# Dataskyddsombudets årsrapport 2023

| Diarienummer | | Senast uppdaterad | Beslutsinstans | Processägare |
|---|---|---|---|---|
| 20230227:036 | | 2024-02-01 | Dataskyddsombud | Dataskyddsombud |

## Dokumentets syfte

Dataskyddsombudets årsrapport tas fram av dataskyddsombudet och syftar till att återkoppla till den personuppgiftsansvariga nämnden och kommunledningsgruppen om dataskyddsombudets iakttagelser av kommunens hantering av personuppgifter under året.

Detta för att nämnden ska kunna ta sitt, enligt dataskyddsförordningen, ställda personuppgiftsansvar och kunna redovisa sin efterlevnad av dataskyddsförordningen.[1]

## Dokumentet gäller för

Årsrapporten riktas främst till respektive personuppgiftsansvarig nämnd och kommunledningen, men är även aktuell för 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, 2023-11-17).

# Innehållsförteckning


**Inledning** ..... **3**

**1 DEL 1 – Dataskyddsombudet tar ordet** ..... **3**

1.1 En utökad problembild ..... 3

1.2 Framgångsfaktorer för inbyggt dataskydd ..... 4

1.3 Dataskyddsombudets granskningar ..... 6

**1.3.1 Några granskningar av större vikt** ..... **7**

1.4 På gång år 2024 ..... 9

**2 DEL 2 - Statistik och dataskyddsombudets reflektioner** ..... **9**

2.1 Danderyds kommuns statistik år 2023 ..... 9

2.2 Behandlingsregistret ..... 10

2.3 Personuppgiftsincidenter ..... 10

**2.3.1 Statistik år 2023 för Danderyds kommun** ..... **11**

**2.3.2 Jämförelse per år** ..... **11**

**2.3.3 Några personuppgiftsincidenter av större vikt** ..... **11**

**2.3.4 Dataskyddsombudet kommenterar antalet personuppgiftsincidenter** ..... **14**

2.4 Skadestånd ..... 14

2.5 Registerutdrag ..... 15

2.6 Andra rättigheter ..... 15

2.7 Tillsyn och sanktioner av tillsynsmyndighet ..... 15

2.8 Risk och konsekvensbedömningar ..... 15

**3 DEL 3 – Rättsutveckling, praxis och vägledning** ..... **15**

3.1 Ny praxis och rättsutveckling ..... 15

**3.1.1 EU-domstolen har satt ned foten om administrativa sanktionsavgifter** ..... **15**

**3.1.2 Google workspace, avsaknad av konsekvensbedömning ledde till sanktionsavgift** ..... **16**

**3.1.3 Allvarlig kritik mot kommun som infört kontinuerligkontroll huruvida anställda dömts för brott** ..... **16**

**3.1.4 Arbetsgivare använde anställds e-postkonto** ..... **17**

**3.1.5 Reklam som riktas efter analys av användarens beteenden – Meta/Facebook** ..... **17**

**3.1.6 Brister i anställdas bärbara datorer ledde till sanktionsavgift** ..... **18**

**3.1.7 Integritetsskyddsmyndighetens nedläggningsbeslut är överklagbara** ..... **18**

3.2 Rykande färska vägledningar ..... 18

**3.2.1 Kamerabevakning** ..... **18**

**3.2.2 DIGG:s och IMY:s vägledning om dataskydd och innovation** ..... **18**

**3.2.3 Artificiell intelligens inom vård- och omsorgssektorn** ..... **19**

# Inledning

Dataskyddsombudets årsrapport syftar till att hålla de personuppgiftsansvariga nämnderna och kommunledningsgruppen informerade om dataskyddsombudets iakttagelser av kommunens hantering av personuppgifter.

Rapporten är indelad i främst tre delar;

1. Dataskyddsombudet tar ordet (och redogör bland annat för sina granskningar av kommunens regelefterlevnad).
2. Dataskyddsombudets redovisar statistik för personuppgiftsincidenter, begäran av skadestånd, registerutdrag eller andra rättigheter, tillsyn och sanktionsavgifter.
3. Dataskyddsombudets redogör för nytillkommen praxis och vägledningar som kan underlätta personuppgiftsarbetet, med rekommendation att dessa beaktas och följs.

Denna årsrapport ska redovisas i samtliga nämnder. Dataskyddsombudets rekommendationer lämnas löpande i texten.

# 1 DEL 1 – Dataskyddsombudet tar ordet

Dataskyddsombudet i Danderyds kommun har sedan den 1 oktober 2023, även axlat rollen som dataskyddsombud för Värmdö kommun och Vaxholms stad. Uppföljning kommer att ske tidig höst år 2024. Berörda kommuner har informerats på intranätet om den nya ordningen.

Detta får stor betydelse i positiv bemärkelse för de tre berörda kommunerna på så sätt att det nu finns möjlighet till samarbete och erfarenhetsutbyte mellan kommunerna, på ett helt nytt sätt. Genom att kommunernas respektive funktioner lär känna varandra, går det att gemensamt förhandla med en leverantör om till exempel personuppgiftsbiträdesavtalet. Det pågår ett arbete att skapa stora och små nätverk mellan kommunerna. Danderyds kommun har bjudit in till en utbildningsdag med samtliga dataskyddssamordnare och kontaktombud som kommer att hållas i Danderyds kommun i februari 2024, se vidare avsnitt 1.4.

I denna årsrapport vill dataskyddsombudet belysa vikten av att ha *inbyggt dataskydd i verksamheten* för att kommunen ska kunna klara av att hålla regelefterlevnaden av dataskyddsförordningen, enligt följande.

## 1.1 En utökad problembild

Utöver att bristande regelefterlevnad av dataskyddsförordningen, inte är laglig[2], finns även några mjukare faktorer att belysa. *Den mänskliga faktorn*

[2] Jfr. art 5.2 dataskyddsförordningen.

har de senaste tre åren varit anledningen till cirka 60 procent av alla rapporterade personuppgiftsincidenter.[3]

- Det medför att verksamheten måste, dels med *tekniska åtgärder* (som *privacy by design* och ”lätt att göra rätt”), dels med *organisatoriska åtgärder* (som framtagande av styrdokument, systemstöd, tillräcklig tid och utbildning) – fokusera på att minska riskerna att göra fel på grund av mänsklig faktor.

Ny praxis från EU-domstolen visar på att den juridiska personen är ansvarig *för överträdelser av varje person* som agerar inom affärsverksamheten och för den juridiska personens räkning. *Det krävs inte att en identifierbar fysisk person vidtagit överträdelsen. Det krävs inte att ledningsgruppen känt till överträdelsen, för att en administrativ sanktionsavgift ska kunna utdömas*.[4]

Det räcker alltså att *en* handläggare i kommunen påbörjat en felaktig behandling av personuppgifter för att personernas fri- och rättigheter skulle kunna äventyras och nämnden kunna ådömas en sanktionsavgift. Detta visar på vikten av att dataskyddskunskap finns hos medarbetarna.

Det är därför av avsevärd vikt att kommunen arbetar långsiktigt med att försöka på hållbart, säkert och långsiktigt sätt bygga in ett starkt dataskydd i sina samtliga verksamhetsområden. Nämnderna och ledningsgruppen måste komma till insikt om, och ta, sitt ansvar.

### 1.2 Framgångsfaktorer för inbyggt dataskydd

Dataskyddsombudet bedömer att det finns några givna framgångsfaktorer för att bygga in det dataskydd i verksamheten, som krävs för regelefterlevnad av dataskyddsförordningen, enligt följande.

i. Nämnd och ledningsgrupp måste aktivt och föredömligt verka för ett gott och inbyggt dataskydd i verksamheten. Förstår inte nämnd och ledningsgrupp sitt ansvar, går det inte att bygga in dataskydd i verksamheten.

ii. Medarbetare ska ha baskunskap i GDPR och ska kunna klara av enklare GDPR-bedömningar på egen hand.

iii. Behandlingsregistret (med kommunens personuppgiftsbehandlingar) ska aktivt hålls uppdaterat så att verksamheten har koll på sina

[3] Rapport om anmälda personuppgiftsincidenter, s. 19, https://www.imy.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2022.pdf (den 14 juni 2023).
(den 11 december 2023).

[4] Samtliga punkter: EU-domstolens mål C-683/21 *Nacionalinis visuomenės sveikatos centras* och C-807/21 *Deutsche Wohnen*; EU-domstolens pressmeddelande nr 184/23, den 5 december 2023, https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-12/cp230184sv.pdf (den 11 december 2023).

behandlingar. Nästa steg är att ha kontroll över sina dataflöden, alltså hur informationen flödar mellan system, underbiträden etc.

iv. En bestämd och tydlig organisation för dataskyddsombud, dataskyddssamordnare och kontaktombud, där samtliga roller har ett klart och uttalat mandat. Varje medarbetare och chef ska känna till var den kan vända sig om den inte kan lösa ut GDPR-frågan på egen hand, och kontaktombudet och dataskyddssamordnaren ska känna att den får gehör för sitt arbete.

v. Särskilt vid upphandling, projektledning och ny digital hantering måste det finnas ett inbyggt dataskydd, med kontrollfunktioner. En miniminivå torde vara att kontaktombudet involveras så fort det är känt att hanteringen inbegriper personuppgiftsbehandling. Redan när upphandlingen tillkännages bör verksamheten ha kravställt hur leverantören ska hantera kommunens personuppgifter vad gäller till exempel säkerhetsåtgärder, dataflöden, lagring och gallring.

vi. En tydlig process för hantering av personuppgiftsincidenter.

vii. Personuppgiftsbiträdesavtal eller datadelningsavtal ska finnas i samtliga fall där personuppgiftsbiträden eller dataflöden mellan olika organ finns.

Vad gäller Danderyds kommun bedömer dataskyddsombudet att en god grund finns för nästan samtliga punkter, att utveckla och kunna stärka upp ifrån, enligt följande.

- En tydlig process för personuppgiftshantering finns (*vi*).
- Dataskyddssamordnaren har under året gjort gedigna insatser att få koll på kommungemensamma behandlingar och att få en enhetlighet i behandlingsregistret (*iii*) samt i övrigt styra upp och stötta vad gäller personuppgiftsbiträdesavtalen (*vii*).
- En tydlig organisation för dataskydd finns i styrdokumentsform (*iv*), men en enkätundersökning visar att vissa kontaktombud inte känner till vilka arbetsuppgifter de har, samt att cheferna förväntar sig att dataskyddsfrågorna inte ska ta någon tid i anspråk.
- Nämnder och ledningsgrupp (*i*) har en grundläggande förståelse för sitt ansvar och uppdrag, men utifrån punkten ovan finns förbättringsåtgärder. Det finns i övrigt både bättre och sämre exempel från verkligheten. Ofta är det i samband med chefsväxlingar som eventuella sämre exempel uppstår.
    - Det finns föredömliga exempel där nämnderna till exempel har stående punkter på sin dagordning för information om pågående dataskyddsfrågor, incidenter och liknande; samt där verksamheten på ett organiserat och strukturerat sätt informerar den personuppgiftsansvariga nämnden inom ansvarsområdet.

- Det finns föredömliga exempel från verksamheten, där gjorda risk- och konsekvensbedömningar nu har ökat, personuppgiftsbiträdesavtalen ses över och nya avtal ingås samt medarbetare har gott engagemang och driv i frågorna (*ii*).
- En något sämre hantering skedde i anslutning till en av dataskyddsombudet större granskningar, som först anmäldes till nämndsammanträdet efter dataskyddsombudets behövt påpeka det. Trots att dataskyddsombudet begärt att muntligen få föredra granskningen för nämnden, skickades ingen kallelse till det aktuella sammanträdet ut. Än så länge betraktas detta som en isolerad händelse, och dataskyddsombudet ser fram emot att få hålla den muntliga föredragningen under våren 2024 i stället.
- En händelse på samma förvaltning, men en annan nämnd, innebar att dataskyddsombudet fick vänta ett halvår på att få svar från chef i en granskning.[5]

- Trots att förenklad och fördjupad utbildning inom dataskydd finns, samt lättillgängliga externa och interna utbildningsfilmer, bedömer medarbetare (*ii*) att dataskydd är för svårt och utbildningarna för mastiga. Det är en svår avvägning om utbildningen ska förenklas och kraven på medarbetare sänkas, eller om det är precis tvärtom, att utbildningen borde vara gedigen för att höja nivån av kunskap. Arbetet pågår.
- Funktioner för inbyggt dataskydd i upphandling, projektledning och digital hantering (*v*) bedömer dataskyddsombudet vara ett viktigt utvecklingsområde.

### 1.3 Dataskyddsombudets granskningar

Dataskyddsombudet övervakar efterlevnaden av dataskyddslagstiftningen och kommunens strategi för skydd av personuppgifter genom granskningar.[6]

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

Danderyds kommuns dataskyddsombud har under år 2023 utfört 38 granskningar fördelade enligt nedan. Notera att granskningar som gällt flera nämnder, endast räknas som *en* granskning under *en* nämnd, vanligen under kommunstyrelsen i sin samordnande funktion. Nämnder som inte nämns har haft 0 granskningar eller kommunövergripande granskningar.

[5] Jfr. art 33 och 38.2 dataskyddsförordningen.
[6] Jfr. art 39.1b dataskyddsförordningen.

| | Svarsalternativ | Antal ärenden | Antal ärenden (procent) |
|---|---|---|---|
| 1 | Kommunstyrelsen | 23 | 60.5 |
| 2 | Socialnämnden | 6 | 15.8 |
| 3 | Utbildningsnämnden | 6 | 15.8 |
| 4 | Valnämnden | 1 | 2.6 |
| 5 | Tekniska nämnden | 1 | 2.6 |
| 6 | Kultur- och fritidsnämnden | 1 | 2.6 |
| | Summa | 38 | 100% |

### 1.3.1 Några granskningar av större vikt

Även om exemplen rör specifika nämnder, är riskerna befintliga för samtliga nämnder. Nämnderna behöver lära av varandra, varför exemplen är relevanta för samtliga nämnder. Avsikten är att exemplen ska vara lärande och inte läxande.

- Samtliga nämnder: Dataskyddsombudet har tagit fram en promemoria med rekommendationer utifrån adekvansbeslutet ”EU-US Data Privacy Framework”, kallat Ramverket, och dess betydelse för verksamheten samt lämnat rekommendationer, till exempel att avtalen bör innehålla en möjlig *exit*-klausul, utan att kommunen ska behöva utge vite/skadestånd.[7]
- Socialnämnden: Dataskyddsombud och dataskyddssamordnare har genom återkommande dialog med StorSTHLM försökt få till ett personuppgiftsbiträdesavtal med regionen för LifeCare, inklusive analys av potentiella risker och behov av riskminimerande åtgärder.
- Samtliga nämnder: Verksamheten har tagit bort en funktion för att skicka säker e-post med kryptering, *säkra meddelanden*, då kostnaden inte bedömts proportionerlig, i och med att ytterst få använt funktionen. Borttagandet skedde mot dataskyddsombudets rekommendationer. Dataskyddsombudet anser att kommunen måste ha möjligheter att skicka säker e-post, och att kommunen i stället borde arbetat med implementering av funktionen. Detta kopplas också till ökade personuppgiftsincidenter vid e-posthantering. Granskningen pågår.
- Kultur- och fritidsnämnden: Dataskyddsombudet har inlett granskning av ny tjänst för e-böcker på biblioteken, som visat sig

[7] I fulltext: Dataskyddsombudets PM med rekommendationer efter adekvansbeslutet EU-US Data Privacy Framework, den 25 september 2023 i ärende 20230921:165.

innehålla profilering, har underbiträden i tredjeland samt hanterar sekretessbelagda uppgifter.[8] Granskningen pågår.

- Socialnämnden: Dataskyddsombudet har granskat en konsekvensbedömning om videoinspelning av handläggare vid klientsamtal inom familjeterapi i utbildningssyfte.
    - Dataskyddsombud såg ingen oförenlighet med dataskyddsförordningen att filma handläggaren med ljud och bild under de premisser med förvaring, lösenord och radering som lagts fram.
    - Däremot avrådde dataskyddsombudet för ljudupptagning av klienters (inbegripet barns) autentiska berättelse.

#### *1.3.1.1 Dataskyddsombudet har granskat grundskolans plattformar[9]*

Utbildningsnämnden har en särställning i förhållande till andra nämnder på så sätt att utbildningsverksamheten i sin verksamhet behandlar i princip uteslutande;

- *extra skyddsvärda personuppgifter* (uppgifter om barn, personnummer, integritetskänsliga uppgifter),
- *känsliga personuppgifter* (uppgifter om hälsa, etniskt ursprung [modersmål] och religion [kost]) och,
- *sekretessbelagda uppgifter* (till exempel uppgifter om hälsa, skyddade personuppgifter).

Dataskyddsombudet har i en större granskning granskat grundskolans plattformar i utbildningsverksamheten. Verksamheten har under granskningens gång tagit fram flera styrdokument (vilka ej har beslutats) och identifierat flera utvecklingsområden samt generellt höjt kunskapen inom GDPR.

Dataskyddsombudet har identifierat brister och utvecklingsområden. Till exempel saknas styrdokument, det finns risker för röjande och samtliga system har bristande gallring. Behandlingsregistret behöver uppdateras. Det saknas konsekvensbedömningar, även om ett arbete pågår. Skolornas möjlighet till individuella avsteg och behörighetstilldelning innebär också risker.

Dataskyddsombudet har rekommenderat att tekniska och organisatoriska åtgärder vidtas. Det är nämndens och ledningens ansvar att se över hanteringen.

---

[8] Bonnier, har i ett annat ärende, ålagts en administrativ sanktionsavgift på 13 miljoner för profilering.

[9] I fulltext: Dataskyddsombudets granskning och rekommendationer för grundskolans system i utbildningsverksamheten (er ref UN 2023/0804), den 17 oktober 2023 i ärende 20221107:74.

### 1.4 På gång år 2024

I februari 2024 har dataskyddsombudet bjudit in till heldag med GDPR i Danderyds kommun för samtliga tre kommuners dataskyddskontakter och centrala dataskyddssamordnare. Syftet är att kommunerna ska få ett utökat kontaktnät i dataskyddsfrågor genom att lära känna sina respektive funktioner på de andra kommunerna.

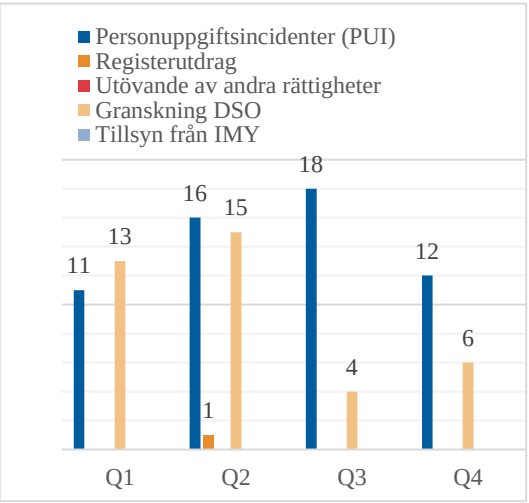
En tämligen tung dagordning av dataskyddsfrågor finns på agendan. Under dagen kommer föreläsare från

- Sveriges Kommuner och Regioner (SKR) som ska fördjupa diskussionerna kring innovation och digitalisering och personuppgiftbiträdesavtal samt
- StorSTHLM som ska fördjupa diskussionerna vad gäller kommungemensamma system och den digitala framtiden.

Därutöver kommer GDPR-utmaningar med personuppgiftsincidenter, personuppgiftsbiträdesavtal och övriga utmaningar under år 2024, att processas under dagen.

# 2 DEL 2 - Statistik och dataskyddsombudets reflektioner

### 2.1 Danderyds kommuns statistik år 2023




| | Objekt | Antal ärenden | Antal ärenden (procent) |
|---|---|---|---|
| 1 | Reklam - Dataskydd | 177 | 44.6 |
| 2 | Underärenden | 62 | 15.6 |
| 3 | PUI | 57 | 14.4 |
| 4 | Övrigt - Dataskydd | 41 | 10.3 |
| 5 | Granskning DSO | 38 | 9.6 |
| 6 | Rådgivning internt | 16 | 4.0 |
| 7 | Rådgivning registrerad | 4 | 1.0 |
| 8 | Rapporter | 1 | 0.3 |
| 9 | Registerutdrag | 1 | 0.3 |
| | Summa | 397 | 100% |

Specificering av kategorier enligt följande.

*Reklam* rör främst erbjudanden om kurser inom dataskydd etc. *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. *Rådgivning internt* är främst huvudkontaktombudets

redskap för intern rådgivning. *IMY* rör främst post eller beslut från Integritetsskyddsmyndigheten gällande anmälda personuppgiftsincidenter. Oftast diarieförs dessa handlingar i verksamhetens system för personuppgiftsincidenten, men ibland skickas de till dataskydd för kännedom. *Rådgivning registrerad* rör främst ärenden där allmänheten ställer frågor till dataskyddsombudet eller huvudkontaktombudet. *Rapporter* rör främst dataskyddsombudets kvartals- och årsrapporter.

## 2.2 Behandlingsregistret

Varje personuppgiftsansvarig nämnd ska föra ett register över personuppgiftsbehandlingar som utförs av nämnden, inbegripet förvaltningen.[10]

Danderyds kommun har 587 registrerade behandlingar av personuppgifter, varav 43 rör kommungemensamma, 178 rör kommunstyrelsen, 68 rör utbildningsnämnden, 33 rör kultur- och fritidsnämnden, 24 rör tekniska nämnden, 177 rör socialnämnden, 5 rör valnämnden, 13 rör överförmyndarnämnden och 46 rör miljö- och stadsbyggnadsnämnden.

Flera utvecklingsområden har identifierats såsom bristande enhetlighet mellan nämnderna och oklarheter *hur* kommungemensamma behandlingar ska registreras. Dataskyddssamordnare och kontaktombuden arbetar för att få till kommungemensam samsyn och rutiner för hanteringen.

Behandlingsregistret är under översyn av dataskyddssamordnare och kontaktombud. Ett nytt register som avser kommungemensamma behandlingar har initierats under året, och vissa av kommunstyrelsen 178 personuppgiftsbehandlingar kommer flyttas till kommungemensamma behandlingar längre fram.

## 2.3 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.
- Personuppgiftsincidenten ska anmälas till Integritetsskyddsmyndigheten inom 72 timmar, *såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter*. Personuppgiftsincidenter ska registreras i respektive nämnds diarium.
- Ärenden identifieras genom till exempel personuppgiftsincidents-anmälan från leverantör, frågor och anmälningar som verksamheten skickat till dataskyddsombudet eller av dataskyddsombudet själv vid

[10] Jfr. art 30 dataskyddsförordningen.

kontakter med verksamheten (genom till exempel granskningar, personuppgiftsincidenter och konsekvensbedömningar).

### 2.3.1 Statistik år 2023 för Danderyds kommun

Danderyds kommun har under år 2023 haft 57 personuppgiftsincidenter, alltså uppskattningsvis cirka en personuppgiftsincident i veckan. De flesta incidenter är av mindre allvarligt slag. Nedan presenteras statistik för samtliga personuppgiftsincidenter som registrerats i systemet för dataskydd under 2023 per nämnd. Ytterligare ärenden som registrerats vid en tidigare tidpunkt kan ha avslutats under året.

Notera att en personuppgiftsincident som rör flera nämnder, endast registreras som *en* incident under *en* nämnd. Nämnder som inte nämns nedan har haft 0 personuppgiftsincidenter.

| | Svarsalternativ | Antal ärenden | Antal ärenden (procent) |
|---|---|---|---|
| 1 | Utbildningsnämnden | 22 | 38.6 |
| 2 | Socialnämnden | 19 | 33.3 |
| 3 | Kommunstyrelsen | 10 | 17.5 |
| 4 | Tekniska nämnden | 5 | 8.8 |
| 5 | Kultur- och fritidsnämnden | 1 | 1.8 |
| | Summa | 57 | 100% |

### 2.3.2 Jämförelse per år

- År 2022: Danderyds kommun hade totalt 54 personuppgiftsincidenter år 2022, varav den nämnd som hade flest hade 27 incidenter och de nämnder som hade minst hade 0 incidenter.
- År 2021: Danderyds kommun hade totalt 38 personuppgiftsincidenter år 2021.

### 2.3.3 Några personuppgiftsincidenter av större vikt

Även om exemplen rör specifika nämnder, är riskerna befintliga för samtliga nämnder. Nämnderna behöver lära av varandra, varför exemplen är

relevanta för samtliga nämnder. Avsikten är att exemplen ska vara lärande och inte läxande.

Några incidenter kan kort kommenteras enligt följande.

- Kommunstyrelsen (och samtliga nämnder): Genom förebyggande arbete upptäcktes att 440 av kommunens personals e-postadresser och lösenord fanns delvis tillgängliga, med möjlighet till tillgängliggörande, på nätet. Upptäckten ledde till omedelbart lösenordsbyte för samtliga medarbetare i kommunen. Incident anmäldes till Integritetsskyddsmyndigheten enligt dataskyddsombudets rekommendation och medarbetare underrättades på intranätet.
    - I senare ärende har också registrerade misslyckade inloggningsförsök konstaterats från Sao Paulo, Peking och så vidare.
- Flera nämnder: Antagonistiska angrepp har år 2023 skett hos kommunens leverantörer vad gäller,
    - Indra (gymnasieantagningen),
    - Ungdoms- och elevdatabasen (UEDB),
    - Trygghetslarm,
    - Samtrans (transport) och
    - Visma (rekryteringssystemet).

  Vid ett identifierat antagonistiskt angrepp stängs systemet i regel ned för att avbryta angreppet. Det kan också röra sig om att den antagonistiska aktören krypterar data i utpressningssyfte. Detta leder vanligen till i vart fall tillfällig *förlust* eller *ändring* av personuppgifter och sätter i regel systemet ur funktion, vilket utgör en personuppgiftsincident. Därutöver kan det antagonistiska angreppet i sig innebära ett *obehörigt röjande* och *obehörig åtkomst*. I vissa fall kan datan behöva återskapas från säkerhetskopior.

  Dataskyddsombudet vill skicka med att det vid i princip varje antagonistiskt angrepp under 2023 har lämnats motsägelsefull, bristfällig och osäker information från leverantören och andra. Dataskyddsombudet rekommenderar att kommunen ställer krav i upphandlingen på loggning och spårbarhet hos leverantörerna, samt att ta den information som kommer från leverantören vid ett antagonistiskt angrepp, med viss försiktighet. Det ligger i leverantörens natur att försöka att inte förlora kundernas förtroende, och inte sällan uppdagas att leverantören brister i dataskyddskomptens när ett angrepp väl skett.

  Dataskyddsombudet rekommenderar aktiv, och gärna systematisk, gallring av personuppgifter som kommunen inte längre behöver, dels är det ett krav enligt dataskyddsförordningen, dels minskar det risken för att någon obehörig kommer över personuppgifterna.

- Socialnämnden, utbildningsnämnden: Flera incidenter har rört leverantören för transport vad gäller *obehörig åtkomst* och *röjande*, eller *ändring* av elevers personuppgifter. Dataskyddsombudet har lämnat rekommendation om anmälan till Integritetsskydds-myndigheten i samtliga fall. Verksamheten har i dialog med leverantören gjort omfattande insatser att få till en korrekt hantering. På senare tid har rapporterade incidenter avtagit.
- Kommunstyrelsen, socialnämnden: Handläggare har fått mejl som utformats för att se ut som, att mejlet varit från chef på kommunledningskontoret och advokatbyrå. Mejlen har inte varit autentiska, utan skickats i otillbörligt syfte att tillskansa sig kommunens medel. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten med mera.
- Socialnämnden: En analysfunktion identifierade att de behandlat personuppgifter i flera års tid utan att ha registrerat sina personuppgiftsbehandlingar. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten.
- Tekniska nämnden: E-postadresser till ca 100 medborgare och andra som valt att prenumerera på information om ett kommunalt projekt röjdes för varandra då kommunen missat att använda dold kopia.
- Utbildningsnämnden: Elever i kommande årskurs laddades upp för tidigt i Vklass, med konsekvens att nya och gamla elever kunde se varandras personuppgifter. Incidenten upptäcktes och raderades inom några timmar.
- Flera nämnder: Dataskyddsombudet har noterat att flera personuppgiftsincidenter har haft koppling till e-posthantering. Till exempel
    - *att* skolor mejlat in information om personer med skyddade personuppgifter till kommunen vid två tillfällen,
    - *att* e-postadresser till vårdnadshavare varit synliga vid kommunens mejlutskick rörande ett kränkningsärende på en skola,
    - *att* e-postadresser till allmänheten varit synliga vid kommunens massutskick till ca 100 personer (nämnt ovan),
    - *att* kommunen angett e-post som en kontaktväg för klienter med följd att klient mejlar in känslig och sekretessbelagd information till kommunen utan kryptering,
    - *att* en e-post mellan två handläggare där en klient nämndes med namn och kontaktuppgifter, skickades oavsiktligen till en av kommunens elever, och

- *att* e-postadresser till vårdnadshavare varit synliga vid kommunens mejlutskick inom samma modersmål, vilket indirekt avslöjat etniskt ursprung som utgör en känslig personuppgift.

Dataskyddsombudet kan bara understryka att kommunen bör kunna erbjuda allmänheten, klienter och andra aktörer kommunikation och information i säkra, konfidentiella och i kommunens egna kanaler, och att bristen på detta leder till identifierade personuppgiftsincidenter. Detta sammanfaller också olyckligt med att kommunen tagit bort funktionen för säker kommunikation.

### 2.3.4 Dataskyddsombudet kommenterar antalet personuppgiftsincidenter

Det finns ingen lägsta nivå för vad som kan utgöra en personuppgiftsincident. Det kan i princip förväntas att i vart fall något mejl, sms, brev eller faktura skickas fel, eller mottas av fel instans eller att något system tillfälligt buggar eller ligger nere. Det innebär att det ska finnas ett flöde av inrapporterade personuppgiftsincidenter, om rapporteringen fungerar. Vissa nämnder hanterar i större utsträckning *extra skyddsvärda* och *känsliga personuppgifter*, än andra nämnder, vilket kan påverka antalet incidenter.

- Om en nämnd har *många personuppgiftsincidenter* kan det tala för att verksamheten har god kännedom om dataskyddslagstiftningen och identifierar samt anmäler personuppgiftsincidenter när sådana inträffar. Det kan också tala för en sämre hantering av personuppgifter.
- Om en nämnd har *få personuppgiftsincidenter* kan det tala för en god hantering av personuppgifter. Det kan också talat för att personuppgiftsincidenter inte identifieras och rapporteras i den utsträckning som dataskyddsförordningen faktiskt kräver.
- Om en nämnd *inte har någon anmäld* personuppgiftsincident under året, rekommenderas nämnden se över huruvida identifikation och rapportering av personuppgiftsincidenter fungerar som dataskyddsförordningen kräver. Det är mindre troligt att ingen personuppgiftsincident skulle ha inträffat under året.

## 2.4 Skadestånd

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

Det har inte kommit till dataskyddsombudets kännedom att något krav på skadestånd riktats mot Danderyds kommun under år 2023.

### 2.5 Registerutdrag

| |
|---|
| Den registrerade har rätt att begära ut ett registerutdrag med information om kommunens personuppgiftsbehandling som rör denne. |

Av vad som kommit till dataskyddsombudets kännedom har en person begärt ut registerutdrag från Danderyds kommuns samtliga nämnder.

### 2.6 Andra rättigheter

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

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

### 2.7 Tillsyn och sanktioner av tillsynsmyndighet

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

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

### 2.8 Risk och konsekvensbedömningar

Risk- och konsekvensbedömningar, vilka ska göras för all personuppgiftsbehandling med hög risk, har ökat från ett fåtal till 28 stycken under året. Detta har skett i samverkan mellan dataskyddssamordnare, kontaktombuden och förvaltningarna.

## 3 DEL 3 – Rättsutveckling, praxis och vägledning

### 3.1 Ny praxis och rättsutveckling

#### 3.1.1 EU-domstolen har satt ned foten om administrativa sanktionsavgifter

EU-domstolen kom fram till följande.[11]

(den 11 december 2023).

- För att tilldelas en administrativ sanktionsavgift krävs *vållande*, alltså antingen *uppsåt* eller *oaktsamhet*.
- Den juridiska personen är ansvarig för överträdelser av dess företrädare, direktörer, förvaltare och *för varje person som agerar inom ramen för den juridiska personens affärsverksamhet och för dennes räkning*. Det krävs inte att en identifierbar fysisk person vidtagit överträdelsen. *Det krävs inte att ledningsgruppen känt till överträdelsen för att administrativ sanktionsavgift ska utdömas*.
- Personuppgiftsansvarig kan påföras administrativ sanktionsavgift för *personuppgiftsbiträdets behandling* av personuppgifter.
- För ett *gemensamt personuppgiftsansvar* krävs inte att det föreligger en formell överenskommelse, utan det räcker att det finns ett gemensamt beslut eller samstämmiga beslut hos parterna. När ett gemensamt personuppgiftsansvar är konstaterat krävs ett inbördes arrangemang för att fastställa respektive parts ansvar.

### 3.1.2 Google workspace, avsaknad av konsekvensbedömning ledde till sanktionsavgift

Ett beslut som vi länge väntat på är Integritetsskyddsmyndighetens beslut om tillsyn av Google workspace i Östersunds kommun, vilket nu har meddelats. Integritetsskyddsmyndigheten tilldelar Östersunds kommun en sanktionsavgift på 300 000 kr för att kommunen inte gjort en konsekvensbedömning innan kommunen tog Google workspace i anspråk.[12]

Integritetsskyddsmyndigheten tog olyckligtvis inte i frågan huruvida amerikanska molntjänster som sådana är lämpliga i skolundervisningen och hur hanteringen förhåller sig till *Ramverket*[13], inbegripet om hantering ryms inom sitt ändamål eller är tillräckligt konfidentiell mot bakgrund av att amerikansk underrättelseinhämtning fortfarande sker.

### 3.1.3 Allvarlig kritik mot kommun som infört kontinuerligkontroll huruvida anställda dömts för brott

Justitieombudsmannen (JO) har kritiserat Södertälje kommun för att ha infört löpande kontroller huruvida samtliga anställda gjort sig skyldiga till brott. Ett externt företag genomförde uppdraget. JO belyste att anställda inte haft möjlighet att påverka vilka uppgifter som det externa företag lämnade till kommunen, eller att få bemöta dessa uppgifter, samt att anställda inte

---

[11] Samtliga punkter: EU-domstolens mål C-683/21 *Nacionalinis visuomenės sveikatos centras* och C-807/21 *Deutsche Wohnen*; EU-domstolens pressmeddelande nr 184/23, den 5 december 2023, https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-12/cp230184sv.pdf (den 11 december 2023).

[12] https://www.imy.se/globalassets/dokument/beslut/2023/beslut-om-tillsyn-barn-och-utbildningsforvaltningen-ostersunds-kommun.pdf (den 5 december 2023).

[13] Adekvansbeslutet; *EU-US Data Privacy Framework,* Brussels, 10.7.2023 C(2023) 4745 final, https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf (den 5 december 2023)

heller i efterhand fått veta vilken information som rapporterats. JO efterlyste kommunens redovisning över vilka rättsliga överväganden som gjorts, och konstaterade att eventuell avsaknad av rättsliga överväganden *självklart* är *helt oacceptabelt*.

JO bedömde att kontrollerna av de anställda utgjorde ett ingrepp i den personliga integriteten på ett sätt som innebar övervakning och kartläggning av enskildas personliga förhållanden samt att kommunen dessutom försökt begränsa insynen i förfarandet. JO fann att hanteringen stred mot 2 kap. 6 § 2 st. regeringsformen och Europakonventionens rätt till respekt för privatlivet, samt i övrigt saknade lagstöd.[14] Integritetsskyddsmyndigheten, liksom lagstiftaren, har informerats om beslutet.

### 3.1.4 Arbetsgivare använde anställds e-postkonto

En arbetsgivare i Belgien hade skickat en e-post från en före detta anställds e-postkonto till företagets kunder. Den före detta anställde hävdade också att företaget läst hans e-post. Tillsynsmyndigheten ansåg att företaget måste respektera de rättigheter som före detta anställda har och informera anställda om hur deras e-postkonton kommer hanteras efter anställningen upphört och fann brister utifrån ändamål, uppgiftsminimering, den rättsliga grunden och kravet på information samt utfärdade en reprimand.[15]

### 3.1.5 Reklam som riktas efter analys av användarens beteenden – Meta/Facebook

- Europeiska dataskyddsstyrelsen (EDPB) har tagit ett brådskande beslut som instruerar tillsynsmyndigheten att införa ett förbud mot behandling av personuppgifter för beteendebaserad reklam, med avtal och berättigat intresse som rättslig grund, vilket riktas mot Meta (Facebook, Instagram, Whatsapp).[16]

  Beskedet har lett till att Meta låter användare använda tjänsterna utan kostnad, om användaren tillåter att dennes information används underhand för att rikta annonser. Tillåter användaren inte detta får användaren börja betala för tjänsten. Huruvida detta är en korrekt hantering, har inte prövats.

- I kölvattnet av detta har 83 nyhetsmedier i Spanien stämt Meta för snedvriden konkurrens på annonsmarknaden. Andra nyhetsmedier har inte haft sådan personlig information om läsaren, vilket Meta

[14] Justitieombudsmannens beslut den 19 oktober 2023 i ärende 7143-2022; https://www.jo.se/app/uploads/resolve_pdfs/1561050_7143-2022.pdf (den 5 december 2023).
[15] Gegevensbeschermingsautoriteits beslut 135/2023 den 21 september 2023 i ärende DOS-2023-03073; waarschuwing-nr.-135-2023.pdf (gegevensbeschermingsautoriteit.be) och https://techlaw.se/belgien-foretag-far-reprimand-for-missbruk-av-tidigare-anstallds-e-postkonto/ (den 5 december 2023).
[16] https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_sv (den 5 december 2023).

haft, och därför inte kunnat rikta sina annonser på motsvarande sätt. Detta menar nyhetsmedierna har lett till snedvriden konkurrens.[17]

### 3.1.6 Brister i anställdas bärbara datorer ledde till sanktionsavgift

Polska tillsynsmyndigheten har utdömt en administrativ sanktionsavgift på 3 400 EUR mot ett bolag som inte vidtagit tillräckliga organisatoriska och tekniska åtgärder för att skydda anställdas bärbara datorer. Datorerna var inte krypterade. Bolaget hade inte tagit fram en policy för användningen av de bärbara datorerna, eller genomfört regelbundna riskanalyser samt förbisett att utbilda sina anställda.

### 3.1.7 Integritetsskyddsmyndighetens nedläggningsbeslut är överklagbara

Högsta förvaltningsdomstolen har kommit fram till att den som gett in ett klagomål till Integritetsskyddsmyndigheten kan överklaga myndighetens beslut att inte utreda klagomålet.[18]

## 3.2 Rykande färska vägledningar

Dataskyddsombudet rekommenderar att kommunen tar del av och följer dessa vägledningar.

### 3.2.1 Kamerabevakning

Integritetsskyddsmyndigheten har släppt en vägledning för kamerabevakning, läs här https://www.imy.se/globalassets/dokument/rapporter/vagledning-vid-kamerabevakning-imy-2021.pdf.[19]

### 3.2.2 DIGG:s och IMY:s vägledning om dataskydd och innovation

Myndigheten för digital förvaltning (fortsättningsvis DIGG) och Integritetsskyddsmyndigheten har tagit fram en vägledning om integritet och innovation riktat till offentliga aktörer.

Dataskyddsförordningen måste löpande beaktas i innovationsprojektet, och det krävs tvärfunktionellt samarbete mellan jurister, tekniker och chefer i innovationsprojektet, läs här: https://digg.se/kunskap-och-stod/metodstod-for-dataskydd-vid-innovation (klicka vidare för ytterligare tips och information).

En bra checklista för innovationsprojekten finns här: https://digg.se/kunskap-och-stod/metodstod-for-dataskydd-vid-innovation/checklista.

[17] https://www.reuters.com/business/media-telecom/spanish-media-association-files-598-mln-lawsuit-against-facebook-owner-meta-2023-12-04/ (den 5 december 2023).
[18] Högsta förvaltningsdomstolens dom i mål nr 6193-22 och 3691-22.
[19] Vägledning vid kamerabevakning, IMY rapport 2021:2.

### 3.2.3 Artificiell intelligens inom vård- och omsorgssektorn

Danska tillsynsmyndigheten, som många gånger är vägledande, har uttalat sig om den rättsliga grunden för utveckling och drift av AI-lösning inom vård- och omsorgssektorn, läs här https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/nov/udtalelse-om-behandlingsgrundlag-til-udvikling-og-drift-af-ai-loesning-inden-for-sundheds-og-omsorgsomraadet (välj översätt till svenska/engelska).[20]

- I korthet framgår att offentliga myndigheter har rätt att utforma, utveckla och testa AI-lösningar *så länge personuppgifter inte behandlas i AI-lösningen*, eftersom det inte finns någon giltig rättslig grund.
- Vidare understryks en risk att användare lägger större vikt vid AI-lösningens bedömning, än sin egen, vilket utgör en egen risk för medborgaren.

Anne Hännestrand
Dataskyddsombud

[20] Udtalelse om behandlingsgrundlag til udvikling og drift af AI-loesning inden for sundheds og omsorgsomraadet, ärende 2023-212-0015, den 17 november 2023. Pressmeddelande: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/nov/kommunes-hjemmel-til-ai-loesning-til-identifikation-af-borgere-med-behov-for-vedligeholdende-traening-og-rehabiliterende-indsats, och ytterligare information här https://techlaw.se/danmark-datatilsynet-uttalar-sig-om-den-rattsliga-grunden-for-utveckling-och-drift-av-en-ai-losning-inom-vard-och-omsorgssektorn/