Årsrapport dataskydd 2022 för miljö- och hälsoskyddsnämnden

Diarienummer	Senast uppdaterad	Beslutsinstans	Ansvarig processägare
20221124:026	2023-01-25	Dataskyddsombud	Dataskyddsombud

Dokumentets syfte

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

Årsrapporten tas fram av dataskyddsombudet och syftar till att hålla den personuppgiftsansvariga nämnden informerad om hur det gått med behandlingen av personuppgifter år 2022. Detta som ett led för att nämnden ska kunna ta sitt personuppgiftsansvar. Vidare tas årsrapporten fram som ett stöd för att nämnden ska att kunna redovisa sin efterlevnad av dataskyddsförordningen.

Dokumentet gäller för

Nämndens årsrapport riktas sig främst till respektive personuppgiftsansvarig nämnd, men kan vara aktuell för alla anställda som direkt eller indirekt arbetar med personuppgifter i nämndens verksamhet. Årsrapporten 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).

Innehållsförteckning

1. Inledning

I denna rapport redovisar dataskyddsombudet hur det gått med behandlingen av personuppgifter år 2022. I rapporten redovisas till exempel statistik och uppgifter om tillsyn, granskningar, personuppgiftsincidenter, registerutdrag, sanktionsavgifter, skadestånd samt dataskyddsombudets årsberättelse och fortsatta planering för år 2023.

Det är den personuppgiftsansvariga nämnden som är ansvarig för sin behandling av personuppgifter. För år 2022 kommer ingen kvartalsrapport för kvartal fyra skrivas fram, utan denna årsrapport sammanfattar hela året.

2. Gällande rätt och kommunens arbete att tillgängliggöra gällande rätt

En personuppgift är i regel en upplysning om en person som kan leda till att personen direkt eller indirekt kan identifieras. Det kan till exempel vara ett namn, ett personnummer, en adress, en GPS-uppgift, en IP-adress eller andra upplysningar som är specifika för en persons fysiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.[2] Sammantaget är väldigt många uppgifter personuppgifter.

På rekommendation av dataskyddsombudet har det tidigare huvudkontaktombudet under år 2022 tagit fram en rutin för behandling av personuppgifter. Avsikten har varit att göra dataskyddsförordningen och behandling av personuppgifter mer begriplig och lättare för kommunens anställda att förstå och praktisera.

Rutinen har förenklat dataskyddsförordningen i fyra steg enkla steg, som skapar en god grund för korrekt hantering av personuppgifter enligt följande.

- Steg 1: Det första är att bestämma en rättslig grund för behandlingen av personuppgifter. Behandlingen av personuppgifter är endast laglig om det finns en rättslig grund för behandlingen.[3] Det finns sex rättsliga grunder. För kommunens del är det framförallt tre grunder som kommunen kan stödja sig på, avtal, rättslig förpliktelse, myndighetsutövning/allmänt intresse, medan kommunen endast sällan eller aldrig ska stödja sig på samtycke, skydda grundläggande intresse och intresseavvägning.
- Steg 2: Efter att rättslig grund bestämts, så ska personuppgifter alltid behandlas i enlighet med principerna i dataskyddsförordningen, nämligen
    - på ett lagligt, korrekt och transparent sätt,
    - samlas in för ett ändamål,
    - vara relevanta och så få som möjligt,
    - vara korrekta,
    - får inte möjliggöra identifiering längre än nödvändigt och

[2] Jfr. art 4 dataskyddsförordningen.
[3] Art 6 dataskyddsförordningen.

- ska behandlas på ett säkert och konfidentiellt sätt.[4]

Inom detta steg ingår också att bedöma personuppgifternas art, om de är känsliga (till exempel uppgifter om hälsa) eller extra skyddsvärda (till exempel barns personuppgifter), vilket ska generera ett starkare skydd och större varsamhet.

- Steg 3: Under det tredje steget ska den vars personuppgifter behandlas (den registrerades) rättigheter beaktas. Enligt unionsrätten och Förenta nationerna tillerkänns alla personer vissa rättigheter som rätt till privatliv, rätt till rättvis rättegång och rätt till effektivt rättsmedel. Därutöver innehåller dataskyddsförordningen vissa specifika rättigheter, som rätt att få information om personuppgiftsbehandlingen, registerutdrag över de behandlingar myndigheten behandlar om en själv samt rätt till radering, rättelse, begränsning, ändring, invändning, portabilitet och dylikt. Dessa rättigheter måste beaktas i hanteringen av personuppgifter.
- Steg 4: Glöm inte att behandlingen av personuppgifter behöver registreras i ett register, och att en personuppgiftsansvarig identifieras för varje behandling.

Varje kvartal tillställes en kvartalsrapport till ledningsgruppen om dataskyddsarbetet. Varje förvaltningschef har att underrätta nämnden om relevanta delar i kvartalsrapporten, och nämnden bör också kontinuerligt efterfråga information om hur det går med personuppgiftsbehandlingen. Kvartalsrapporterna utgör också ett led i att personuppgiftsansvariga ska kunna redovisa för, nämndens regelefterlevnad av dataskyddsförordningen.

3. Dataskyddsombudets årsberättelse 2022

Nedan presenterar dataskyddsombudet de viktigaste händelserna under år 2022 enligt följande.

- På kommunens intranät har ”Veckans lagtext” publicerat sju avsnitt om GDPR för att sprida kunskap om lagstiftningen och för att ge konkreta råd till verksamheten.
- Det tidigare huvudkontaktombudet har spelat in en ny utbildningsfilm på kommunens intranät om dataskydd.
- Kommunen arbetar med att ta fram en digital utbildningsplattform, *LMS/Learnifier*. Till plattformen har det tagits fram ett omfattande, men lättillgängligt och överblickbart, GDPR-paket med konkreta tips och råd. Liksom i rutinen för behandling av personuppgifter, presenteras samma flera stegs-modell, som ska vara ett praktiskt stöd vid behandling av personuppgifter. Även den, av det tidigare huvudkontaktombudet, framtagna utbildningsfilm finns att ta del av där, uppdelad i korta avsnitt.

[4] Jfr. art 5 dataskyddsförordningen.

- Det tidigare huvudkontaktombudet har tagit fram den rutin av behandling av personuppgifter som nämns i föregående avsnitt, vilken dataskyddsombudet har granskat. Till rutinen har ett modellavtal tagits fram som kommunen kan använda för att ingå avtal med personer gällande bild och film. Avtalet medför att kommunen kan stödja sig på rättsliga grunden avtal i dessa fall. Värt att särskilt notera är avsnittet om sociala medier som riktar sig till den som publicerar personuppgifter på sociala medier.
- En e-tjänst för anmälan av personuppgiftsincidenter har tagits fram som ett led att förenkla processen. E-tjänsten används idag i princip uteslutande för samtliga personuppgiftsincidenter.
- Tidigare huvudkontaktombud har avslutat sin anställning vid kommunen. Nytt huvudkontaktombud har inträtt i september 2022. Det pågår rekrytering av nytt huvudkontaktombud.
- Manualen för kommunens mediabank, som det tidigare huvudkontaktombudet stöttat verksamheten med, är inte klar. Mediabanken nås av alla anställda från intranätet och består av kommunens bildbank. Dataskyddsombudet har efterfrågat status från verksamheten, och betonat att det till exempel inte finns någon rättslig grund för att ha bilder på anställdas barn i mediabanken.
- Dataskyddsombudet har i flera fall granskat kommunens användning av sociala medier och dess förenlighet med dataskyddsförordningen vilket lyfts till ledningsnivå. Dataskyddsombudet har under året intensifierat arbetet i dessa frågor och kontinuerligt lämnat rekommendationer.

  Det är inte förenligt med dataskyddsförordningen att använda personuppgifter i sociala medier med säte utanför EU/EES. Personuppgifterna delas genom publiceringen med tredje land och tredje part. Hanteringen innebär bland annat att personuppgifterna inte hanteras på ett säkert eller konfidentiellt sätt. Den registrerade berövas sina, enligt unionsrätten, tillerkända rättigheter. All hantering med personuppgifter ska i regel också vara *nödvändig*, vilket användningen av sociala medier sällan är.

  I det fall kommunen, i strid med dataskyddsombudets rekommendationer, vill fortsätta publicera personuppgifter på sociala medier ska rättslig grund identifieras, personuppgifterna minimeras till lägstanivå för att nå ändamålet med publiceringen, konsekvensbedömning göras och rutiner för kontinuerlig gallring tas fram. De vars personuppgifter som behandlas på sociala medier ska informeras om att de berövas sina tillerkända rättigheter och att hanteringen inte är konfidentiell och säker. Vissa typer av personuppgifter till exempel, känsliga eller extra skyddsvärda, bör inte alls publiceras.

  Dataskyddsombudet bedömer att kommunens kompetens har höjts inom området och att verksamheten i större omfattning börjat använda bilder från bildbyrå, även om det fortfarande sker att bilder

och filmer på medarbetare publiceras på sociala medier samt att verksamheten uppmuntrar anställda att synas på bild och film.

- Dataskyddsombudet, det tidigare huvudkontaktombudet och kommunens systemförvaltare har haft ett möte med Microsoft.
    - Ett av syftena var att få ut deras behandlingsregister för kommunen, som ett led att kommunen ska kunna identifiera varje dataflöde och behandling av Microsofts tjänster. Kommunen har endast fått Microsofts generella förteckning över kategorier av personuppgifter. Dataskyddsombudet har lämnat rekommendation till huvudkontaktombudet, att verksamheten ser över kommunens behandlingsregister för Microsofts tjänster och lämnat förslag på olika tillvägagångssätt, till exempel genom att samla kontaktombuden eller IT för genomlysning av kommunens processer.[5] Verksamheten har, vad dataskyddsombudet känner till, inte följt rekommendationen.
    - Viva Insight är en funktion i Microsofts tjänster som sammanställer information om anställdas kalendrar, tid och vilka personer de haft mest kontakt med och dylikt. Tidigare har verksamheten stängt av utskick av e-post med den informationen. Microsoft har nu meddelat att funktionen kan stängas av utan negativ konsekvens för kommunen.

      Dataskyddsombudet har rekommenderat att funktionen ska stängas av, eller att verksamheten måste identifiera rättslig grund, göra konsekvensbedömning och informera de anställda om att loggning sker. Verksamheten utreder frågan, men har ännu inte tagit ställning till rekommendationen. Verksamheten har inte vidtagit de ovan nämnda åtgärderna för i det fall Viva insight ska finns kvar.
    - I chattfunktionen i Teams visas sedan en tid tillbaka svarsförslag. Dataskyddsombudet ville få svar på om analysen var kopplad till enskilda personer (personuppgiftsbehandling) eller var en generisk analys. Microsoft förklarade att systemet gör en analys av tidigare lokal korrespondens. Dataskyddsombudet bedömer att frågan är en del av en större fråga om lämpligheten att använda amerikanska molntjänster som helhet.
- Under år 2022 har frågan om tredje landsöverföringar fortfarande varit högst aktuell. Överföringar till tredje land är problematiskt då dataskyddsförordningen inte gäller i tredje land, varför den registrerade fråntas sina, enligt unionsrätten, tillerkända rättigheter och inte kan få sin sak prövad i domstol. Vidare bedöms hanteringen

[5] Även Datatilsynets krav gällande Google workspace innehåller att det ska klargöras vem som bär ansvaret för varje dataflöde (personuppgiftsansvarige, personuppgiftsbiträdet eller ett gemensamt ansvar), vilket visar på att frågan är högst aktuell.

inte säker eller konfidentiell när amerikansk underrättelsetjänst och myndighet har möjlighet att ta del av uppgifter från bolag med säte i USA.

Senaste nytt inom området redovisas enligt följande.

- EU och USA har uttryckt en vilja att ta fram en ny överenskommelse, vilket givetvis får följas med stort intresse.
- Danska tillsynsmyndighetens (Datatilsynets) granskning av Google workspace i skolans verksamhet i Helsingörs kommun. Tillsynsmyndigheten har bedömt att det finns en hög risk för elevers och lärares rättigheter och att risker inte har identifierats och begränsats. Tillsynsmyndigheten ålade kommunen vissa krav, vid äventyr av fängelse, vilket givetvis får följas upp.
- Frankrike har förbjudit Google workspace i skolundervisningen.

Dataskyddsombudet har gjort en kort promemoria av lagar, domar och beslut om rättigheter *kontra* otillåten tredje landsöverföring[6], som distribuerats till berörda när det uppkommit frågor om tredje landsöverföringar. Detta som ett led i att öka förståelsen.

- Verksamheterna har visat flera exempel på ökad förståelse och vilja att efterleva dataskyddsförordningen.
- Kommunledningsgruppen har arbetat för att ta fram en konsekvensbedömning för publicering av anställda på bild och i film, vilken dataskyddsombudet förgranskat. Dataskyddsombudet, som ser positivt på att en konsekvensbedömning görs, vill likväl belysa att en konsekvensbedömning inte kan läka brister i förenligheten med dataskyddsförordningen. Om verksamheten inte finner en korrekt rättslig grund eller kommer till bukt med otillåten tredje landsöverföring är den fortfarande inte laglig, även om en konsekvensbedömning gjorts. En konsekvensbedömning kan dock förbättra situationen, genom att riskminimerande åtgärder (uppgiftsminimering, gallring, styrdokument etc.) kan identifieras och sättas in.
- Dataskyddsombudet har flaggat för att kontaktombuden uppgett att dataskyddsuppgifter läggs på ordinarie arbetsuppgifter, istället för att kontaktombuden får avsatt tid för sitt uppdrag. Den 6 december 2018 rekommenderade det tidigare dataskyddsombudet för ledningsgruppen att kontaktombuden skulle få 20 procent av sin arbetstid avsatt för att utföra uppdraget som kontaktombud. Dataskyddsombudet instämmer i den rekommendationen.

[6] En kort sammanställning av lagar, domar och beslut om rättigheter kontra otillåten tredje landsöverföring inbegripet Teams och sociala medier, ärendenummer 20220628:024.

4. Register för behandlingar

Varje nämnd ska föra register över de personuppgiftsbehandlingar som nämnden utför och ansvarar för.

Miljö- och hälsoskyddsnämnden har 18 behandlingar av personuppgifter i sitt register.

5. Personuppgiftsincidenter

En personuppgiftsincident är en incident som leder till obehörigt röjande av eller åtkomst till personuppgifter. Det kan också röra sig om oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter.[7] Personuppgifts-incidenter upptäcks vanligen av verksamheten eller av dataskyddsombudet i samband med granskning eller kontakt med verksamheten; eller av kommunens leverantörer.

Om en personuppgiftsincident inträffar ska den anmälas till dataskyddsombudet. Dataskyddsombudet utreder incidenten vidare. Dataskyddsombudet gör en rekommendation till verksamheten om incidenten behöver anmälas till tillsynsmyndigheten. Den personuppgiftsansvarige ska sen utan onödigt dröjsmål, inom 72 timmar efter att ha fått vetskap om personuppgiftsincidenten, anmäla den till tillsynsmyndigheten, såvida det inte är *osannolikt* att incidenten medför *risk* för *fysiska personers rättigheter och friheter*.[8] Personuppgiftsincidenter ska registreras i respektive nämnds diarium.

Det finns ingen lägsta nivå för vad som kan utgöra en personuppgiftsincident. Det kan i princip förväntas att i vart fall någon e-post skickats fel eller mobiltelefon förlorats under året, varför i vart fall några incidenter årligen talar för en väl fungerande dataskyddsorganisation, genom att sådana personuppgiftsincidenter upptäcks och rapporteras.

Det är oerhört komplext att identifiera en lämplig nivå för antalet personuppgiftsincidenter. Olika personuppgiftsansvariga nämnder hanterar olika mängd och typ av personuppgifter. Vissa nämnder hanterar i större utsträckning extra skyddsvärda och känsliga personuppgifter, än andra nämnder. Olika nämnder har olika frekvens på arbetet. Om en nämnd har *många personuppgiftsincidenter* kan det tala för att verksamheten, med stöd i god kännedom om dataskyddslagstiftningen, identifierar och 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 upptäcks eller anmäls i den utsträckning som dataskyddsförordningen kräver.

Kommunen har totalt haft 54 personuppgiftsincidenter år 2022. De nämnder som har haft minst personuppgiftsincidenter har haft noll incidenter. Den nämnd som haft flest incidenter har haft 27 stycken under året.

[7] Art. 4.12 dataskyddsförordningen.
[8] Art 33 dataskyddsförordningen.

Under år 2022 har noll personuppgiftsincidenter från miljö- och hälsoskyddsnämnden kommit till dataskyddsombudets kännedom.

6. Dataskyddsombudets stora granskning

Dataskyddsombudet har genomfört en stor planerad granskning av kommunens rutiner för behandling av personuppgifter och personuppgiftsincidenter under år 2022. Varje nämnd har genom förvaltningen fått redovisa sitt arbetssätt och sina rutiner, på av dataskyddsombudet ställda frågor. Dataskyddsombudet har redovisat resultatet av granskningen den 20 juni 2022.

Dataskyddsombudet har kommit fram till

- att kommunikationen mellan den personuppgiftsansvarige nämnden och förvaltningen behöver bli bättre, för att nämnden ska bedömas kunna ta sitt, enligt dataskyddsförordningen, ålagda ansvar,
- att kunskapsnivån bedöms ha höjts över lag i verksamheten, men att chefer och ledningsgrupper behöver vara mer involverade i arbetet med dataskydd, och
- att beslut om anmälan till tillsynsmyndigheten bör fattas på nämndens delegation, samt att den chef/delegat som står tillräckligt långt ifrån ärendet för att kunna göra en objektiv bedömning, ska skicka in anmälan till tillsynsmyndigheten.

Kommundirektören har föreslagit att kopia på anmälan ska anmälas som delegationsbeslut till nämnden för att undvika administration. Dataskydds-ombudet har inget att invända mot en sådan hantering.

Vad dataskyddsombudet känner till har endast någon nämnd noterat rapporten från den stora granskningen i nämnden. Detta är olyckligt eftersom det är nämnden som är ansvarig för det som granskningen gällde – behandling av personuppgifter och personuppgiftsincidenter. Det dataskyddsombudet fann i granskningen, att nämnden måste bli mer informerad för att kunna ta sitt enligt dataskyddsförordningen ålagda ansvar, synes i vart fall, i det sammanhanget, inte ha hörsammats.

7. Dataskyddsombudets reaktiva granskningar

Dataskyddsombudet kan på eget initiativ initiera granskning av efterlevnaden av dataskyddsförordningen. Det vanliga är att dataskyddsombudet själv, eller i kontakt med verksamheten upptäcker något, som dataskyddsombudet vill titta närmare på.

Vid en typisk granskning ställer dataskyddsombudet frågor till verksamheten om behandling av personuppgifterna eller vid upphandlingar, om kommande behandling av personuppgifter. Utifrån svaren på frågorna kan dataskyddsombudet lämna bestämda rekommendationer om fortsatt tillvägagångssätt. Svaren kan också leda till att högsta förvaltningsnivå, den

personuppgiftsansvarige nämnden eller till att tillsynsmyndigheten informeras.[9]

Totalt har dataskyddsombudet gjort 37 reaktiva granskningar under år 2022. Den nämnd som har mest har haft 20 granskningar. De nämnder som har haft minst har haft noll granskningar.

Dataskyddsombudet har under år 2022 utfört noll reaktiva granskningar av miljö- och hälsoskyddsnämndens verksamhet.

8. Tillsyn

Tillsynsmyndigheten har inte under år 2022 genomfört någon tillsyn eller annonserat någon kommande tillsyn hos någon av kommunens nämnder.

9. Registerutdrag

En person har rätt att begära att få veta om dennes personuppgifter behandlas av kommunen. Om kommunen behandlar personens personuppgifter har personen rätt att få veta ändamålet med behandlingen och annan information.[10]

Miljö- och hälsoskyddsnämnden har fått sex förfrågningar om registerutdrag under år 2022.

10. Administrativa sanktionsavgifter

Tillsynsmyndigheten kan påföra den som behandlat personuppgifter i strid med dataskyddslagstiftningen en administrativ sanktionsavgift, som ska vara effektiv, proportionell och avskräckande.[11] För mindre allvarliga överträdelser ska avgiften uppgå till högst 5 miljoner kronor och för mer allvarliga överträdelser till högst 10 miljoner kronor för myndigheter.[12]

Tillsynsmyndigheten har inte påfört någon administrativ sanktionsavgift på kommunen under år 2022.

11. Skadestånd

Varje person som lidit skada till följd av en överträdelse av dataskyddslagstiftningen ska ha rätt till ersättning (skadestånd). Varje personuppgiftsansvarig nämnd som medverkat till behandling i strid med dataskyddslagstiftningen ska ansvara för skadan.[13]

Ingen av kommunens nämnder har fått in begäran om skadestånd för felaktig behandling av personuppgifter under år 2022.

[9] Jfr. art 38 dataskyddsförordningen.
[10] Art. 15 dataskyddsförordningen.
[11] Art 83 dataskyddsförordningen.
[12] 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[13] Art 82 dataskyddsförordningen.

12. Planering för år 2023

Dataskyddsombudet har avsikten att genomföra några planerade granskningar år 2023 och framåt.

- 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.
- Dataskyddsombudet bedömer att det finns utrymme att fundera kring varför vissa nämnder har flertalet personuppgiftsincidenter och granskningar, medan vissa nämnder inte har några. Frågan är komplex eftersom många personuppgiftsincidenter, inte behöver innebära en sämre hantering, utan kan tala för att verksamheten identifierar och anmäler incidenter när de sker, och vice versa. Olika nämnder hanterar också olika mängd och typer av personuppgifter.

  Dataskyddsombudet initierar också reaktiva granskningar vid kontakt med verksamheten. De nämnder dataskyddsombudet har minst kontakt med, tenderar därför att bli mindre granskade, vilket är olyckligt. Detta gäller även om dataskyddsombudet planerade granskning 2022 riktade sig till samtliga nämnder.

  Dataskyddsombudet skulle därför under våren 2023, tillsammans med huvudkontaktombudet och kontaktombuden, försöka få ett samlat grepp om problematiken och se om det finns alternativa metoder för att etablera kanaler med samtliga nämnder.