Dataskyddsombudets rapport

Kvartal 1 2023

Diarienummer	Senast uppdaterad	Beslutsinstans	Processägare
20230227:036	2023-04-14	Dataskyddsombud	Dataskyddsombud

Dokumentets syfte

Den personuppgiftsansvariga nämnden har en skyldighet enligt dataskyddsförordningen att ansvara för, och kunna visa på, att dataskyddslagstiftningen efterlevs.[1]

Kvartalsrapporten tas fram av dataskyddsombudet och syftar till att hålla den personuppgiftsansvariga nämnden och kommunledningsgruppen informerad om dataskyddsombudets iakttagelser av kommunens hantering av personuppgifter. Detta som ett led för att nämnden ska kunna ta sitt personuppgiftsansvar och kunna redovisa sin efterlevnad av dataskyddsförordningen.

Dokumentet gäller för

Rapporten riktar sig främst till kommunens personuppgiftsansvariga nämnder och ställs till kommunledningen i sin kommunövergripande funktion. De personuppgiftsansvariga nämnderna bör underrättas om rapportens innehåll i relevanta delar.

Kvartalsrapporten riktas främst till respektive personuppgiftsansvarig nämnd, men är även aktuell för alla chefer och anställda som direkt eller indirekt arbetar med personuppgifter. Rapporterna utgör ett led av kommunens systematiska kvalitetsarbete för att säkra korrekt behandling av personuppgifter.

[1] Art 5.2 dataskyddsförordningen, (hyperlänk i hela dokumentet: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679, 2022-06-29).

DANDERYDS KOMMUN

Innehållsförteckning

1 Inledning

Dataskyddsombudets kvartalsrapport syftar till att hålla de personuppgiftsansvariga nämnderna och kommunledningsgruppen informerad om dataskyddsombudets iakttagelser av kommunens hantering av personuppgifter. I rapporten redovisas statistik och uppgifter om granskningar, personuppgiftsincidenter, begäran av registerutdrag, sanktionsavgifter, tillsyn, skadestånd samt dataskyddsombudets berättelse och fortsatta planering.

Det är den personuppgiftsansvariga nämnden som är ansvarig för sin behandling av personuppgifter och bör underrättas om rapportens innehåll i relevanta delar.

2 Dataskyddsombudets berättelse för kvartal 1 2023

2.1 Nytt huvudkontaktombud

Nytt huvudkontaktombud har rekryterats och påbörjat sin anställning den 13 mars 2023. Huvudkontaktombudet kommer arbeta heltid med dataskyddsfrågor, vilket är en rejäl förstärkning av stöd till verksamheten. Överlämning och introduktion har påbörjats och fortgår.

2.2 Rutin för mediabanken

Huvudkontaktombudet har stöttat verksamheten i att ta fram en rutin för arbetet med mediabanken. Mediabanken har tidigare granskats av dataskyddsombudet. Huvudkontaktombudet har i det senaste utkastet av rutinen lämnat kommentarer. Dataskyddsombudet och huvudkontaktombudet har efterfrågat status från verksamheten, som uppgett att rutinen ska vara klar i mars 2023. Dataskyddsombudet vill granska rutinen.

2.3 Behandlingsregistret

Varje personuppgiftsansvarig nämnd ska föra ett register över behandling som utförts under dess ansvar.[2]

Dataskyddsombudet bedömer att en process utgör *en* behandling. Det räcker alltså med *en* behandling för till exempel rekrytering. Det behövs alltså *inte* registreras en behandling för inskickande av personligt brev och CV, en behandling för intervju och en behandling för referenstagning etcetera.

Den nämnd som har flest registrerade behandlingar har 165 behandlingar i sitt register, medan den nämnd som har minst har en (1) behandling registrerad i sitt register. I och med att olika nämnder hanterar olika mängd och typ av personuppgifter kan finnas skäl för vissa skillnader, men vissa frågor väcks ändå utifrån skillnaden mellan antalet registreringar mellan nämnderna.

- Kontaktombuden har efterlyst en samsyn mellan nämnderna på behandlingar som registreras, så att registreringarna sker på likartat sätt mellan nämnderna.

[2] Art 30 dataskyddsförordningen.

- Kontaktombuden har uppgett att det finns en osäkerhet om varje nämnd ska registrera e-post, kalender och kommungemensamma system eller om det hanteras genom kommunövergripande registreringar. I denna fråga ligger även frågan om kommungemensamma processer och vem som ansvarar för dessa. Dataskyddsombudet ser att det går att göra på olika sätt, men vill i denna del understryka att senare praxis starkt betonar vikten av att varje dataflöde, och personuppgiftsansvarig för flödet, ska identifieras. Verksamheten bör därför bestämma sig.
- Dataskyddsombudet har rekommenderat verksamheten att utifrån Microsofts generella förteckning av kategorier av personuppgifter, se över kommunens behandlingsregister för Microsofts tjänster för att identifiera personuppgiftsansvarig och behandling för varje dataflöde. Även i övrigt borde en genomlysning göras. Dataskyddsombudet vidhåller rekommendationen.

Dataskyddsombudet bedömer att dessa frågor bör kunna lösas av verksamheten, med stöd av huvudkontaktombudet.

2.4 Sammanställning av anställdas kalendrar, tid och kontakter

Viva insights är en funktion i Microsofts tjänster som sammanställer information om anställdas kalendrar, tid och vilka personer de haft mest kontakt med. Tidigare har verksamheten stängt av utskick av epost med sammanställningen. Microsoft meddelade tidig höst 2022 att funktionen kunde stängas av. Dataskyddsombudet har rekommenderat att verksamheten stänger av funktionen och att annars göra en konsekvensbedömning, vidtar riskminimerande åtgärder, informera anställda om att deras kalender och kontakter sammanställs, samt att behandlingen måste registreras. Verksamheten har deaktiverat funktionen. Verksamheten menar fortfarande att själva summeringen inte kan slås av.

2.5 Dataskyddsombudets kanaler till nämnderna

Dataskyddsombudet har i årsrapporterna 2022 konstaterat att de nämnder som har många personuppgiftsincidenter också har många granskningar.

En nämnd hade, mot bakgrund av sina 153 registrerade behandlingar, 27 personuppgiftsincidenter och 20 reaktiva granskningar år 2022 som exempel. En annan nämnd hade mot bakgrund av sin enda registrerade behandling, noll personuppgiftsincidenter och noll reaktiva granskningar i jämförelse. Detta mönster, att vissa nämnder har många rapporterade personuppgiftsincidenter och granskningar, medan vissa nämnder inte har några varken rapporterade personuppgiftsincidenter och granskningar, är återkommande genom statistiken.

Olika nämnder hanterar olika mängder och typer personuppgifter vilket kan vara en del av förklaringen, men troligtvis inte hela förklaringen. Eftersom det inte finns någon *lägstanivå* för incidenter bör ett visst antal incidenter kunna förväntas ske varje år. För de nämnder som varken har några rapporterade personuppgiftsincidenter eller granskningar under året, finns en farhåga att dataskyddsombudet inte informeras i tillräcklig omfattning om nämndens personuppgiftshantering och eventuella incidenter.

Företeelsen har stämts av med kontaktombuden för att kunna identifiera alternativa arbetssätt. Sammantaget ser dataskyddsombudet över om det, utöver utbildningsinsatser för förvaltningarna och de personuppgiftsansvariga nämnderna, går att skapa ömsesidiga kanaler, eller skärpa de som redan finns, mellan dataskyddsombud eller huvudkontaktombud till samtliga nämnder och förvaltningar.

2.6 Aktuellt

Integritetsskyddsmyndigheten har den 7 februari 2023 börjat granska en kommuns användning av Google workspace (amerikansk molntjänst som används i skolverksamheten) och dess förenlighet med dataskyddsförordningen.[3] Danska tillsynsmyndigheten (Datatilsynets) har sedan tidigare inlett granskning av Google workspace i skolans verksamhet i Helsingörs kommun. Även andra länder, som till exempel Frankrike, har förbjudet Google workspace i skolundervisningen.

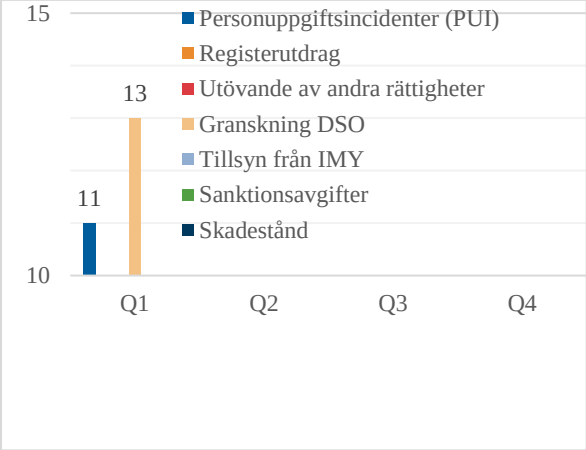
Utbildningsnämnden bör noga följa utvecklingen. Flera personuppgiftsansvariga nämnder skulle kunna berörda av utgången.

3 Redovisning av statistik

Statstiken kommer från kvartal 1 2023, presenteras på ett litet annat sätt än tidigare genom att arbetet nu effektiviseras och statistik plockas ut direkt från diariet. Nedan presenteras statistik för samtliga ärenden som registrerats i systemet för dataskydd under kvartal 1 2023.

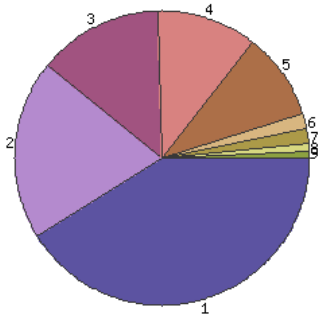
3.1 Statistik[4]

	Objekt	Antal ärenden	Antal ärenden (procent)
1	Reklam	48	41.0
2	Övrigt	23	19.7
3	Underärenden	16	13.7
4	Granskning DSO	13	11.1
5	PUI	11	9.4
6	Rådgivning internt	2	1.7
7	IMY (beslut, sanktion, förelägganden, tillsyn)	2	1.7
8	Rådgivning registrerad	1	0.9
9	Rapporter	1	0.9
	Summa	117	100%



[3] IMY-2023-1647

[4] Specificering av kategorier: *Reklam* rör främst erbjudanden om kurser inom dataskydd etc.*Övrigt* rör främst systemuppdateringar. *Underärenden* rör främst en ärendeuppbyggnaden i systemet. Vissa ärenden som skickats in till dataskydd utan ärendekoppling måste ärendekopplas och läggs sen som underärenden för att statistiken ska bli korrekt. *Granskning DSO* rör ärenden där dataskyddsombudet granskar nämndernas efterlevnad av dataskyddslagstiftningen. En granskning kan initieras genom att en fråga ställs till dataskyddsombudet, att dataskyddsombudet själv uppmärksammar något som bör granskas närmare eller i samband med personuppgiftsincidenter. *PUI* rör personuppgiftsincidenter som anmälts eller kommit till dataskyddsombudet kännedom. Ibland rekommenderar dataskyddsombudet anmälan till Integritetsskyddsmyndigheten. *Rådgivning internt* är främst huvudkontaktombudets redskap för intern rådgivning. Dataskyddsombudet uttalar sig främst via granskningar och personuppgiftsincidenter. *IMY*



3.2 Kommentar

Statistiken bygger på uppgifter som verksamheten meddelat dataskyddsombudet eller som dataskyddsombudet själv upptäckt i kontakt med verksamheten genom till exempel granskningar, personuppgifts-incidenter och konsekvensbedömningar.

3.3 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.

Under kvartal 1 2023 har 11 personuppgiftsincidenter kommit till dataskyddsombudets kännedom, varav anmälan till tillsynsmyndigheten har rekommenderats av dataskyddsombudet i 5 fall.

- I ett av dessa fem ärenden har verksamheten tagit delegationsbeslut att inte anmäla händelsen till Integritetsskyddsmyndigheten.
- Verksamheten har därutöver anmält två incidenter till Integritetsskyddsmyndigheten, utan att dataskyddsombudet rekommenderat det. I ena ärenden bedömde dataskyddsombudet att ytterligare utredning behövde ske, och i det andra ärendet gjordes anmälan på rekommendation från leverantören, utan att dataskyddsombudet hann yttra sig.

Nedan nämns några personuppgiftsincidenter enligt följande.

- En person med sekretessmarkering hade ställt en fråga och lämnat viss information till förvaltningen. Förvaltning svarade personen till en tidigare angiven e-postadress. E-postadressen gick till en annan person som fick del av informationen som den sekretessmarkerade

---

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.

lämnat. Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten, vilket ombesörjdes av verksamheten.

- En leverantör av transporter för skolskjuts och transport för brukare hade genom antagonistiskt angrepp fått sina personuppgifter obehörigen krypterade (”kidnappade”) och helt förlorade under ca en till två dygn. Därtill kom det olika uppgifter huruvida det kunde uteslutas om personuppgifterna läckt eller inte. Dataskyddsombudet konstaterade att det rörde sig om känsliga personuppgifter (hälsa, transport till särskola, korttidsboenden, korttidsvistelser och särskilda behov vid transporten) och extra skyddsvärda personuppgifter (uppgifter om barn, barn inom LSS). Två nämnder berördes.

  Kommunen bedömde initialt att leverantören var personuppgiftsansvarig för behandlingen. Leverantören bedömde att det inte fanns någon risk för personuppgifterna och att anmälan till Integritetsskyddsmyndigheten inte behövdes. Driftsmiljön skulle återuppbyggas med back up data. Sedermera framkom att leverantören själv ansåg att deras information till kommunen om incidenten varit i egenskap av biträde och att kommunen hade ansvaret att anmäla incidenten till Integritetsskyddsmyndigheten.

  Ärendet var rörigt av flera skäl enligt följande.

  - Kommunen och leverantören hade inte samsyn på vem som var personuppgiftsansvarig. Avtalet synes innefatta både moment av leverantörens självständiga personuppgiftsansvar som biträdesansvar.
  - Flera olika företag var inblandade, både koncernbolaget och tidigare okända underleverantörer till leverantören kontaktade kommunen med olika, ibland sinsemellan, motsägelsefulla uppgifter. Dataskyddsombudet kan poängtera att vid en bestämd relation mellan personuppgiftsansvarig och biträde hade kommunen fått kännedom om vilka underbiträden som leverantören använde.
  - Kommunen lade viss vikt vid att leverantören skulle kunna ta illa vid sig av kommunens hantering. Kommunens avvägning mellan å ena sidan kundrelationen, å andra sidan dataskyddslagstiftningen, upplevdes som något egendomlig eftersom leverantören (oavsett i sin egenskap som personuppgiftsansvarig eller biträde) var bunden av dataskyddsförordningen och att ett dokumenterat antagonistiskt angrepp med i vart fall tillfällig förlust av personuppgifter faktiskt skett.
  - En förvaltning ville vid ett skede inte fortsätta utreda ärendet, trots att det framkom fler och fler bekymmersamma element. Förvaltningen ändrade sig dock.

  De två berörda nämnderna anmälde slutligen incidenten till Integritetsskyddsmyndigheten. Dataskyddsombudet har därtill

rekommenderat att kommunen och leverantören måste definiera dataflödena och bestämma personuppgiftsansvaret för varje flöde, och att upphandlingsenheten ska arbeta mer i dialog med huvudkontaktombudet och kontaktombuden.

- Trygghetslarm för äldre sattes ur funktion genom antagonistiskt angrepp. Verksamheten arbetade med akuta åtgärder för att upprätthålla liv och hälsa. Efter någon dags utredning meddelade leverantören att de inte kunde varit säkra på om det inte förelåg en pågående risk för personuppgifterna (uppgifter om hälsa/uppgifter som normalt är belagda med tystnadsplikt, namn, adress) varför kommunen rekommenderades att göra en personuppgiftsanmälan till Integritetsskyddsmyndigheten. Detta ombesörjdes av verksamheten under helgen.
- Dokumentation om fyra elevers extra anpassningar i utbildningsverksamheten har varit diarieförda i en annans elev digitala journal. Uppgifter om extra anpassningar kan tangera området hälsa som är en *känslig personuppgift* och dessutom fanns en utvärderande del som utgör *extra skyddsvärda personuppgifter*. När den senare elevens journal begärdes ut av vårdnadshavaren, skickades uppgifterna om de fyra andra elevernas extra anpassningar med i kuvertet. Vårdnadshavaren kontaktade omgående skolan. Dataskyddsombudet rekommenderade att skolan begärde att återfå handlingarna för makulering och anmälan till Integritetsskyddsmyndigheten.
- Vid en utbildning för ca 65 förtroendevalda samt ytterligare personer från förvaltningen visade en förvaltning flera filmer på kommunens elever innehållande extra skyddsvärda personuppgifter (om barn och nyanlända) och känsliga personuppgifter (om etnicitet och hälsa). En av filmerna var redigerad utifrån GDPR. Tre av filmerna var inte det. För en av filmerna hade dataskyddsombudet dessutom rekommenderat personuppgiftsanmälan till Integritetsskyddsmyndigheten ett år tidigare.

  Dataskyddsombudet rekommenderade anmälan till Integritetsskyddsmyndigheten, även för denna händelse. Den rättsliga grunden var tveksam, personuppgifterna hade kunnat minimeras och både känsliga och extra skyddsvärda personuppgifter förekom i filmerna. Mot bakgrund av att förvaltningen känt till att en av filmerna ett år tidigare bedömts utgöra en personuppgiftsincident av dataskyddsombudet, så borde riskminimerande åtgärder och begränsningar satts in. Verksamheten tog delegationsbeslut att inte anmäla personuppgiftsuppgiftsincidenten.
- I ett ärende skickade en skola en epost utan kryptering till tjänstepersoner på kommunen med information om en ungefärlig boendeplats för ett barn med sekretessmarkering. Dataskyddsombudet bedömde att skolan hade att själv ta ställning till sin del i incidenten samt att tjänstepersonerna på kommunen skulle radera mejlet, tömma papperskorgen och kontakta IT för eventuell ytterligare radering. Eftersom tjänstepersonerna på

kommunen var betrodda, innebar *läsandet* av eposten inte sådan risk att läsandet behövde anmälas till Integritetsskyddsmyndigheten.

- Någon hade skickade en påhittad inbjudan till fest hos en privat adress i grannkommunen (vilka inte alls ville befattas med någon fest), till en hel årskurs (500 elever) på en skola. Epostadresserna verkade på okänt sätt ha kommits över i kommunens system. Vid samverkan med andra myndigheter spreds också samtliga elevers e-postadresser till grannkommunen. Även i det fall mottagare av mejlet skickat vidare mejlet har personuppgifterna spridits vidare. Dataskyddsombudet bedömde att en personuppgiftsincident skett i flera led och rekommenderade anmälan till Integritetsskyddsmyndigheten, samt information till de registrerade.
- Det har framkommit att en förvaltning fick ut en lista med en före detta anställds personnummer, trots att denne hade sekretessmarkering, från ett system för budget. Personnummer är en extra skyddsvärd personuppgift. Vid utredningen framkom att i vart fall anställdas födelsedata måste framgå i systemet för att systemet ska kunna räkna ut den anställdes arbetsgivaravgift. De anställda behövde vidare identifieras för att chefen ska få korrekt behörighet.

  Systemet användes endast av betrodd personal, främst chefer, som endast fick tillgång till sin egen personal i systemet (för vilkas personnummer de redan känner till genom andra system). Dataskyddsombudet, bedömde att incidenten inte behövde anmälas till Integritetsskyddsmyndigheten. Däremot rekommenderade dataskyddsombudet att det behövde utredas om hela personnumret verkligen behövde föras över i systemet, och att eventuell rutin eller instruktioner i systemet skulle tas fram. Verksamheten anmälde händelsen till Integritetsskyddsmyndigheten.

3.4 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 under kvartalet.

3.5 Registerutdrag

Den registrerade har rätt att begära ut ett registerutdrag med information om kommunen behandlar personuppgifter om denne och i så fall varför.

Under kvartalet har ingen begäran om registerutdrag inkommit till kommunen.

3.6 Andra rättigheter

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

Under kvartalet har inte någon begäran om att utöva dessa rättigheter kommit till dataskyddsombudets kännedom.

3.7 Tillsyn och sanktioner av tillsynsmyndighet

Tillsynsmyndigheten har inte genomfört eller annonserat något kommande tillsynsärende mot kommunen. Kommunen har inte ålagts att betala några administrativa sanktionsavgifter.

3.8 Påbörjade och planerade granskningar

- Dataskyddsombudet har påbörjat en granskning av systemen vilka används i utbildningsverksamheten. Dataskyddsombudet har fått en presentation av flera olika system som används och har själv tagit några stickprover. Arbetet fortsätter.
- Dataskyddsombudet planerar på sikt följa upp användningen av samtycke för de nämnder som redovisat brister i behandlingen av personuppgifter med samtycke som rättslig grund vid dataskyddsombudets granskning år 2020.

3.9 Reaktiva granskningar

Dataskyddsombudets övervakar efterlevnaden av dataskyddslagstiftningen och kommunens strategi för skydd av personuppgifter genom granskningar.[5] 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.

Dataskyddsombudet har genomfört 13 reaktiva granskningar under kvartalet bland annat enligt följande.

- En vårdnadshavare kontaktade dataskyddsombudet och påtalade att hen fick e-post som verkade vara interna på kommunen. Verksamheten tog bort mejlgruppen. Dataskyddsombudet gick igenom logglistan, men kunde inte identifiera någon allvarligare incident.
- Dataskyddsombudet har granskat text om hantering av personuppgifter vid upphandling av entreprenad.
- Dataskyddsombudet har vid flera tillfällen fått yttra sig om en konsekvensbedömning av bild och film på medarbetare på egna kommunikationskanaler och sociala medier som ledningsgruppen tagit fram.

  Dataskyddsombudet vill understryka att dataskyddsförordningen måste följas och att en konsekvensbedömning inte kan läka om dataskyddsförordningen inte följs, även om det är bättre att riskminimera, än att inte göra det. Dataskyddsombudet bedömde sammantaget att verksamheten inte tillräckligt tydliggjort den höga

[5] Art 39.1b dataskyddsförordningen.

risken för medarbetares rättigheter och friheter samt bedömt risknivån för lågt. Verksamheten bör på kort och lång sikt arbeta för att minska riskerna för personuppgifterna i kommunens kanaler.

Dataskyddsombudet ser positivt på *att* konsekvensbedömningen gjorts, *att* den gjorts på ledningsnivå, *att* film på medarbetare inte ska publiceras på sociala medier, *att* rutinen för behandling av personuppgifter ska följas samt *att* gallringstid ska ha bestämts till ett kortare intervall för personuppgifter på sociala medier.

- Dataskyddsombudet har granskat mediabanken, som utgör kommunens fotobank, och anmärkt på att en omfattande mängd foton innehöll bilder på anställdas barn. Detta utan att det fanns någon rättslig grund. Verksamheten har nu huvudsakligen raderat bilderna där anställdas barn gått att identifiera.
- Dataskyddsombudet har granskat kommunens planer att ingå nytt avtal om intelligens- och personlighetstester vid rekrytering, innebärande tredjelandsöverföring. Viss pseudonymisering skulle användas. Dataskyddsombudet bedömde att personuppgifterna indirekt kunde identifieras och ställde frågan om hanteringen även i övrigt var lämplig. Ärendet fortsätter.
- I ett ärende hade en anställd arbetat med fakturering, som delvis kunde innehålla känsliga uppgifter om hälsa, från tredje land. Dataskyddsombudet bedömde inte möjligt att identifiera skyddsnivån i det tredje landet, utan en mer fördjupad utredning samt poängterade att närmsta chef även skulle kunna ha svårt att göra bedömningen om distansarbete, varför en vägledning med fördel kunde tas fram.
- Den nämnd som endast haft en registrerad behandling av personuppgifter har av dataskyddsombudet rekommenderats att se över om nämnden inte behandlar uppgifter i större utsträckning än så, och i så fall registrera behandlingarna.