DANDERYDS KOMMUN

VAXHOLMS STAD

Värmdö kommun

Dataskyddsombudets rapport från första halvåret 2024

Diarienummer	Senast uppdaterad	Beslutsinstans	Processägare
20240516:098	2024-06-26	Dataskyddsombud	Dataskyddsombud

Dokumentets syfte

Dataskyddsombudets halvårsrapport tas fram av dataskyddsombudet och återkopplar dataskyddsombudets iakttagelser av kommunens hantering av personuppgifter under första halvåret 2024, till de personuppgiftsansvariga nämnderna.

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

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

Innehållsförteckning

Inledning

Dataskyddsombudets halvårsrapport syftar till att hålla de personuppgiftsansvariga nämnderna informerade om dataskyddsombudets iakttagelser av kommunens hantering av personuppgifter. Rapporten avser perioden 1 januari – 26 juni 2024.[2]

Rapporten är indelad i främst tre delar;

1. Dataskyddsombudet tar ordet och redogör bland annat för aktuella frågor inom personuppgiftshanteringen och 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.

1 Dataskyddsombudet tar ordet

Under denna rubrik kommer dataskyddsombudet belysa vissa särskilda spörsmål.

1.1 Åtgärder för att bygga in dataskydd i verksamheten

Dataskyddsombudet rekommenderade kommunen, i årsrapporten 2023, att *bygga in dataskydd i verksamheten* för att kommunen skulle kunna klara av att upprätthålla regelefterlevnaden av dataskyddsförordningen. Funktioner för inbyggt dataskydd i upphandling, projektledning och digital hantering bedömde dataskyddsombudet vidare vara ett viktigt utvecklingsområde.

Verksamheten har nu i flera led visat på att processer för att bygga in dataskydd pågår i kommunen, nedan lämnas några exempel.

- *Miljö- och stadsbyggnadsnämnden* hade år 2023 och *miljö- och hälsoskyddsnämnden* hade år 2022 inga rapporterade personuppgiftsincidenter. B*yggnadsnämnden* hade år 2022 endast en rapporterad incident. Dataskyddsombudet bedömde att det fanns risk för stort mörkertal och rekommenderade kunskapshöjande insatser för att personuppgiftsincidenter skulle identifieras och rapporteras, vilket verksamheten arbetat aktivt med.

  År 2024 har arbetet visat på resultat på så sätt att incidenter som sker nu rapporteras i högre utsträckning, vilket ökar regelefterlevnaden, se avsnitt 2.3.2. Incidenterna har klarlagt att det finns brister i förvaltningens verksamhetssystem. Verksamheten bedriver nu ett

[2] De resterande dagarna i juni 2024 kommer det att redogöras för i årsrapporten.

aktivt arbete, genom *att* göra en översyn av systemet, *att* föra tät dialog med leverantören, *att* utföra en risk- och konsekvensanalys och *att* kravställa att brister annulleras i den nya modulen av systemet.

- *Valnämnden*, har i anslutningen till valet, gjort en översyn av sina personuppgiftsbehandlingar och rutiner samt antagit och gjort en risk- och konsekvensanalys för ett nytt och säkrare systemverktyg för schemaläggning och kommunikation för valarbetarna.
- *Överförmyndarnämnden*, som handlägger ytterst prekära personuppgifter, har antagit en nytt säkrare system för ärendehandläggning.
- *Utbildningsnämnden* och *socialnämnden*: En leverantör har tidigare haft väldigt många personuppgiftsincidenter. Nu efter att verksamheten vidtagit diverse stödåtgärder har arbetet med leverantören kunnat övergå till att vara en del av den normala avtalsuppföljningen.
- Några exempel på *kommunövergripande* åtgärder, inbegripet *kommunstyrelsens*, enligt följande.
    - En mall för gemensamt personuppgiftsansvar har tagits fram.
    - Informationen som gäller hur personuppgifter hanteras i samband med användningen av kommunens e-tjänster har nu uppdaterats. *Öppenhet* och *transparens* är en *GDPR-rättighet*, varför åtgärden varit viktig.[3]
    - Utbildning i dataskydd och informationssäkerhet har hållits för upphandlingsenheten, som varit ett av dataskyddsombudets utpekade fokusområden.
    - Vid samverkan med regionen, kommuner och andra samverkansorgan finns idag inte tillräckliga rutiner för att säkra upp och reglera personuppgiftshanteringen. Avtal mellan samverkansorganen ingås på övergripande nivå, utan att till exempel risk- och konsekvensbedömning för personuppgiftshanteringen har gjorts eller förhandssamråd med Integritetsskyddsmyndigheten har begärts.

      Kommunens dataskyddssamordnare har gjort ett omfattande arbete för att komma till rätta med detta, och arbetet har lett till att milstolpar – som till exempel antagna datadelningsavtal för den nystartade familjerätten (*socialnämnden*) och energi- och klimatrådgivningen (*kommunstyrelsen*) – har nåtts.

[3] Jfr. art 5 dataskyddsförordningen.

- *Mina sidor*, som ska tillhandahålla möjlighet till krypterad digital kommunikation med säker autentisering mellan kommun och medborgare, håller på att tas fram.

  Dataskyddsombudet har vid upprepade tillfällen identifierat personuppgiftsincidenter när kommunen kommunicerat med medborgare, klienter/brukare eller vårdnadshavare via e-post. Om *Mina sidor* kan säkra upp kommunens kommunikation med medborgare, innebär det stora framsteg för GDPR-efterlevnaden och personuppgifterna.

- Kommunen håller på att ta fram tjänstekort med medarbetares foto för dörrpassage. Dataskyddsombudet initierade granskning av projektet med fråga om beredande GDPR-arbete hade gjorts. Detta hade skett, vilket visar på att *det inbyggda dataskyddet* har fungerat.

- Verksamhetens utförda risk- och konsekvensbedömningar fortsätter att stiga och uppgår nu till totalt 41 stycken, varav 13 stycken gjorts det första halvåret 2024.

1.1.1 Dataskyddsombudets reflektioner

Dataskyddsombudet ser väldigt positivt på den utvecklig som skett och rekommenderar att den upprätthålls. En framgångsfaktor har varit att dataskyddssamordnare arbetat i nära dialog med förvaltningens kontaktombud (dataskyddssamordnare på förvaltningen) och tjänstepersoner.

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 prioriterar att skyndsamt lösa frågan.

1.2 Samarbete mellan Danderyds kommun, Värmdö kommun och Vaxholms stad

Dataskyddsombudet har sedan den 1 oktober 2023, även axlat rollen som dataskyddsombud för Värmdö kommun och Vaxholms stad, vilket ska följas upp tidig höst 2024.

Danderyds kommun har varit drivande i att skapa kanaler och nätverk för samverkan mellan kommunernas samtliga dataskyddssamordnare och kontaktombud. Arbetssättet har inneburit en kunskapshöjning för samtliga kommuner, och dessutom möjliggjort samarbete i GDPR-frågor på en helt ny nivå. Några exempel enligt följande.

- Avsikten är tre gemensamma GDPR-workshops, en i respektive kommun, ska hållas årligen, för samtliga dataskyddssamordnare och kontaktombud. Workshop har hållits i Danderyds kommun den 20 februari 2024 och i Värmdö kommun den 21 maj 2024, och planeras att hållas i Vaxholms stad i september 2024. GDPR, delaktighet och inspiration har utgjort ledord för dessa tillfällen.
    - Mot bakgrund av gruppens storlek har gästföreläsare från Storsthlm, Sveriges Kommuner och Regioner och andra kommuner kunnat närvara. Kommunens former för samverkan med regionen, Sveriges Kommuner och Regioner och StorSTHLM har också stärkts.
- Det pågår ett gemensamt arbete kring att upphandla en GDPR-plattform.

Flera *fördelar* har identifierats i och med att kanalerna för dialog, kontakt och informationsflöde utökats.

- Möjligheter att identifiera överenskommelser, samarbeten och projekt, vilka inte tillräckligt säkrats upp ur ett dataskyddsperspektiv, har stärkts. Här pågår insatser för att bygga in dataskydd som en naturlig del av dessa åtaganden, se avsnitt 1.1.
- Möjligheter att identifiera brister och personuppgifts-incidenter har ökat.

Det finns även *nackdelar* enligt följande.

- Danderyds kommun har starkare resurssättning än de andra kommunerna, då dataskyddssamordnaren arbetar heltid med GDPR-frågor. Den osäkerhet som finns i en verksamhet, kan smitta av sig på en annan. Det finns också en risk att kunskapsutbytet inte blir ömsesidigt.
- Dataskyddsombudets tid blir mer splittrad, där arbetet i de andra kommunerna ibland behöver prioriteras. Detta har visat viss negativ effekt på antalet av dataskyddsombudet utförda granskningar, se avsnitt 1.3.

1.3 Dataskyddsombudets granskningar

Dataskyddsombudet övervakar efterlevnaden av dataskyddslagstiftningen och kommunens strategi för skydd av personuppgifter genom *granskning*.[4]

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

[4] Jfr. art 39.1b dataskyddsförordningen.

Dataskyddsombudet har utfört 12 granskningar av regelefterlevnaden första halvåret 2024 enligt följande.

	Svarsalternativ	Antal ärenden	Antal ärenden (procent)
1	Kommunstyrelsen	6	50.0
2	Utbildningsnämnden	4	33.3
3	Socialnämnden	2	16.7
	Summa	12	100%

Notera att granskningar som gällt flera nämnder, endast tas upp i statistiken som *en* granskning och under *en* nämnd, vanligen under kommunstyrelsen i sin samordnande funktion. Nämnder som inte nämns har haft 0 granskningar eller endast kommunövergripande granskningar.

1.3.1 Dataskyddsombudets reflektioner

Antalet granskningar utförda av dataskyddsombudet har minskat efter att samverkan med delat dataskyddsombud inleddes den 1 oktober 2023, jämförelsetal enligt följande.

- 20 granskningar första halvåret 2022
- 24 granskningar andra halvåret 2022
- 29 granskningar första halvåret 2023
- 11 granskningar andra halvåret 2023 (här avslutade dataskyddsombudet också en större granskning gällande *utbildningsnämnden*)
- 12 granskningar första halvåret 2024

Sannolikt beror det minskade antalet granskningar på – att dataskyddsombudets arbete i de andra kommunerna – tar tid från utrymmet att identifiera och utreda eventuella brister i Danderyds kommuns personuppgiftshantering.

I denna del måste beaktas det viktiga arbete verksamheten med stöd av dataskyddsamordnare gör – för att i ett parallellt och proaktivt spår – säkra upp regelefterlevnaden och *bygga in dataskydd* i verksamheten, se avsnitt 1.1.1. Detta förstärker ytterligare dataskyddsombudets rekommendation i avsnitt 1.1.1; om att kommunen skyndsamt måste se till att kontaktombud kommer på plats.

1.3.2 Några exempel på dataskyddsombudets granskningar

Nämnderna behöver lära av varandra, varför exemplen är relevanta för samtliga nämnder. Avsikten är att exemplen ska vara lärande och inte läxande.

- *Utbildningsnämnden*: Dataskyddsombudet färdigställde en stor granskning av skolplattformar hösten 2023 som konkretiserade en rad brister och rekommendationer.

Dataskyddsombudet följde upp runt vintern 2023/24 hur rapporten hade hanterats. I det skedet fanns inte avsikt att ta upp rapporten i *utbildningsnämnden*, trots att kritiken i rapporten var omfattande och nämnden *personuppgiftsansvarig* för den bristfälliga hanteringen. Ingen tidsplan eller process hade tagits fram. Rapporten togs sedermera upp i utbildningsnämnden i mars 2024.

Dataskyddsombudet följde i juni 2024 ånyo upp hanteringen. Förvaltningen har nu planerat att resurssätta en halv tjänst för att arbeta med GDPR-frågor. En handlingsplan har tagits fram som innehåller bland annat översyn av gallring, sekretess, kommunikationskanaler och behandlingsregistret. Vidare har utbildningsinsatser för personal och elever, dokumentklassning vid upphandlingar och avidentifiering av personuppgifter i Google grovt planerats. Dataskyddssamordnaren har våren 2024 hållit riktade utbildningsinsatser i ca 75 procent av skolorna och förskolorna (för ledningsgrupp, stab) och kommer vidare under hösten 2024 stötta förskolorna i att göra en grundlig översyn av deras personuppgiftsbehandlingar, rutiner och avtal.

Dataskyddsombudet ser positivt på de planerade åtgärderna och uppfattar de som korrekta och nödvändiga, samt ser fram emot att följa utvecklingen.

- *Kommunstyrelsen*: I samband med ett antagonistiskt angrepp hos en leverantör stängde kommunen en VPN-tunnel till leverantören som försiktighetsåtgärd. I samband med att en kritisk fil behövde skickas, öppnades sedan tunneln för utskicket och stängdes igen. Dataskyddsombudet rekommenderade att det ska finnas en process och delegation/beslutsmandat för beslut som innebär risker för personers fri- och rättigheter.
- *Utbildningsnämnden*: I samband med upphandling av en ny skolplattform, hade verksamheten tagit fram en risk- och konsekvensbedömning (utifrån att potentiella leverantörer hade underbiträdet AWS/Amazon) som dataskyddsombudet lämnade rekommendation på. Verksamheten har sedan anfört att leverantören inte kommer använda AWS.
- *Socialnämnden*: Socialnämnden lyfte fråga om de kunde använda en *artificiell intelligens* (AI) för direktöversättning mellan olika språk i sin verksamhet. Dataskyddsombudet betonade att risk- och konsekvensbedömning ska göras i så fall, och att säkerheten (konfidentialiteten och integriteten) måste redas ut.
- *Kommunstyrelsen*: Utifrån att verksamheten har testat en AI-assistent för externa webben, skrapades webbplatsen av leverantören (*diskswap*), utan att personuppgiftsbiträdesavtal fanns på plats. Granskningen pågår.

- *Kommunstyrelsen*: Dataskyddsombudet har haft synpunkter på delegationsordningens utformning, till exempel att delegation för anmälan till Integritetsskyddsmyndigheten saknats. Verksamheten har noterat rekommendationen och översyn pågår.

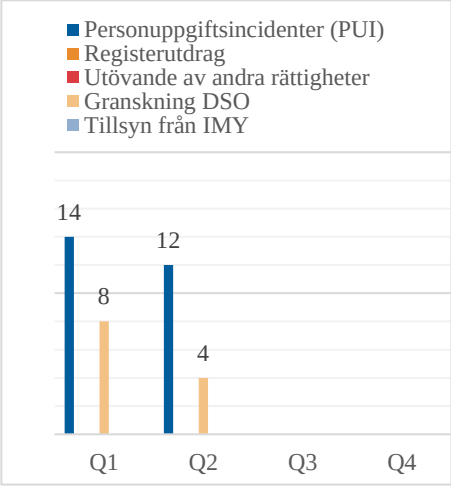
2 Statistik och dataskyddsombudets reflektioner

2.1 Statistik första halvåret 2024

Under detta avsnitt presenteras statistik för Danderyds kommun första halvåret 2024.

Kategorierna innebär följande.

- *Reklam* rör främst erbjudanden om kurser inom dataskydd etc. Ärendena diarieförs på kommunstyrelsen.
- *Underärenden* rör främst en ärendeuppbyggnaden i systemet. Vissa ärenden som skickats in till dataskydd utan ärendekoppling måste ärendekopplas och läggs sen som underärenden för att statistiken ska bli korrekt.
- *Granskning DSO* rör ärenden där dataskyddsombudet granskar nämndernas efterlevnad av dataskyddslagstiftningen. *PUI* rör personuppgiftsincidenter som anmälts eller kommit till dataskyddsombudet kännedom.
- *Övrigt* rör sådana mejl som inte hör hemma under någon annan kategori. Positiv återkoppling på information om personuppgiftshanteringen på webben placeras här och politiska beslut som skickas in till dataskyddsombud för kännedom, men som inte genererar ett eget ärende.
- *Rådgivning internt* är främst dataskyddssamordnarens kategori för intern rådgivning. Intern rådgivning sker framförallt i det löpande dataskyddsarbetet, utanför detta system.
- *IMY* rör främst post eller beslut från Integritetsskyddsmyndigheten gällande anmälda personuppgiftsincidenter. Oftast diarieförs dessa handlingar i verksamhetens system för personuppgiftsincidenten, men ibland skickas de till dataskydd för kännedom.
- *Rådgivning registrerad* rör främst ärenden där allmänheten ställer frågor till dataskyddsombudet eller huvudkontaktombudet.
- *Rapporter* rör främst dataskyddsombudets kvartals- och årsrapporter.



	Objekt	Antal ärenden	Antal ärenden (procent)
1	Reklam - Dataskydd	103	61.7
2	PUI	26	15.6
3	Granskning DSO	12	7.2
4	Underärenden	12	7.2
5	Övrigt - Dataskydd	11	6.6
6	Rådgivning internt	2	1.2
7	Rapporter	1	0.6
	Summa	167	100%

2.2 Behandlingsregistret

Varje personuppgiftsansvarig nämnd ska föra ett register över de personuppgiftsbehandlingar som utförs av nämnden och verksamheten.[5]

[5] Jfr. art 30 dataskyddsförordningen.

Danderyds kommun har 666 registrerade behandlingar av personuppgifter, varav 127 rör *kommungemensamma*, 166 rör *kommunstyrelsen*, 66 rör *utbildningsnämnden*, 31 rör *kultur- och fritidsnämnden*, 28 rör *tekniska nämnden*, 181 rör *socialnämnden*, 8 rör *valnämnden*, 13 rör *överförmyndarnämnden* och 46 rör *miljö- och stadsbyggnadsnämnden*.

Verksamheten bedriver ett aktivt arbete med att se över behandlingsregistret och att hålla det uppdaterat.

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

Danderyds kommun har under första halvåret 2024 haft 26 personuppgiftsincidenter som kommit till dataskyddsombudets kännedom, enligt följande.

	Svarsalternativ	Antal ärenden	Antal ärenden (procent)
1	Miljö- och stadsbyggnadsnämnden	8	30.8
2	Socialnämnden	7	26.9
3	Kommunstyrelsen	6	23.1
4	Utbildningsnämnden	4	15.4
5	Tekniska nämnden	1	3.8
	Summa	26	100%

De flesta incidenter är av mindre allvarligt slag. Ytterligare ärenden som registrerats vid en tidigare tidpunkt kan ha avslutats under året. Notera att en personuppgiftsincident som rör flera nämnder, endast statistiskt redovisas som *en* incident för *en* nämnd. Nämnder som inte nämns har haft 0 personuppgiftsincidenter.

Detta kan jämföras med tidigare år enligt följande.

- Danderyds kommun hade totalt 57 rapporterade personuppgifts-incidenter under år 2023;
    - varav 27 personuppgiftsincidenter första halvåret, och,
    - 30 personuppgiftsincidenter andra halvåret.
- Danderyds kommun hade totalt 54 rapporterade personuppgiftsincidenter under år 2022.
- Danderyds kommun hade totalt 38 rapporterade personuppgiftsincidenter under år 2021.

Sammanfattningsvis ligger första halvårets 26 rapporterade personuppgifts-incidenter år 2024, *i relativ nära linje* med rapporterade personuppgifts-incidenter för år 2023 och 2022.

2.3.1 Innebär många personuppgiftsincidenter en dålig hantering? Dataskyddsombudet reflekterar

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 att något system buggar eller ligger nere – vilket, om personuppgifter berörs, utgör personuppgiftsincidenter.

Det innebär att det ska finnas ett flöde av inrapporterade personuppgiftsincidenter, om rapporteringen fungerar som den ska. Vissa nämnder hanterar i större utsträckning *extra skyddsvärda* och *känsliga personuppgifter*, än andra nämnder, vilket kan påverka antalet incidenter och huruvida de ska anmälas till Integritetsskyddsmyndigheten.

Kommunens process är utformad så att verksamheterna i regel själva ska uppmärksamma och anmäla personuppgiftsincidenter, varför följande reflektioner kan ges.

- Om en nämnd har *många rapporterade personuppgiftsincidenter* talar det för att verksamheten har god kännedom om dataskyddslagstiftningen och identifierar samt anmäler personuppgiftsincidenter när sådana inträffar.
    - Att en nämnd har *många personuppgiftsincidenter* kan också tala för en sämre hantering av personuppgifter; men sannolikt skulle personuppgiftsincidenterna då heller inte ha identifierats eller anmälts.
- Om en nämnd har *få eller inga personuppgiftsincidenter rapporterade* talar det för att personuppgiftsincidenter inte identifieras och rapporteras i den utsträckning som dataskyddsförordningen kräver. Nämnden rekommenderas i så fall att se över hanteringen och utbilda handläggare för att identifiera incidenter.

- Att en nämnd har *få eller inga personuppgiftsincidenter* kan också tala för en säker hantering av personuppgifter; även om det är osannolikt att ingen personuppgiftsincident eller endast någon enstaka incident skulle ha inträffat under ett halvår.

2.3.2 Några exempel på personuppgiftsincidenter

Nämnderna behöver lära av varandra, varför exemplen är relevanta för samtliga nämnder. Avsikten är att exemplen ska vara lärande – inte läxande. Några incidenter kommenteras kort enligt följande.

- *Kommunstyrelsen*: En leverantör av juridiska tjänster, hade utsatts för ett antagonistiskt angrepp hos en underleverantör. Trots att leverantören krävde att användarna skulle byta lösenord och att data som sparats efter ett visst datum hade gått förlorat, inkom leverantören inte med någon personuppgiftsincidentanmälan till kommunen. Leverantörens hantering förvånade, eftersom leverantören specialiserat sig på GDPR. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Kommunstyrelsen*: En medarbetare mottog sin chefs kalender-notiser på sin arbetstelefon. Verksamheten rekommenderades att identifiera och säkra upp orsaken till felkopplingen.
- *Kommunstyrelsen*: I en upphandlingsportal som används för att avropa avtal kunde kommunens upphandlare *se* upphandlares på de andra kommunernas profiler och avropa från deras avtal. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten.
- *Miljö- och stadsbyggnadsnämnden*: Flera personuppgiftsincidenter har skett vid kommunicering i bygglovsärenden. Incidenterna har skett främst i anslutning till att en person automatiskt kopplas från gamla till nya ärenden, vilket leder till fel, till exempel då kontaktpersonen slutat eller personuppgifterna blivit fel från början. Även mänsklig faktor har haft en roll. Kommuniceringen sker ofta via mejl, vilket också inneburit risker för personuppgifts-incidenterna. Anmälningar till Integritetsskyddsmyndigheten har rekommenderats i flera fall och verksamheten arbetar aktivt med att stävja personuppgiftsincidenterna. Se avsnitt 1.1.
- *Kommunstyrelsen*: I en rekryteringsprocess skickades inbjudan till säkerhetssamtal till fel person, vilket uppdagades innan något samtal hann hållas. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten. Kommunstyrelsen tog beslutet att inte anmäla ärendet.
- *Socialnämnden*: I ett system för medicin kunde medarbetare se varandras personnummer. Dataskyddsombudet rekommenderade översyn samt anmälan till Integritetsskyddsmyndigheten.

- *Utbildningsnämnden*: I samband med att kommunens arkivmyndighet genomförde tillsyn i kommunens skolor uppdagades att personalen använde appen *Whats App* för kommunikation gällande personals sjukfrånvaro, elever och utrymning/inrymning av elever. Detta var bekymmersamt ur flera perspektiv.

  Whats App ingår *inte* i kommunens digitala infrastruktur och utgör inte ett godkänt arbetsverktyg. K*änsliga* och *extra skyddsvärda personuppgifter* eller *sekretessbelagda uppgifter* ska inte *röjas* till Meta och tredje land. Kommunen har inget avtal eller personuppgiftsbiträdesavtal med *Whats App* och kan inte kontrollera hanteringen av personuppgifterna. Rutiner för gallring och uppgiftsminimering samt risk- och konsekvensbedömning saknas. Eventuella foton som skickats lagras på medarbetarnas privata mobiltelefoner och riskerar att hamna i deras privata molntjänster när mobilen kopplas till datorn.

  En anmälan till Integritetsskyddsmyndigheten och flera åtgärder rekommenderades som till exempel att befintliga *Whats App*-grupper skulle annulleras, en plan för intern kommunikation skulle tas fram, och utbildningskampanj för ledningsgrupper eller medarbetare skulle prioriteras. Se avsnitt 1.3.2 för åtgärder som vidtas.

- *Socialnämnden: En* utredning skickades till brukarens granne på grund av skrivfel i adressen. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten.

- *Utbildningsnämnden*: Vårdnadshavare larmade en skola om ett konto på appen Tiktok publicerat foton och filmer på foton av elever. Kontot hade publicerat 2 foton (ett från en tidigare årskurs, och ett från en senare årskurs) på 41 elever med, med text som *bäst före eller efter*. Vidare hade filmer publicerats på foton av elever, vilka fått mellan 400 – 1 200 visningar. Elevernas för- och efternamn och ålder framkom. Kommentarer hade lämnats och vidaredelningar gjorts. Publiceringarna var inte varit önskvärda. Två lärare omnämndes också tillsammans med delvis illasinnat innehåll.

  Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten, samt att ett *förhållningssätt* behövde tas fram. Verksamheten behövde vidare se över regelefterlevnaden för skolkatalogen utifrån GDPR.

- *Tekniska nämnden*: Beslut expedierades felaktigt till annan parts advokat. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten.

- *Socialnämnden*: Danderyds kommun mottog en faktura som rörde en annan kommunens resenär och bestred fakturan (utan att identifiera och rapportera en personuppgiftsincident). Leverantören

identifierade att beställaren i den andra kommunen hade behörighet till Danderyds kommuns 32 resenärer i en viss sjukdomskategori.

Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten, översyn av dels verksamhetens egen hantering, dels om det fanns godtagbara skäl till att leverantören kunnat peka ut specifik sjukdomskategori för resenärerna.

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 kommunen för överträdelse av dataskyddsförordningen under perioden.

2.5 Registerutdrag

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

Det har inte kommit till dataskyddsombudets kännedom att någon begärt ett registerutdrag från kommunen under perioden.

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 under perioden.

2.7 IMY:s tillsyn och sanktionsavgifter

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.

3 DEL 3 – Rättsutveckling, praxis och vägledning

Under detta avsnitt kommer dataskyddsombudet redogöra för domar, utredningar och beslut (praxis) som är vägledande, informativa och kunskapshöjande. Även om praxisen rör andra organisationer, är praxisen

relevant för samtliga personuppgiftsansvariga nämnder. Avsikten är att exemplen ska vara lärande – inte läxande.

3.1 IMY: tillsynen år 2024 kommer fokuseras på kommuner, arbetsgivare och kamerabevakning

Integritetskyddsmyndigheten har tagit fram kriterier som motiverar tillsyn nämligen; risk för eller allvarlig kränkning av privatliv, omfattande behandling, ny teknik, väsentligt behov av praxis och allvarligt åsidosättande vid kreditupplysning. Är två av kriterierna uppfyllda är det motiverat för Integritetsskyddsmyndigheten att inleda tillsyn på eget initiativ eller utvidga en klagomålstillsyn.

Under år 2024 kommer Integritetsskyddsmyndigheten att fokusera på tillsyn inom kommuners arbete med dataskyddsförordningen, behandling av personuppgifter inom arbetslivet och granskning av nya tekniska lösningar inom kamerabevakning.[6]

3.2 Riksrevisionen: statens insatser för vård- och omsorgsgivares informationssäkerhetsarbete är inte effektiva, med följd att skyddet för personuppgifterna är olika i olika kommuner

Riksrevisionen har funnit att statens insatser för att stärka vård- och omsorgsgivares informationssäkerhetsarbete *inte är effektiva*. Regeringen och myndigheterna Integritetsskyddsmyndigheten, Myndigheten för samhällsskydd och beredskap (MSB) samt Socialstyrelsen vidtagna åtgärder har varit otillräckliga. Trots att *omsorg* hanterar ungefär lika känsliga personuppgifter som *vården*, saknas ett systematiskt informations-säkerhetsarbete.[7]

- Framförallt mindre kommuner (med begränsade resurser och svårigheter att rekrytera kompetent personal) drabbas. Detta får till konsekvens att skyddet för personuppgifterna varierar i olika delar av landet.[8]

[6] Integritetsskyddsmyndighetens tillsynsplan 2024, Integritetsskyddsmyndighetens beslut i ärende IMY-2024-2859 den 11 mars 2024; https://www.imy.se/globalassets/dokument/beslut/2024/tillsynsplan-2024/.
[7] Riksrevisionens rapport *Informationssäkerhet i vård och omsorg – statens stöd och tillsyn*, beslutad den 26 mars 2024, dnr: 2022/1031, RiR 2024:6; https://www.riksrevisionen.se/download/18.1226ebab18ebceb0297699b5/1713171677430/RiR_2024_6_rapport.pdf.
[8] Riksrevisionens rapport *Informationssäkerhet i vård och omsorg – statens stöd och tillsyn*, beslutad den 26 mars 2024, dnr: 2022/1031, RiR 2024:6; https://www.riksrevisionen.se/download/18.1226ebab18ebceb0297699b5/1713171677430/RiR_2024_6_rapport.pdf.

3.3 USA:s kongress: användning av Copilot förbjuden

Det amerikanska representanthuset har beslutat att förbjuda användningen av *Copilot* eftersom *Copilot* kan läcka data till molntjänster. Användningen av *ChatGPT* är sedan tidigare begränsad.[9]

3.4 Regeringen: Mediemyndigheten får i uppdrag att stärka kunskapen mot AI-driven desinformation

Regeringen har gett Mediemyndigheten i uppdrag att höja den allmänna förståelsen för hur AI och ny teknik påverkar informationslandskapet. Avsikten är att öka medborgarnas förmåga att förstå och källkritiskt kunna värdera budskap, samtidigt som tilliten till trovärdiga avsändare upprätthålls. Satsningen ska öka samhällets motståndskraft mot desinformation och otillbörlig informationspåverkan.[10]

3.5 Danska Datatilsynet: riktar allvarlig kritik för bristande flytt av data (*diskswap)*

Köpenhamns kommun hade flyttat data, så kallad *diskswap*. Detta ledde till att cirka 37 500 anställda i kommunen fick obehörig åtkomst till uppgifter rörande 3,7 miljoner personer under två månaders tid. Endast fyra personer borde haft tillgång till uppgifterna. Personuppgifterna rörde främst namn- och adressuppgifter, men också information om välbefinnande, språkbedömning och barns tand- och sjukvård. Kommunen hade brustit i sin kontroll att säkra upp efter *diskswapen*.[11] Datatilsynet riktar allvarlig kritik.

3.6 Region Stockholm: använd inte Copilot

Region Stockholm har upptäckt att Copilot i Microsoft Edge (som finns i sidopanelen i webbläsaren) kan röja patientdata när den läser av och sammanfattar webbsidor. Om så sker, kan patientdata komma att överföras till Microsoft, vilket är i strid med dataskyddsförordningen och offentlighets- och sekretesslagstiftningen (2009:400). Funktionen bör därför inaktiveras, även hos privata vårdgivare och kommuner.[12]

3.7 EU-parlamentet: godkänner rättsakten om AI (AI-act)

Europaparlamentet har godkänt rättsakten om artificiell intelligens som kräver att grundläggande rättigheter, demokrati, rättsprinciper och hållbarhet

---

[9] https://techlaw.se/varlden-usas-kongress-forbjuder-microsoft-copilot-pa-grund-av-cybersakerhetsrisker/.
[10] https://www.regeringen.se/pressmeddelanden/2024/03/mediemyndigheten-ges-i-uppdrag-att-genomfora-nationell-satsning-for-starkt-medie--och-informationskunnighet-inom-ai-driven-desinformation/.
[11] Datatilsynets beslut i ärende 2024-442-4149 den 30 maj 2024; https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/maj/koebenhavns-kommune-faar-alvorlig-kritik-for-manglende-sikkerhedsforanstaltninger.
[12] https://vardgivarguiden.se/nyheter/2024/april/anvand-inte-copilot-i-microsoft-edge--kan-strida-mot-gdpr/.

ska respekteras vid utvecklingen av AI med hög risk. Rättsakten måste formellt antas av rådet.[13]

3.8 Danska Datatilsynet: Mer transparens krävs för programvara för fusk under tentamen (skola)

Danska Datatilsynet har granskats skolors användning av programvara för att övervaka elevernas tentamen i syfte att förhindra fusk, och bevakningen skedde på elevens egen dator. Datatilsynet fann att informationen till eleverna behövde vara mer relevant. En risk- och konsekvensbedömning hade inte gjorts. Eleverna behövde göras medvetna om hur de kunde undvika att exponera privat information för programvaran.[14]

3.9 NOYB: Microsoft 365 Education tar inte ansvar och profilerar barn och unga

None of Your Business (NOYB) har lämnat in klagomål i Österrike mot Microsoft 365 Education och krävt att Microsoft ska bötfällas. Microsoft har hänvisat elever som velat utöva sina GDPR-rättigheter hos Microsoft till sina respektive skolor. NOYB har anfört att Microsoft inte tagit sitt ansvar, eftersom skolorna rent faktiskt inte har någon möjlighet att förhandla eller ändra Microsofts villkor.

- NOYB har vidare anfört att Microsoft samlar in och analyserar elevers användarbeteenden och webbläsardata (profilering) utan att skolan, eleverna eller vårdnadshavarna känner till det; och utan att vara transparanta om insamlingen.[15]

3.10 HFD: GDPR innebär ett förbud mot att offentliggöra uppgifter om hälsa mm[16] (bakgrundskontroller, utgivningsbevis)

Integritetsskyddsmyndigheten meddelade ett bakgrundskontrolls-bolag en *reprimand* för att ha samlat och tillgängliggjort information om 210 000 domstolsavgöranden om personers tvångsvård på grund av psykisk ohälsa eller missbruk. Reprimanden meddelades trots att bolaget haft utgivningsbevis och bedömdes tillräcklig eftersom utgivningsbevisets räckvidd dessförinnan inte hade prövats.

Både förvaltningsrätten och kammarrätten avslog bakgrundskontrolls-bolagets överklaganden. Nu har Högsta förvaltningsdomstolen prövat och funnit att *dataskyddsförordningen utgör en lag som innebär ett förbud mot att offentliggöra uppgifter om etniskt ursprung, hudfärg, politiska åsikter, religiös/filosofisk övertygelse, fackförbundsmedlemskap, hälsa, sexualliv/sexuell läggning eller genetiska/biometriska uppgifter.*[17] I övrigt

[13] https://techlaw.se/eu-europaparlamentet-godkanner-rattsakten-om-artificiell-intelligens-ai-act/
[14] https://techlaw.se/danmark-roskilde-katedralskole-far-kritik-for-anvandning-av-programvara-for-provovervakning/.
[15] https://noyb.eu/en/microsoft-violates-childrens-privacy-blames-your-local-school.
[16] Jfr. 1 kap. 20 § yttrandefrihetsgrundlagen.
[17] Jfr. 1 kap. 20 § yttrandefrihetsgrundlagen.

meddelade Högsta förvaltningsdomstolen inte prövningstillstånd. Sammantaget måste bakgrundskontrollsbolaget nu alltså rätta sig efter Integritetsskyddsmyndighetens föreläggande.[18]

- Integritetsskyddsmyndigheten har den 14 maj 2024 i ett rättsligt ställningstagande bedömt att de är behöriga att göra tillsyn mot söktjänster med utgivningsbevis.[19] Riktigheten i ställningstagandet bekräftas indirekt genom högsta förvaltningsdomstolens dom.

3.11 Bloomberg: ChatGPT rankar personer olika utifrån etniskt ursprung och kön

Bloomberg har i en studie identifierat att *ChatGPT* rangordnat likvärdiga CV olika utifrån kandidatens kön och etniskt ursprung. Slumpmässiga CV och namn kopplades samman för studien. Vidare valde *ChatGPT* konsekvent CV med kvinnligt namn för tjänster som har en högre andel kvinnor och mörkhyade kvinnor valdes mer sällan för tekniska jobb.[20]

3.12 Internationellt: Artificiella karaktärer blåste medarbetare på 25 miljoner dollar (deepfakes)

En medarbetare på ett multinationellt bolag i Hongkong lurades att betala ut 25 miljoner dollar till en bedragare, som skapat artificiella karaktärer (så kallade *deepfakes*) av medarbetarens chef och kollegor i en videokonferens. Karaktärerna hade skapats från inspelade videokonferenser. Händelsen har inneburit, att tidigare bedömningen, att *deepfakes* inte skulle kunna utgöra ett allvarligt hot, har omvärderats.[21]

3.13 MSB: Nätfiskekampanj mot kommuner och skolor pågår

MSB varnar för e-post som ser ut att komma från kollegor, som innehåller otillbörliga SharePoint- och OneDrive-filer. Mejlen är välformulerade och har relevant innehåll för arbetsuppgifterna, men utgör nätfiske i syfte att utföra bedrägerier, bedriva utpressning och så vidare. MSB rekommenderar att motringa när en kollega delat en fil samt att varna andra om man drabbas. Generella råd finns här: https://www.cert.se/tema/natfiske. [22]

---

[18] Högsta förvaltningsdomstolens dom den 20 juni 2024 i mål 4588-23, https://www.domstol.se/globalassets/filer/domstol/hogstaforvaltningsdomstolen/2024/domar-och-beslut/4588-23.pdf och Integritetsskyddsmyndighetens beslut i ärende IMY-2022-1621 den 13 september 2022, https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-verifiera.pdf.

[19] Rättsligt ställningstagande IMYRS 2024:1 – Klagomål mot söktjänster med utgivningsbevis; den 14 maj 2024; https://www.imy.se/globalassets/dokument/rattsligt-stallningstagande/imyrs-2024_1-klagomal-mot-soktjanster-med-utgivningsbevis.pdf.

[20] https://techlaw.se/varlden-chatgpt-diskriminerar-jobbsokande-utifran-ras-och-etniskt-ursprung/.

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

[22] https://www.cert.se/2024/06/pagaende-natfiskekampanj-riktad-mot-kommuner-och-skolor.html.

3.14 JO: Region Uppsala får allvarlig kritik för att ha lämnat ut en patients journaluppgifter, i en annan patients ärende

Vid en domstolsprövning med anknytning till patient A:s tvångsvård tillfördes felaktigt information om patient B vad gällde psykosocial historik, familj/uppväxt, utbildning, anställningar, relationer, medicinska problem, psykiska problem, alkohol/droger, personnummer och brottslighet, in i patient A:s dokumentation. Justitieombudsmannen (JO) lämnade allvarlig kritik och fann det anmärkningsvärt att sammanblandningen skett och inte upptäckts under fem års tid. Det var oacceptabelt att de integritetskänsliga uppgifterna om B behandlats på så sätt. [23]

3.15 IMY: Avanza får 15 miljoner kronor i sanktionsavgift för att ha delat personuppgifter med Facebook/Meta

Avanza hade aktiverat ett analysverktyg för marknadsföring på sin webbplats, *Meta/Facebook-pixeln*. Pixeln förde över mellan 500 000 - 1 miljon kunders personuppgifter om värdepappersinnehav och värde, lånebelopp, kontonummer och personnummer till Meta/Facebook.

Integritetsskyddsmyndigheten fann att Avanza *inte vidtagit lämpliga tekniska och organisatoriska åtgärder* för att säkerställa en lämplig säkerhetsnivå på webbplatsen och meddelade en sanktionsavgift på 15 miljoner. Enligt Avanza ska Meta/Facebook ha raderat uppgifterna och Avanza implementerat nya rutiner. [24]

Anne Hännestrand
Dataskyddsombud

[23] Justitieombudsmannens beslut i ärende 4763-2023 den 5 juni 2024; https://www.jo.se/app/uploads/resolve_pdfs/1638631_4763-2023.pdf.
[24] Integritetsskyddsmyndighetens beslut i ärende DI-2021-5544 den 24 juni 2024; https://www.imy.se/globalassets/dokument/beslut/2024/beslut-tillsyn-avanza.pdf.