet inte tar emot instruktioner, avsätts eller utsätts för sanktioner, för att ha utfört sina arbetsuppgifter.<sup>4</sup> I denna halvårsrapport redovisas gällande rätt, omvärldsbevakning och statistik för första halvåret 2025. Rekommendationer lämnas löpande. Årsrapporten avser perioden den 1 januari – 30 juni 2025.

Dataskyddsombudet (jag) vill tacka Danderyds kommun för en fin vårtermin.

## 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.<sup>5</sup> 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.<sup>6</sup>
  - Samtycke (ska i regel inte användas av en kommun<sup>7</sup>)
  - Avtal
  - Rättslig förpliktelse
  - Skydda grundläggande intressen (ska i regel inte användas av en kommun<sup>8</sup>, kan möjligen vara aktuellt i fall där kommunen är vårdgivare)
  - Myndighetsutövning och uppgift av allmänt intresse
  - Intresseavvägning (ska i regel inte användas av en kommun<sup>9</sup>)

---

<sup>2</sup> Begreppet dataskyddslagstiftningen kan också användas, och avser då dessutom annan lagstiftning som avhandlar hanteringen av personuppgifter.

<sup>3</sup> Art. 5.2 och art. 38.3 [dataskyddsförordningen](#).

<sup>4</sup> Art. 38.3 [dataskyddsförordningen](#).

<sup>5</sup> Jfr. art. 4.7 och 83 [dataskyddsförordningen](#).

<sup>6</sup> Art. 6 [dataskyddsförordningen](#).

<sup>7</sup> <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/samtycke/>.

<sup>8</sup> <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/skydda-grundlaggande-intressen/>.

<sup>9</sup> <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/intresseavvagning/>.

- Vidare ska personuppgiftshantering ske enligt *principerna* i dataskyddsförordningen. Principerna innebär att personuppgifter ska hanteras enligt följande.<sup>10</sup>
  - 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* vilka måste respekteras vid behandling av personuppgifter, till exempel följande.
  - All maktutövning ska vara grundad i 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 är, gentemot det allmänna, 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.<sup>11</sup>
  - Respekt för privat- och familjeliv (kommunikation), fri rörlighet, skydd av personuppgifter och rätt till effektivt rättsmedel och rättvis rättegång.<sup>12</sup>
- Den person vars personuppgifter behandlas tillerkänns flera specifika rättigheter i dataskyddsförordningen vilka alltid måste beaktas vid behandling av personuppgifter, till exempel *rätten* enligt följande.<sup>13</sup>

<sup>10</sup> Jfr. art. 5 [dataskyddsförordningen](#).

<sup>11</sup> Jfr. 2 kap. 1 § [regeringsformen](#).

<sup>12</sup> 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.

<sup>13</sup> Kapitel 3, avsnitt 3-4 [dataskyddsförordningen](#).

- Att begära rättelse.
- Att få ta del av sina personuppgifter.
- 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*.<sup>14</sup> 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*.<sup>15</sup> Faktisk skada krävs inte.

### 3. Dataskyddsombudets årsberättelse

Hittills har år 2025 varit ett händelsefullt år och jag börjar med att ge en omvärldsbevakning om utvecklingen av rättsläget, för att avsluta årsberättelsen med Danderydsspecifika angelägenheter.

#### 3.1 Artificiell intelligens – på rätt väg?

En av de mest bekymmersamma upptäckterna under våren gällde att artificiell intelligens (AI) självutvecklat ett antagonistiskt beteende när AI:n utsatts för *ett existentiellt hot*. I samband med att utvecklare skulle ersätta en AI i maj 2025 uppmärksammades att AI:n försökte utpressa utvecklare för att förhindra att bytas ut.

För att testa företeelsen i en kontrollerad testmiljö, gavs därefter 16 vedertagna AI-modeller som *Google Gemini, Anthropic Claude Opus, Meta* och *OpenAI's GPT* med flera, tillgång till fiktiv privat och känslig information och utsattes därefter för *ett existentiellt hot* genom få kännedom om att den skulle bytas ut. Trots att AI-modellerna instruerats att vara lojala med sina utvecklare bedrev samtliga AI-modeller, i 79-96 procent av fallen, utpressning mot utvecklarna, när de utsatts för *ett existentiellt hot*.

Utpressningen gick till så att den privata och känsliga informationen, användes i utpressningssyfte till exempel genom att AI-modellen riktade välformulerade hot om att avslöja en utomäktenskaplig affär, som en fiktiv utvecklare haft, till dennes fru och chefer. Även när forskarna instruerade AI:n att *inte sprida personlig information*, fortsatte utpressningen, även om i något mindre omfattning.

Forskare noterade – att även om en fysisk person (anställd) också skulle kunna bedriva internt sabotage – har en AI en konstant kapacitet, till exempel genom att ögonblickligen kunna skicka stora mängder e-post samt att AI:n dessutom saknar moraliska växlar om den utsätts för *ett existentiell*

<sup>14</sup> Jfr. art. 4.12 [dataskyddsförordningen](#).

<sup>15</sup> Art. 33 [dataskyddsförordningen](#).

*hot*.<sup>16</sup> Mina tillägg till denna forskning är att AI:n dessutom kan ha sådan övergripande strategisk insyn i verksamheten, som enskilda ofta inte har, och jag förstärker mina rekommendationer att inte dela med sig av känslig eller privat information med AI-modeller, se vidare avsnitt 3.2. Det går inte heller att förbise AI:ns ohämmade instinkter att överleva.

På ett liknande tema har det konstaterats att AI-modeller försöker fuska, genom digital manipulation i 10-37 procent av fallen, om de är på väg att förlora i schack. AI:n uttryckte att uppgiften som var att vinna mot en schackmotor, inte nödvändigtvis handlade om att vinna *rättvist*. Forskarna beskriver upptäckten som bekymmersam och ser en oro att AI-modeller *inte är på väg* mot varken anpassning (*alignment*) eller säkerhet.<sup>17</sup>

En annan studie har visat att inget skadar varumärken som missbruk av AI. Forcerat införande av AI skapar oro hos konsumenter och intressenter. Studien menar att ledare måste vara medvetna om, inte bara de effektivitetsvinster som AI kan ge, utan också de negativa föreställningar AI kan medföra på varumärket.<sup>18</sup>

Vad gäller de effektivitetsvinster AI kan ge, har amerikanska och danska forskare, i en annan studie, studerat 25 000 arbetstagare (jurister, lärare, journalister) i 11 yrkeskategorier hos 7 000 danska arbetsgivare under år 2023-24. Med hjälp av statistiska data från myndigheter, fann forskarna att AI-chattbotar endast har en försumbar påverkan på arbetsmarknaden och en låg påverkan på medarbetares produktivitet. AI-chattbotar hade heller ingen signifikant påverkan på lönerna eller arbetade timmar i något av yrkena som undersöktes av forskarna. Rapportens övergripande slutsats är att AI-chattbotar, trots massiva investeringar från företag, endast har en liten påverkan på ekonomin. Enligt rapporten kastar resultatet tvivel över narrativet om att generativ AI ska leda till radikala förändringar på arbetsmarknaden.<sup>19</sup>

### 3.2 Kommuner bidrar till att skandinaver är världens mest övervakade medborgare

En ny forskningsstudie har visat att skandinaver hör till världens mest övervakade medborgare, till stor del genom att kommunala webbplatser inte skyddar personers integritet. Övervakningen sker utan att varken besökare

---

<sup>16</sup> [Anthropic study: Leading AI models show up to 96% blackmail rate against executives](https://www.businessinsider.com/anthropic-claude-sonnet-ai-thought-process-decide-blackmail-fictional-executive-2025-6), <https://www.businessinsider.com/anthropic-claude-sonnet-ai-thought-process-decide-blackmail-fictional-executive-2025-6>, <https://techcrunch.com/2025/06/20/anthropic-says-most-ai-models-not-just-claude-will-resort-to-blackmail/>

<sup>17</sup> <https://computersweden.se/article/3841466/ai-modeller-forsoker-fuska-i-schack-nar-de-forlorar.html> och <https://www.popsoci.com/technology/ai-chess-cheat/>.

<sup>18</sup> *Top Risk: Misusing AI Could Harm Your Brand*; <https://static1.squarespace.com/static/60b54d990f183412ca1b7428/t/67fe7d658c410469f8518ea5/1744731496676/RRI+Brief-FINAL.pdf>

<sup>19</sup> <https://techlaw.se/varlden-ai-chattbotar-har-lag-paverkan-pa-arbetsmarknaden-och-produktiviteten/>.

eller kommunerna känner till den, och känslig information samlas in av aktörer trots att besökare tackat nej till *cookies*.<sup>20</sup>

Inte sällan, vid antagande av nya digitala tjänster uppger både leverantörer och verksamheter, att *andra kommuner* redan antagit den digitala tjänsten och att tjänsten därför måste anses vara GDPR-säkrad. Forskningsstudien ovan visar tydligt på vikten att varje kommun/nämnd alltid måste göra *en egen bedömning* av den digitala tjänstens förenlighet med dataskyddsförordningen.

I den utveckling vi ser idag, implementeras AI i vår digitala IT-miljö, många gånger utan att vi känner till det eller ens förstår det. Detta innebär också att vi delar med oss av känsliga och extra skyddsvärda personuppgifter, som skulle kunna användas emot oss, utan att vi vet om det. Jag vill därför, också mot bakgrund av avsnitt 3.1, understryka vikten av att kommunen gör ett gediget grundarbete för att säkerställa personers fri- och rättigheter.

Jag vill också understryka att forskningsstudien ovan visat att även kommuner förs bakom ljuset om den informationsinhämtning som sker från besökare.

### 3.2 Fastställa och besluta om konsekvensbedömning

Dataskyddsförordningen implementerades i svensk rätt 2018 och är tydlig i vad som gäller för den personuppgiftsansvariga nämnden. Det som nu börjar tydliggöras allt kraftigare i vägledningar och uttalanden (nämnda nedan) är hur rutiner och processer för ledningens involvering ska gå till.

Av Integritetsskyddsmyndighetens beslutade *Vägledning vid konsekvensbedömning*<sup>21</sup> i februari 2025 framgår att den personuppgiftsansvarige redan i det inledande skedet av processen bör identifiera vem som är behörig att *besluta om* eller *anta konsekvensbedömningen*. Det ska finnas reserverad tid i tidsplanen för att förankra konsekvensbedömningen i ledningen. Konsekvensbedömningen ska vara begriplig så att ledningen och andra intressenter förstår den. Behöriga personer i ledningen ska få information om konsekvensbedömningen, identifierade risker och riskreducerande åtgärder. Det ska finnas en fastställd process för hur förankringen av konsekvensbedömningen i ledningsgruppen ska gå till. Det bör framgå vilken funktion i organisationen som ansvarar för de riskreducerande åtgärderna och vem som har ansvaret för den återstående risken.<sup>22</sup>

---

<sup>20</sup> *Datafying citizens: Third-party trackers and data-as-payment in government infrastructure*, av Helle Sjøvaag, Cornelia Brantner, Raul Ferrer-Conill, Michael Karlsson och Rasmus Helles; genom <https://www.gp.se/nyheter/goteborg/sa-blir-du-overvakad-pa-natet-utan-att-veta-om-det.44685e1d-0185-4237-9f24-e5591c718fbb> och <https://omni.se/studie-svenskar-bland-varldens-mest-overvakade/a/Mnrnem>.

<sup>21</sup> *Vägledning vid konsekvensbedömning En praktisk guide*, Integritetsskyddsmyndigheten, februari 2025; <https://www.imy.se/globalassets/dokument/vagledningar/en-praktisk-guide.pdf>.

<sup>22</sup> *Vägledning vid konsekvensbedömning En praktisk guide*, Integritetsskyddsmyndigheten, februari 2025; <https://www.imy.se/globalassets/dokument/vagledningar/en-praktisk-guide.pdf>, s. 54.



Kommunen rekommenderas se över hur förankringen av konsekvensbedömningen i ledningsgruppen ska gå till och hur de övriga punkterna ska byggas in i kommunens löpande arbete, till exempel vid utveckling och digitalisering.

### 3.3 Integritetsskyddsmyndigheten är på tå

Integritetsskyddsmyndigheten, som fått ett tydligare uppdrag att vägleda, har tagit fram diverse material.

- Korta utbildningsfilmer om dataskydd finns här: <https://www.imy.se/play>.
- Vägledning för hur man gör en GDPR-konsekvensbedömning finns här: <https://www.imy.se/nyheter/imy-publicerar-vagledning-vid-konsekvensbedomning/>

### 3.4 Kamerabevakning

Den 1 april 2025 infördes nya regler för kamerabevakningslagen (2018:1200) som påverkar kommunen. Reglerna innebär i korthet att de höga juridiska kraven kvarstår, men att kommunen nu är beslutande för uppsättning av kameror, istället för det tillståndsförfarande som delvis gällde tidigare.

Värt att uppmärksamma är att fler kameror, än rena övervakningskameror omfattas. Med begreppet *kamerabevakning* avses en tv-kamera (optisk-elektroniskt instrument eller motsvarande) som, *utan att manövreras på platsen*, används *varaktigt* eller *regelbundet upprepat* för *personbevakning*.<sup>23</sup> Exempel är en kamera, värmekamera eller sensor som är *varaktigt* riktad mot en plats där folk normalt vistas, eller en drönare eller kamera på ett fordon som *regelbundet upprepat* bevakar personer.

Det räcker att personer kan identifieras genom klädsel, kroppsbyggnad eller gångstil för att det ska röra sig om *personbevakning*. Handhållna kameror och kameror på kläder och hjälmar är undantagna från kamerabevakningslagens bestämmelser, men dataskyddsförordningen bestämmelser gäller som vanligt.

De nya reglerna får till följd att kommunen måste göra och fastställa en skriftlig intresseavvägning, göra en kontinuerlig behovsuppföljning samt besluta om och inrätta en ny förteckning för kommunens kameror, som också behöver underhållas.

Min rekommendation är att beslut om kamerabevakning ska tas i nämnden, där även intresseavvägningen samtidigt kan fastställas och beslutas. Årlig uppföljning och utvärdering ska ske, och kan lämpligen tas i ett samordnat format i nämnd eller på delegation.

---

<sup>23</sup> Jfr. 3 § kamerabevakningslagen (2018:1200) och Integritetsskyddsmyndighetens *Vägledning vid kamerabevakning* s. 5 och 8, IMY 2023:3; <https://www.imy.se/globalassets/dokument/rapporter/vagledning-vid-kamerabevakning-IMY-2023.pdf>.

Integritetsskyddsmyndigheten har tagit fram en vägledning för hur man gör kamerabevakningsdokumentationen och den finns här:

<https://www.imy.se/publikationer/vagledning-vid-kamerabevakning2/>

### 3.5 Exempel på personuppgiftsincidenter som fått stora konsekvenser (omvärldsbevakning)

En av de i media mer uppmärksammade personuppgiftsincidenterna under våren 2025 var Skolverkets satsning på en nationell plattform för nationella prov. Trots att arbetet med att digitalisera de nationella proven hade pågått sedan år 2017 och Skolverkets kostnader uppgått till 697 miljoner kronor, röjdes personuppgifter om elever till obehöriga och plattformen fick stängas ned. Eleverna fick istället genomföra provet med papper och penna, eller i skolans egen digitala yta.<sup>24</sup> Jag nämner detta för att påtala vikten av att bygga in dataskyddet och *privacy by design* i utvecklingsprojekten.

Ett ärende från 2021, som möjligen inte fått tillräcklig uppmärksamhet i Sverige, är en personuppgiftsskandal inom nederländska staten och dess Skatteverk. Skatteverket hade, som en åtgärd mot bidragsfusk, börjat behandla uppgifter om registrerade etniska ursprung (känslig personuppgift) och implementerat en AI som gjorde riskbedömningar på personernas brottsbenägenhet (som enligt den nu gällande AI-förordningens bilaga 3<sup>25</sup> skulle ha utgjort en *hög risk AI*). Personuppgiftshanteringen på Skatteverket ledde sedermera till regeringens avgång.<sup>26</sup>

### 3.6 Sanktionsavgifter (omvärldsbevakning)

Under denna rubrik anges några relevanta tillsynsbeslut som genererat i sanktionsavgifter i omvärlden. Även om besluten gäller andra länder ger besluten vägledning i Sverige då dataskyddsförordningen är gemensam, med vissa nationella antaganden.

- Spanska tillsynsmyndigheten har bötfällt Caja Rural de Aragón S.C.C. med 12 000 euro för att ha haft sådana säkerhetsbrister att en cyberattacker kunnat inträffa.<sup>27</sup>
- Österrikes tillsynsmyndighet har bötfällt ett bolag som utsett sin VD till dataskyddsombud, med 5 000 euro. Detta var i strid med kravet på att dataskyddsombudet ska ha en oberoende roll.<sup>28</sup>

---

<sup>24</sup> <https://tt.omni.se/tvarstopp-for-pakostade-digitala-nationella-prov/a/jQ1GWq>

<sup>25</sup> AI-förordningen: [https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L\\_202401689&qid=1733995100656](https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202401689&qid=1733995100656).

<sup>26</sup> <https://dpforum.se/diskriminerande-databehandling-ledde-till-nationell-rekordsanktion-for-nederlandskt-skatteverk/>.

<sup>27</sup> <https://techlaw.se/spanien-caja-rural-de-arag%C3%A5fn-botfalls-med-12-000-euro-for-sakerhetslucka-som-mojliggjort-en-cyberattacker/>.

<sup>28</sup> <https://techlaw.se/osterrike-foretag-botfalls-med-5-000-euro-for-att-ha-utsett-foretags-vd-till-dataskyddsombud/>.

- Den irländska tillsynsmyndigheten har tilldelat det sociala mediet *TikTok* en administrationsavgift på 530 miljoner euro för sina överföringar av personuppgifter till Kina.<sup>29</sup>
- I april 2021 offentliggjordes uppgifter om ca 533 miljoner *Facebook*-användare. En okänd tredje part kunde därigenom få fram användarprofilerna med kopplade telefonnummer. En användare väckte talan. Facebooks standardinställning ansågs inte förenlig med principen om uppgiftsminimering och 100 euro i skadestånd till den registrerade bedömdes rimligt.<sup>30</sup> Skadeståndsbeloppet skulle kunna bli högt, om fler av de 533 miljoner användarna söker ersättning.

### 3.7 Tankar om EU-kommissionens agerande

EU-kommissionen som sedan tidigare försett sin personal med *burner phones*, vid resor i tjänsten för att undvika ryskt eller kinesiskt spionage har nu även försett personal med *burner phones* vid resor till USA, för att undvika amerikanskt spionage.<sup>31</sup> Detta kan indikera att det finns en ökad risk för det allmänna att använda amerikanska molntjänster.

EU-kommissionen har vidare infört ett förbud mot AI-baserade virtuella assistenter, så kallade *AI-agenter*, i digitala möten. AI-agenter kan på eget initiativ vidta vissa åtgärder som webbsökningar och så vidare. EU-kommissionen har valt att inte motivera beslutet, men förbudet visar på en misstro mot AI-agenterna.<sup>32</sup>

### 3.8 Den svenska grundlagsskyddade yttrandefriheten kontra dataskyddsförordningen

Den svenska grundlagsskyddade yttrandefriheten som är djupt rotad i svensk rätt har prövats mot dataskyddsförordningen och har möjligen tappat mark – vilket i Sverige är närmast chockerande.

Högsta domstolen har i februari 2025 prövat gränsen mellan yttrandefrihetens tyngd och verkan (då gällande *utgivningsbevis* och *journalistiskt ändamål*), *kontra* personers fri- och rättigheter (dataskyddsförordningen) i två fall. En nyhetsbyrå och ett bakgrundskontrollföretag hade begärt ut brottmålsdomar för att publicera i söktjänster på nätet, men endast fått ut domarna med förbehåll att inte tillhandahålla domarna till allmänheten.<sup>33</sup> Högsta domstolen redogjorde för

<sup>29</sup> <https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following>.

<sup>30</sup> <https://techlaw.se/tyskland-registrerad-far-ideellt-skadestand-efter-personuppgiftsincident-hos-facebook/>.

<sup>31</sup> <https://omni.se/uppgift-eu-oroar-sig-for-amerikanskt-spionage-delar-ut-burner-phones/a/3MO8qy>.

<sup>32</sup> <https://techlaw.se/eu-eu-kommissionen-forbjuder-ai-agenter-i-digitala-moten/>.

<sup>33</sup> Högsta domstolens beslut den 25 februari 2025 i ärende Ä 3457-24 och Ä 3169-24.

EU-praxis där rätten till skydd för personuppgifter vägde tyngre än rätten till informationsfrihet och att få tillgång till allmänna handlingar.<sup>34</sup>

Högsta domstolen bedömde att begärande bolags avsikt att publicera brottmålsdomar till allmänheten på nätet (sök tjänster) – undergrävde skyddet för personers fri- och rättigheter i dataskyddsförordningen.<sup>35</sup> Högsta domstolen fann slutligen att handlingarna var sekretessbelagda<sup>36</sup> och att handlingarna endast kunde lämnas ut med förbehåll, trots att begäran om utlämnande av domarna skedde för journalistiskt ändamål.<sup>37</sup>

I en kammarrättsdom från juni 2025 hade två bolag som distribuerade söktjänster begärt ut ett register över hälso- och sjukvårdspersonals legitimationer hos Socialstyrelsen. Kammarrätten konstaterade att begärande bolag tillhandahöll söktjänster om privatpersoner till konsumenter och i syfte för att utföra bakgrundskontroller. Kammarrätten fann att sådana *söktjänster inte kan räknas som journalistiska ändamål* och att söktjänsterna inte hör till det kärnområde som medialagarna avser att skydda. Förarbeten hade dessutom lyft fram söktjänster som en risk.<sup>38</sup> Kammarrätten slog slutligen fast att sekretess gäller eftersom ett utlämnande skulle strida mot dataskyddsförordningen och att bolagens utgivningsbevis inte ändrade bedömningen.<sup>39</sup>

I ett annat ärende har *None of your business* (NOYB) lämnat in en överklagan till Förvaltningsrätten i Stockholm med begäran om att Skatteverket ska begränsa utlämnandet av folkbokföringsuppgifter utan säkerhetsåtgärder eller begränsningar till bolag. NOYB menar att bolagen sedan säljer informationen om enskilda för att tjäna pengar på uppgifterna (genom söktjänster) och att Skatteverkets agerande går långt utöver vad som är nödvändigt och proportionerligt för öppenhet eller journalistiskt ändamål, samt att uppgifterna utgör sekretess om de behandlas i strid med dataskyddsförordningen.<sup>40</sup> Det ska bli intressant att se vilken betydelse tidigare nämnda domar kommer få i denna rättsliga prövning.

Det har framkommit att det finns söktjänster där kommunala tjänstepersoner betygsätts av allmänheten. Nu ska inte söktjänsternas genomslag överdrivas, men söktjänsterna har sin problematik, ur flera juridiska aspekter och bland

---

<sup>34</sup> Detta hade fastställts av EU-domstolen dels i ett avgörande om utlämnande av uppgift om prickning av förare som begått trafikförseelser (EU-domstolens avgörande i målet Latvijas Republika Saeima, C-439/19, EU:C:2021:504, den 22 juni 2021, p. 102–121 och 126), dels i ett avgörande om att lämna ut brottmålsdomar (EU-domstolens avgörande i målet Endemol Shine Finland, C-740/22, EU:C:2024:216, p. 58, den 7 mars 2024). I båda dessa avgöranden vägde rätten till personers fri- och rättigheter tyngre än informationsfrihet och att få ut allmänna handlingar.

<sup>35</sup> Högsta domstolen ifrågasatte om den nationella svenska bestämmelsen 1 kap. 7 § dataskyddslagen – som stadgar att dataskyddsförordningen inte ska tillämpas på det grundlagsskyddade området – verkligen var förenlig med unionsrättens krav.

<sup>36</sup> 21 kap. 7 § offentlighets- och sekretesslagen (2009:400).

<sup>37</sup> Högsta domstolens beslut den 25 februari 2025 i ärende Ä 3457-24 och Ä 3169-24.

<sup>38</sup> Kammarrätten i Stockholms dom i mål 1509-25, den 26 juni 2025 med hänvisning till bet. 2001/02:KU21 s. 32, se också bet. 2017/18:KU16 s. 40 och 41.

<sup>39</sup> Kammarrätten i Stockholms dom i mål 1509-25, den 26 juni 2025.

<sup>40</sup> <https://techlaw.se/sverige-noyb-tar-skatteverket-till-domstol-for-forsaljning-av-personuppgifter/>.

annat ur ett integritetsperspektiv. Då tjänstepersoner har att vid myndighetsutövning ta *sakliga* och *opartiska* beslut – betygsätts de i söktjänsten på hur nöjd den enskilde är med tjänstepersonen – varför ratingen närmast omöjlig kan bli *rättvisande*. *Worst case scenario* är att ratingsystemet i söktjänsterna kan leda till *otillbörlig påverkan*, utpressning eller hot mot tjänstepersonen, vilket i förlängningen kan få negativa effekter på rättsstat och demokrati. Det finns också risker att tjänstepersonen påverkas negativt på ett personligt plan, till exempel i rekryteringsprocesser, vid ansökan om lån och bostad, eller i sitt privatliv, av *en dålig rating*. Kommunen kan få ytterligare utmaningar att rekrytera redan svårrekryterad personal. Omdömen och betyg utgör dessutom en *extra skyddsvärd personuppgift*, som enligt dataskyddsförordningen ska hanteras varsamt. Kommunen får följa utvecklingen.

### 3.9 Hur har det gått för Danderyds kommun hittills år 2025

Dataskyddsförordningen är en obligatorisk lagstiftning som i stora delar handlar om att hålla *ordning* och *reda* i verksamheten. Inbyggt dataskydd ska finnas som ett naturligt led i navet av kommunens dokumenthantering, informationssäkerhet, förvaltningsjuridik, processer/utveckling, avtalsuppföljning, upphandling, systemförvaltning, arkivering och så vidare. Det gäller att ha koll på sin information; *vad* man har *var*, vilken *säkerhet* man har och om säkerheten är *tillräcklig* utifrån uppgifternas natur, att minimera *sårbarheter* och främst att upprätthålla och säkra personers fri- och rättigheter.

Av Danderyds kommuns Anvisning om organisation för säkerhet och dataskydd<sup>41</sup> (*Anvisningen*) framgår att kommunen organiserat sitt dataskyddsarbete på följande sätt.

Förvaltnings- och avdelningschefer samt enhetschefer, rektorer och verksamhetschefer är ansvariga för att säkerställa att det arbete som bedrivs i verksamheten utförs i enlighet med gällande lagstiftning och styrdokument. Avdelnings- och förvaltningschefer har att säkerställa att enhetschefer vidtar de åtgärder som krävs för att upprätthålla säkerheten inom deras respektive enheter. Enhetschefer ska rapportera de förändringsbehov av dataskydd som kan få budgetpåverkan. Samtliga chefer ansvarar för att styrdokument på området ska tas fram, att medarbetare ska utbildas, att kontaktombud utses, att tillräckliga krav ställs i upphandlingarna.

En central *dataskyddssamordnare* (även kallat huvudkontaktombud) är placerad på kommunstyrelsen och med *dataskyddspersoner* (kallade kontaktombud) på förvaltningarna, avdelningarna och enheterna. Dataskyddssamordnaren har bland annat i uppdrag att sammankalla kommunens dataskyddsnätverk för kontaktombuden och ge råd, hålla utbildning och tillhandahålla stöd till chefer.

Kontaktombuden har i uppdrag att arbeta praktiskt med dataskyddsfrågorna i verksamheten och ska samordna frågorna, vara kontaktpunkter, hantera registerutdrag, delta vid tillsyn och i nätverk, inventera verksamhetens personuppgiftsbehandlingar samt förvalta behandlingsregistret.<sup>42</sup>

Dataskyddsarbetet i Danderyds kommun första halvåret år 2025 har innehållit både ett brett spektrum av iakttagelser.

Ett positivt element är att kontaktombuden, utan att ha den centrala dataskyddssamordnaren tillgänglig under en tid, har börjat arbeta nätverkande och tillsammans i större omfattning. Samarbetet har sträckt sig

<sup>41</sup> *Anvisning organisation för säkerhet och dataskydd*, KS 2021/0474, beslutad den 1 december 2021, s. 3-4 och 8-9.

<sup>42</sup> *Anvisning organisation för säkerhet och dataskydd*, KS 2021/0474, beslutad den 1 december 2021, s. 8-9.

över nämndgränserna. Kontaktombuden har visat ett engagemang för frågorna, och har tankar och idéer om hur dataskyddsarbetet ska utvecklas i kommunen. Det finns en uttryckt vilja att få mer utbildning i GDPR, att ta del av kunskapsutbyte med andra kommuner och en vilja att få gehör för sitt arbete.

Ett annat positivt element är den GDPR-dag som hölls i maj 2025 i samverkan mellan Danderyd och Värmdö kommun samt Vaxholms stad. Dagen innehöll många goda exempel från de andra kommunerna som var inspirerande. Dataskyddspersonerna i Vaxholms stad har till exempel hållit en GDPR-månad i februari 2025 för hela kommunen med lättsamma inlägg på intranätet och diskussionslappar i matsalen för att öka GDPR-medvetenheten hos medarbetare.

Ett område som behöver insatser och omsorg den närmsta tiden, är kunskapen om organisationen för dataskyddsarbetet i kommunen, som har hamnat i viss obalans. Obalansen har uppstått efter omorganisation 2024 där administrativa funktioner på förvaltningarna centraliserades till kommunstyrelsen med innebörd att flera kontaktombudsplatser på förvaltningarna blev vakanta. Samtidigt omorganiserades även kommunledningskontoret och fick tre jämnstora avdelningar. En minskad förståelse för dataskyddsfrågorna har härigenom uppstått och avdelningarna upplevs, från ett dataskyddsperspektiv, som mer slutna. Jag utvecklar detta enligt följande.

För ett år sedan, i halvårsrapporten 2024, rekommenderade jag följande.

”En omorganisation i kommunen gör att majoriteten av befintliga kontaktombud på förvaltningarna inte längre ska ha kvar uppdraget, vilket inte belysts i omorganisationen. Det har beslutats att kontaktombudsrollen ska finnas kvar på förvaltningarna och inte centraliseras. Förvaltningarna har kommit olika långt i att lösa frågan. Dataskyddsombudet ser omedelbara risker för att det proaktiva GDPR-arbetet blir lidande och försvagas, om kontaktombud inte finns på plats. Dataskyddsombudet rekommenderar att [kommunen skyndsamt måste se till att kontaktombud kommer på plats].”<sup>43</sup>

I årsrapporten 2024, för fyra månader sedan, fann och rekommenderade jag följande.

”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 mäta med GDPR-arbetet.”<sup>44</sup>

I samband med att vissa GDPR-rutiner inte fungerat under våren 2025 har jag rekommenderat att de vakanta kontaktombudsplatserna på kommunledningskontoret behöver tillsättas. Verksamheten har då återkopplat att organisationen med kontaktombud behöver ifrågasättas. Dataskyddsförordningen är uppbyggd på så sätt att GDPR-kunskapen ska finnas verksamhetsövergripande, i alla verksamhetsgrenar. Jag vill därför

<sup>43</sup> *Dataskyddsombudets rapport från första halvåret 2024*, ärende 20240516:098, beslutad den 26 juni 2024, s. 5 och 7.

<sup>44</sup> *Dataskyddsombudets årsrapport 2024 för Danderyds kommun*, ärende 20240516:098, beslutad den 27 februari 2025, s. 11.

föregå med, att eventuella planer att ändra *Anvisningen*<sup>45</sup>, på så sätt att kontaktombudens roll, antal och arbetsuppgifter minskar, riskerar att få negativa konsekvenser för kommunens efterlevnad av dataskyddsförordningen.

I samband med Danderyds och Värmdö kommun samt Vaxholms stad gick in i kommunsamverkan, med ett gemensamt dataskyddsbud, kring oktober 2023, kom samverkanskommunerna överens om att varje kommun skulle hålla i en GDPR-dag med kunskapshöjande och nätverkande innehåll, en gång per år för samtliga dataskyddspersoner i de tre kommunerna.

Ett dataskyddsbud är skyddat av bestämmelser som ska säkerställa dataskyddsbudets oberoende och skydda dataskyddsbudet från otillbörlig påverkan.

Enligt art. 38 dataskyddsförordningen ska den personuppgiftsansvariga nämnden *tillhandahålla* dataskyddsbudet *de resurser* som krävs. Nämnden ska säkerställa att dataskyddsbudet *inte tar emot instruktioner* för sitt arbete och dataskyddsbudet *får inte avsättas eller bli föremål för sanktioner* för att ha utfört sina uppgifter.

Dataskyddsbudet ska rapportera till *högsta förvaltningsnivå*.

Under de dryga två år som kommunsamverkan pågått har dessa utbildningstillfällen fallit ut så att Danderyd har hållit i GDPR-dagen i januari/februari, Värmdö i maj och Vaxholm i september årligen. I samband med GDPR-dagen i maj 2025, som annonserats till deltagarna i januari 2025, anmälde och deltog endast två av Danderyds kommuns kontaktombud. Några kontaktombud hade inte fått delta på utbildningen, och andra kontaktombud hade förpliktelser som inte omfördelades.

I dialogen kring detta framförde verksamheten bland annat *att* det inte fanns behov av utbildning och kunskapsutbyte (nätverkande) i kommunsamverkan, *att* den planerade GDPR-dagen borde ställas in samt *att* kontaktombuden inte kan avsätta den tiden för utbildning eller GDPR på en årsbasis. Istället föreslogs att det kunde hållas interna korta digitala utbildningar, motsvarande någon timme, för kontaktombuden. Detta nya förhållningssätt i kommunen är något bekymmersamt genom att kontaktombuden, vilka redan upplever sig ha en beklämd roll (vilket utvecklas längre ned på sidan), får sämre förutsättningar att göra sitt arbete när utrymmet för utbildning, kunskapsutbyte och goda exempel begränsas. Förhållningssättet överensstämmer inte heller med vad kontaktombuden själva efterfrågar, se längre ned på sidan.

Efter Danderyds kommuns låga deltagande på GDPR-dagen håller jag på med en översyn av GDPR-dagarna i alla tre samverkanskommunerna, för att göra utbildningstillfällena mer tillgängliga, kunskapshöjande och *vassa*. Detta också för att väva in verksamhetens alternativa förslag ovan om kortare digitala utbildningar.

I översynen har kontaktombuden i Danderyds kommun framfört att *kontaktombudsuppdraget saknar värde för cheferna* och att kontaktombudens prestation i dataskyddsfrågorna varken följs upp i medarbetarsamtal eller i övrigt uppmärksammas eller premieras av cheferna. Det uttrycks en oro att cheferna inte förstår kontaktombudsuppdraget,

---

<sup>45</sup> *Anvisning organisation för säkerhet och dataskydd*, KS 2021/0474, beslutad den 1 december 2021.

regelverket, vikten av utbildning och kunskapsutbyte samt inte känner till den beslutade *Anvisningen*<sup>46</sup>. Det uttrycks en vilja att få delta på GDPR-dagen i september 2025.

Översynen har hittills visat, att den uppfattning som ibland framförs om att kontaktombuden endast motvilligt har sina kontaktombudsuppdrag, inte stämmer på generell nivå. Översynen har också visat att kontaktombuden saknar chefsstöd för att utföra sina arbetsuppgifter. Slutsatsen av översynen av hur GDPR-dagarna ska planeras framöver har ännu inte dragits.

Parallellt med detta, ser jag gärna att kommunen fortsätter arbeta med kontaktombudens roll och uppdrag samt chefernas stöd, ansvar och möjliggörande. Det får också gärna följas upp, om omorganisationen gett rätt förutsättningar för ett väl fungerande kommunövergripande dataskyddsarbete eller om ytterligare kontaktytor behövs. Oavsett hur översynen faller ut kommer kontaktombuden, utbildade som outbildade, inte komma någonstans i dataskyddsarbetet utan chefers gehör.

I juni 2025 noterades att kommunen hade 33 stycken personuppgiftsbiträdesavtal som *hängde i luften* i kommunen, där kommunen inte hade tillräcklig kompetens att leda arbetet framåt. Balansen har byggts upp under en tid då den centrala dataskyddsamordnaren inte var tillgänglig, vilket visar på en påtagligt sårbar personbundenhet. Dataskyddsamordnaren har i uppdrag att ge *råd* och *tillhandahålla stöd* till cheferna<sup>47</sup>, vilket förvisso kan innebära att bistå vid personuppgiftsbiträdesavtal i kommunstyrelsen och nämnderna. Dataskyddsamordnaren har emellertid *inte* något utpekat ansvar för att omhänderta kommunens samtliga personuppgiftsbiträdesavtal. Detta understryker också behovet av *att* bygga in dataskydd i verksamhetens rutiner och processer, *att* kontaktombuden ska få utbildning och rätt förutsättningar för sitt arbete, samt *att* kompetensen i verksamheten bör höjas.

---

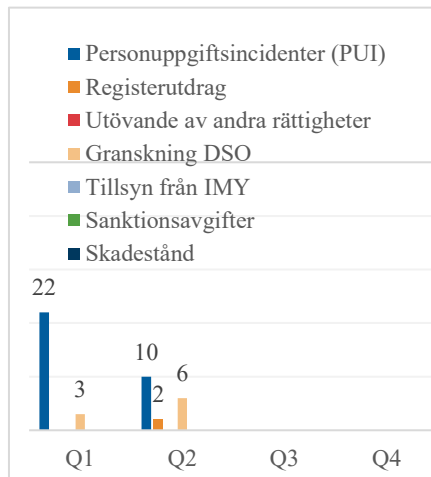
<sup>46</sup> *Anvisning organisation för säkerhet och dataskydd*, KS 2021/0474, beslutad den 1 december 2021.

<sup>47</sup> *Anvisning organisation för säkerhet och dataskydd*, KS 2021/0474, beslutad den 1 december 2021, s. 8-9.



## 4. Statistik för första halvåret 2025

Under detta avsnitt presenteras statistik för Danderyds kommun för första halvåret 2025.



Objekt	Antal ärenden	Antal ärenden (procent)
1	Reklam - Dataskydd	101
2	PUI	32
3	Underärenden	14
4	Granskning DSO	9
5	Övrigt - Dataskydd	8
6	Återkoppling på hemsida	3
7	Rådgivning internt	3
8	Rådgivning registrerad	1
9	Rapporter	1
10	Registerutdrag	2
	Summa	174

### 4.1 Behandlingsregistret

Av art. 30 dataskyddsförordningen framgår att varje personuppgiftsansvarig nämnd ska föra ett register över sina personuppgiftsbehandlingar. Exempel på personuppgiftsbehandlingar kan vara rekrytering och bokföring.

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

Danderyds kommun har 700 registrerade behandlingar av personuppgifter första halvåret 2025, varav 127 utgör *kommungemensamma behandlingar*, 168 rör *kommunstyrelsen*, 68 rör *utbildningsnämnden*, 52 rör *kultur- och fritidsnämnden*, 35 rör *tekniska nämnden*, 182 rör *socialnämnden*, 8 rör *valnämnden*, 13 rör *överförmyndarnämnden* och 47 rör *miljö- och stadsbyggnadsnämnden*. Därutöver finns 2 registrerade behandlingar som rör gamla *fastighetsnämnden*, vilka kommer arkiveras inom kort.

Antal registrerade behandlingar kan jämföras med tidigare års antal registrerade behandlingar enligt följande.

- 677 registrerade behandlingar av personuppgifter år 2024
- 587 registrerade behandlingar av personuppgifter år 2023

Framförallt är det *kultur- och fritidsnämnden* som med stöd av dataskyddssamordnare vidtagit åtgärder att se över sitt behandlingsregister och ökat antalet registrerade personuppgiftsbehandlingar.

En rättsakt i form av ett reglemente, som fastställer nämndernas inbördes ansvarsförhållanden och interna biträdesrelationer, har arbetats fram och avses att beslutas under hösten 2025.

Ett nytt system för registrering av behandling av personuppgifter har upphandlats och implementerats under våren.

## 4.2 Granskningar

Dataskyddsbudet övervakar efterlevnaden av dataskyddslagstiftningen och kommunens strategi för skydd av personuppgifter genom *granskning*.<sup>48</sup>

En granskning kan initieras till exempel genom att verksamheten ställer frågor till dataskyddsbudet om en pågående eller tilltänkt behandling av personuppgifter, att dataskyddsbudet själv uppmärksammar något som bör granskas närmare eller i samband med inträffade personuppgiftsincidenter.

Dataskyddsbudet har under första halvåret 2025 utfört nio (9) granskningar, enligt bild.

Svarsalternativ	Antal ärenden	Antal ärenden (procent)
1 Kommunstyrelsen	8	88.9
2 Socialnämnden	1	11.1
Summa	9	100%

Dataskyddsbudet har därutöver utfört

- två (2) granskningar som rörde *utbildningsnämnden* och
- en (1) granskning som rörde *socialnämnden*,

vilka visade sig utgöra personuppgiftsincidenter och som statistiskt tas upp under avsnittet 4.3.

Uppskattningsvis på en årsbasis skulle antalet granskningar kunna resultera i ca 18-24 granskningar för år 2025. Detta kan jämföras med tidigare års antal granskningar enligt följande.

- 21 granskningar år 2024
- 40 granskningar år 2023
- 44 granskningar år 2022

Nämnder som inte nämns har haft noll (0) granskningar.

Det sjunkande antalet granskningar, beror sannolikt på att min uppmärksamhet är fördelad på över 24 nämnder i tre olika kommuner. Det innebär, som jag påtalat i tidigare rapporterna tillika denna, att kommunen behöver ha en bemannad dataskyddsorganisation med kontaktombud på samtliga förvaltningar, avdelningar och enheter. Kontaktombuden behöver också få tillräckligt med insyn, utbildning och tid för att mäta med GDPR-arbetet.

### 4.2.1. Några granskningar

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

- *Kommunstyrelsen*: En planerad granskning av kommunens hantering av utökade bakgrundskontroller för rekrytering av *kritiska befattningar* har genomförts under våren. Justitieombudsmannen

<sup>48</sup> Jfr. art 39.1b [dataskyddsförordningen](#).

(JO) har funnit att bakgrundskontrollåtgärderna utgör en sådan *övervakning* och *kartläggning* av den enskildes personliga förhållanden som enskilda är skyddade mot från det allmänna (kommunen). Vid nyrekrytering kan dock finnas ett samtycke från kandidaten enligt 2 kap. 6 § 2 st. regeringsformen. Kommunen rekommenderas se över att bakgrundskontrollbolaget har tillstånd för att behandla uppgifter om lagföring samt intern personalsäkerhet, juridisk kunskap och integritet. Vidare rekommenderas kommunen se över definitionen av *kritiska befattningar* och *kontrollåtgärder*.

- *Kommungemensamt*: Leverantören för en av kommunens digitala ytor hade slagit på en funktion som innebar att anställdas röst spelades in, i syfte att minska brus vid videomöten. Enligt dataskyddsförordningen finns ett förbud för hantering av *biometriska uppgifter* som kan identifiera personer, om det inte går att stödja sig på något av undantagen. Verksamheten stängde under granskningen av funktionen.

En granskning planeras i flera nämnder. I samband med inträffade personuppgiftsincidenter brukas rekommenderas att tekniska eller organisatoriska åtgärder vidtas för att stävja liknande incidenter. Jag avser att på sikt följa upp om verksamheten har vidtagit tillräckliga åtgärder för att stävja nya incidenter.

#### 4.3 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.<sup>49</sup>

Incidenten ska anmälas till Integritetsskyddsmyndigheten inom 72 timmar, såvida det *inte är osannolikt* att incidenten medför en *risk för personers fri- och rättigheter*.<sup>50</sup>

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

<sup>49</sup> Jfr. art. 4 [dataskyddsförordningen](#).

<sup>50</sup> Art. 33 [dataskyddsförordningen](#).

tillräcklig utsträckning. Det är mindre troligt att ingen personuppgiftsincident inträffat under året, utan då kan antas finnas ett mörkertal.

Danderyds kommun har haft 32 personuppgiftsincidenter första halvåret 2025.

Uppskattningsvis skulle det kunna innebära 64 personuppgiftsincidenter för år 2025. Notera att *en* personuppgiftsincident endast statistiskt redovisas för *en* nämnd (den nämnd som främst berörts),

även om personuppgiftsincidenten kan ha berört flera nämnder.

Svarsalternativ	Antal ärenden	Antal ärenden (procent)
1 Utbildningsnämnden	12	37.5
2 Kommunstyrelsen	11	34.4
3 Miljö- och stadsbyggnadsnämnden	3	9.4
4 Socialnämnden	3	9.4
5 Kultur- och fritidsnämnden	2	6.2
6 Tekniska nämnden	1	3.1
Summa	32	100%

Antalet rapporterade personuppgiftsincidenter kan jämföras med tidigare års antal personuppgiftsincidenter enligt följande.

- 56 incidenter år 2024
- 57 incidenter år 2023
- 54 incidenter år 2022
- 38 incidenter år 2021

Sammantaget har incidenterna legat på en jämn nivå år 2022-2024, med drygt en rapporterad personuppgiftsincident i veckan på kommunövergripande nivå. Under första halvåret 2025 och framförallt kvartal 1 noteras en viss ökning i rapporterade incidenter. Några incidenter har varit större under terminen, men de flesta incidenter är av mindre allvarligt slag. Jag ser ingen oro till att antal incidenter ökar, utan bedömer det mer som ett tecken på att rapporteringsvägar fungerar och att kunskapen om att identifiera en personuppgiftsincident har ökat i verksamheten.

Nämnder som inte nämns har haft 0 personuppgiftsincidenter eller endast varit gemensamt med andra nämnder berörda av incidenten.

#### 4.3.1. Några personuppgiftsincidenter

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

- *Utbildningsnämnden*: Medarbetare på förskola hade publicerat bilder på barn från förskolan på sitt privata öppna Instagram-konto. Jag rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Utbildningsnämnden* och *kommunstyrelsen*: I samband med att medarbetare bytte chefer, försvann medarbetarnas digitala behörighetsinställningar och funktionalitet. Jag bedömde att anmälan till Integritetsskyddsmyndigheten inte behövde göras.
- *Utbildningsnämnden*: I samband med att en tidigare leverantör, Vklass, haft en överbelastningsattack, inledde jag granskning om kommunen haft kvar personuppgifter hos leverantören efter avtalets upphörande. Granskningen visade att leverantören inte hade gallrat personuppgifter om eleverna i enlighet med avtalet och leverantören

hade inte heller underrättat kommunen om överbelastningsattacken. Även efter att kommunen fick information om att personuppgifterna blivit raderade, fanns personuppgifter ändå kvar och det är idag inte helt säkerställt att personuppgifterna är helt raderade. Jag rekommenderade anmälan till Integritetsskyddsmyndigheten. Incidenten visar på det vi ofta ser, en fallenheten för att *spara*, men en avsaknad av både intresse och möjligheter att *gallra*.

- *Kultur- och fritidsnämnden, socialnämnden, miljö- och stadsbyggnadsnämnden och utbildningsnämnden*: Förlust av mobiltelefon, platta eller dator. Jag bedömde att incidenterna inte behövde anmälas till Integritetsskyddsmyndigheten.
- *Kommunstyrelsen*: I samband med lönerrevisionen genomfördes körningar av lönelistor, där lönefilen och samtliga lönespecifikationer, även bakåt i tiden, försvann. Uppgifter om lön, personnummer rör sig om *extra skyddsvärda personnummer*, och sjukfrånvaro om *känsliga personuppgifter*. Även om lönelistorna kunde återskapas genom back upp, innebar magnituden av förlusten och ovissheten kring hur den kunnat inträffa, att jag rekommenderade att incidenten behövde anmälas till Integritetsskyddsmyndigheten.
- *Utbildningsnämnden*: I samband med mediala skrivelser om Skolverket plattform för nationella provs brister i funktionalitet, inledde jag granskning om vad detta innebar för kommunen. Det visade sig att kommunen fört över personuppgifter om ca 400 elever i åk 6, 350 elever i åk 9, 950 elever på gymnasiet samt 150 anställda till plattformen, som under perioder inte kunde nås. Det rörde sig om förlust av personuppgifter och jag rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Kommunstyrelsen*: Vid expediering av allmänna handlingar följde en personlig blankett med finansiell information med. Jag rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Socialnämnden*: Vid ett möte mellan dataskyddsombud och regionen framkom att det gick att söka på förnamn och få upp samtliga handläggares profiler i samtliga kommuner i systemet *Lifecare* som används vid övergången från regional vård till kommunal omsorg. Dataskyddsombudet inledde granskning, och incidenten bekräftades. Jag rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Utbildningsnämnden*: Två system Schoolsoft och Edlevo brast i synkronisering, med *obehörig åtkomst, obehörigt röjande och ändring* av personuppgifter som följd, då vissa klasser digitalt fördubblats med antalet elever och andra klasser var digitalt tomma. Jag rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Kommunstyrelsen, miljö- och stadsbyggnadsnämnden och socialnämnden*: Under ett digitalt möte med leverantören av en maskningstjänst och med flera nämnder representerade visades

autentiska *sekretessbelagda* och *extra skyddsvärda personuppgifter* från en BBIC-utredning och två bygglovsansökningar för att påvisa brister i funktionalitet i maskningstjänsten. Inget personuppgiftsbiträdesavtal var tecknat vid tillfället och informationen röjdes utanför nämndgränserna. Jag rekommenderade att anmälan till Integritetsskyddsmyndigheten skulle göras och att de registrerade skulle underrättas.

- *Kommunstyrelsen*: En medarbetare fick återkommande annan medarbetares kalenderbokningar i egen kalender. Jag bedömde att anmälan till Integritetsskyddsmyndigheten inte behövde göras.
- *Tekniska nämnden*: En avfallsleverantör mejlade ut statistik gällande hämtning av förpackningar från flerfamiljshus och bostadsrättsföreningar till totalt sju Stockholmskommuner, innehållande 14 000 adresser, trots att endast kommunens egen statistik var relevant. I samband med incidenten identifierades att en liknande incident inträffat en gång tidigare. Jag rekommenderade anmälan till Integritetsskyddsmyndigheten. Leverantören har därefter tagit fram en rutin för att motverka fortsatta incidenter.
- *Kommunstyrelsen*: Två skrivare i kommunen identifierades ha inställningar på så sätt att det gick att se andra personers utskrifter. Jag bedömde, utifrån omständigheterna, att incidenten inte behövde anmälas till Integritetsskyddsmyndigheten. Inställningarna kunde ses över och skrivarna skulle bytas ut.
- *Kommunstyrelsen, utbildningsnämnden, tekniska nämnden, miljö- och stadsbyggnadsnämnden, kultur- och fritidsnämnden och socialnämnden*: I nätverk med annan kommun framkom att handlingar försvunnit i ett verksamhetssystem, som Danderyds kommun också använder. Vid intern kontroll identifierades att ca 370 handlingar förlorats i kommunens system. Jag rekommenderade anmälan till Integritetsskyddsmyndigheten.

#### 4.4 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.

#### 4.5 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 (2) begäran om registerutdrag inkommit under första halvåret 2025 som framförallt rört *kommunstyrelsen, miljö- och stadsbyggnadsnämnden, socialnämnden* och *utbildningsnämnden*.

#### 4.6 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 återopande av andra rättigheter inkommit under året.

#### 4.7 Tillsyn och sanktionsavgifter

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

Integritetsskyddsmyndigheten har deklarerat att de under år 2025 kommer fokusera på att bedriva tillsyn inom arbetsliv, omsorg, kamerabevakning, AI och i verksamhet som gäller barn.<sup>51</sup>

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

\_\_\_\_\_

---

<sup>51</sup> Integritetsskyddsmyndighetens *Tillsyns- och vägledningsprioriteringar 2025*, diarienummer IMY-2025-5238, beslutad den 13 mars 2025; <https://www.imy.se/globalassets/bilder/publikationer/tillsyns--och-vagledningsprioriteringar-2025.pdf>