Dataskyddsombudets rapport

Granskning av hantering av personuppgifter och personuppgiftsincidenter

Diarienummer	Senast uppdaterad	Beslutsinstans	Processägare
20211207:044	2022-06-20	Dataskyddsombud	Dataskyddsombud

Dokumentets syfte

Syftet med rapporten är att meddela resultatet av granskningen av kommunens rutiner för hanteringen av personuppgifter och personuppgiftsincidenter i Danderyds kommun.

Rapporten avser att stödja den personuppgiftsansvariga i dennes skyldighet att ansvara för, och kunna visa på, att dataskyddsförordningen efterlevs.

Dokumentet gäller för

Rapporten riktar sig främst till personuppgiftsansvariga i Danderyds kommun och ställs till kommunledningen i dess kommunövergripande funktion.

DANDERYDS KOMMUN

Innehållsförteckning

1 Inledning

Dataskyddsombudet har granskat kommunens rutiner för hanteringen av personuppgifter och personuppgiftsincidenter. Utgångspunkten för granskningen är att god struktur förbättrar förutsättningarna för en korrekt hantering av personuppgifter enligt dataskyddsförordningen. Det har också funnits en bakomliggande avsikt att kommunens dataskyddsarbete på sikt ska bli så bra och rättssäkert som möjligt. Syftet med denna rapport är att meddela resultatet av granskningen.

Granskningen har gått till så att remiss med frågor har skickats till förvaltningarna. Eftersom det rört sig om redovisning av arbetssätt, vilket inte krävt bedömningar eller överväganden, har förvaltningarna lämnat svar å sina nämnders vägnar. Samtliga remissinstanser har svarat. Sammantaget ger svaren en god insyn i hur hanteringen av personuppgifter och personuppgiftsincidenter går till i kommunen.

2 Gällande rätt

I kommunen är nämnderna *personuppgiftsansvariga* för sin behandling av personuppgifter. Den personuppgiftsansvarige nämnden ska ansvara för och kunna visa att dataskyddsförordningen efterlevs.[1] Den personuppgiftsansvarige nämnden bestämmer ändamålen och medlen för behandling av personuppgifter och kan tilldelas administrativa sanktionsavgifter av tillsynsmyndigheten.[2] De personuppgiftsansvariga nämndernas ansvar kan inte delegeras till förvaltningen, även om arbetsuppgifterna kan det.

1. Behandlingen av personuppgifter är endast laglig om det finns en *rättslig grund* för behandlingen.[3] För att få behandla personuppgifter måste alltså en rättslig grund först identifieras. Följande rättsliga grunder finns[4]:
    - Samtycke (ska i regel inte användas av kommun[5])
    - Avtal
    - Rättslig förpliktelse
    - Skydda grundläggande intressen (används inte av kommun[6])
    - Myndighetsutövning och uppgift av allmänt intresse
    - Intresseavvägning (ska i regel inte användas av kommun[7])

[1] Art 5 dataskyddsförordningen (Hyperlänk: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679, 2022-05-10).
[2] Jfr. art 4.7 och 83 dataskyddsförordningen.
[3] Art 6 dataskyddsförordningen.
[4] Art 6 dataskyddsförordningen.
[5] Samtycke som rättslig grund | IMY (Hyperlänk: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/samtycke/, 2022-06-17).
[6] Skydda grundläggande intressen | IMY (Hyperlänk: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/skydda-grundlaggande-intressen/, 2022-06-17)
[7] Intresseavvägning som rättslig grund | IMY (Hyperlänk: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/intresseavvagning/, 2022-06-17)

2. Vidare ska hantering av personuppgifter ske enligt *principerna* i dataskyddsförordningen. Principerna innebär att personuppgifter ska[8]:

    - Behandlas på ett lagligt, korrekt och transparent sätt
    - Samlas in för ett angivet ändamål
    - Ska vara relevanta och så få som möjligt
    - Ska vara korrekta
    - Får inte möjliggöra identifiering längre än nödvändigt
    - Ska behandlas på ett säkert och konfidentiellt sätt, med beaktande av integritet

3. En person inom EU är tillerkänd flera rättigheter, vilka alltid måste beaktas vid behandling av personuppgifter, till exempel rätt till[9]:

    - Respekt för privat- och familjeliv (kommunikation)
    - Skydd av personuppgifter

    Den registrerade tillerkänns enligt dataskyddsförordningen flera specifika rättigheter vilka alltid måste beaktas vid behandling av personuppgifter, till exempel rätt till[10]:

    - Rättelse
    - Ta del av sina uppgifter
    - Information
    - Begränsning
    - Invända
    - Flytta uppgifter

2.1 Personuppgiftsincidenter

En korrekt och effektiv hantering av *personuppgiftsincidenter* är ett viktigt led i dataskyddsarbetet. En personuppgiftsincident är en *oavsiktlig* eller *olaglig* händelse (till exempel felaktig hantering) som leder till förstöring, förlust, ändring, obehörigt röjande eller obehörig åtkomst av personuppgifter.[11]

Vid en personuppgiftsincident *ska* den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar, *anmäla* incidenten till tillsynsmyndigheten, om det *inte* är *osannolikt* att personuppgiftsincidenten medför *risk* för *personers rättigheter* (se avsnittet ovan punkt 3) *och friheter*.[12] Med andra ord, finns det *en sannolik risk* för fysiska personers rättigheter och friheter *ska* personuppgiftsincidenten anmälas till tillsynsmyndigheten. Faktisk skada vid krävs inte.

[8] Jfr. art 5 dataskyddsförordningen.
[9] Art 7 och 8 europeiska unionens stadga om de grundläggande rättigheterna (Hyperlänk: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:12012P/TXT&from=SV, 2022-06-17).
[10] Kapitel 3, avsnitt 3-4 dataskyddsförordningen.
[11] Jfr. art 4.12 dataskyddsförordningen.
[12] Art 33 dataskyddsförordningen.

2.2 Dataskyddsombudets roll

Dataskyddsombudet har till uppgift att övervaka hur kommunen efterlever dataskyddsförordningen. Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet inte tar emot instruktioner eller blir utsatt för sanktioner för att ha utfört sina uppgifter.[13]

3 Resultat och bedömning

Remissinstanserna har redogjort för sin hantering på olika sätt och under olika frågor. Därför blir det osammanhängande att redovisa svaren fråga för fråga.

Nedan redovisas resultatet av granskningen av hanteringen av personuppgifter och personuppgiftsincidenter, fördelat i tre specifika områden.

- Den personuppgiftsansvariga nämndens hantering
- Verksamhetens hantering
- Vem beslutar om anmälan av personuppgiftsincidenter till tillsynsmyndigheten och vem fyller i anmälan

Varje avsnitt avslutas med dataskyddsombudets bedömning och rekommendation.

3.1 Den personuppgiftsansvariga nämndens hantering

Samtliga remissinstanser har uppgett att de utsett kontaktombud och att de personuppgiftsansvariga nämnderna godkänner dataskyddsombudets årsrapport i nämnden.

- Kommunstyrelsen har vidare anfört att hantering av personuppgifter endast sker på förvaltningsnivå.
- Tekniska nämnden och Fastighetsnämnden har vidare anfört att kontroll sker i internkontrollen och rapporteras till nämnden två gånger per år.

3.1.1 Dataskyddsombudets bedömning och rekommendation

Remissinstansernas svar ger inga egentliga svar på hur de personuppgifts-ansvariga nämnderna faktiskt tar sitt ansvar för hanteringen av personuppgifter. Svaren indikerar att arbetet med personuppgiftshantering främst sköts på förvaltningsnivå och utvecklas genom förvaltningens egna initiativ och arbete, utan de personuppgiftsansvariga nämndernas engagemang.

Det är i regel endast dataskyddsombudets årsrapport som redovisas till nämnderna vad gäller hanteringen av personuppgifter. Det innebär att information om hantering av personuppgifter och personuppgiftsincidenter kan komma att anmälas till den personuppgiftsansvariga nämnden, mer än ett helt år efter att de inträffat. Genom kvartalsrapporterna, som ställs till kommunledningen, finns i vart fall förutsättningar för kommunledningen eller direktören att i ett tidigare skede informera de personuppgiftsansvariga

[13] Art 38-39 dataskyddsförordningen.

nämnderna vid behov. Vissa remissinstanser har uppgett att så skulle kunna ske.

Dataskyddsförordningen är inte är primärt utvecklad efter kommuners organisation och har inte fäst avseende vid förhållandet mellan de personuppgiftsansvariga nämnderna (vilka har ansvaret för hanteringen) och förvaltningen (som rent faktiskt arbetar med hanteringen av personuppgifter och personuppgiftsincidenter). Inte heller har dataskyddsförordningen harmoniserats med vad som kommunalrättsligt gäller för verkställighet och beslut. Detta leder till en rad svårigheter.

Eftersom de personuppgiftsansvariga nämnderna har ansvaret för sin hantering av personuppgifter och personuppgiftsincidenter, borde nämnderna vara mer informerade i dessa frågor. Att vänta in dataskyddsombudets eventuella kritik i årsrapporten (den metod som verkar vara gällande) är inte tillräckligt för att den personuppgiftsansvariga nämnden ska kunna bedömas ha tagit sitt, i enlighet med dataskyddsförordningen, ålagda ansvar.[14] Notera att de personuppgiftsansvariga nämndernas ansvar inte kan delegeras till förvaltningen.

En med enkla medel verkställbar åtgärd skulle kunna vara att punkten ”aktuellt inom personuppgiftshantering” anmäls muntligen vid varje nämndsammanträde. Detta skulle också ha en preventiv verkan, genom att det kontinuerligt påminner den personuppgiftsansvariga nämnden om deras ansvar.[15]

Sammanfattningsvis står klart att de personuppgiftsansvariga nämnderna behöver bättre, mer aktuell och kontinuerlig information om hantering av personuppgifter och personuppgiftsincidenter, för att kunna ta det personuppgiftsansvar som de enligt dataskyddsförordningen är ålagda att ta.[16]

3.2 Verksamhetens hantering

Samtliga remissinstanser har redogjort för sin organisation med utsedda kontaktombud och uppgett att de följer informationen om personuppgiftsincidenter som finns på intranätet, att utbildningsinsatser har genomförts och att personuppgiftsincidenter diarieförs i ett samlingsärende.

- Kommunstyrelsen har vidare anfört att respektive avdelningschef bär ansvaret för att personuppgiftsincidenter hanteras korrekt.
- Byggnadsnämnden samt miljö- och hälsoskyddsnämnden har vidare anfört att kontaktombuden planerar med chef per halvår och följer upp.
- Utbildningsnämnden samt kultur- och fritidsnämnden har vidare anfört att beslut om begäran av skadestånd och övriga rättigheter är delegerade till en funktion inom förvaltningen.

[14] Jfr. art 5.2 dataskyddsförordningen.
[15] Jfr. art 5.2 dataskyddsförordningen.
[16] Jfr. art 5.2 dataskyddsförordningen.

- Socialnämnden har vidare anfört att ledningsgruppen fattar beslut om hanteringen av personuppgifter och att egna rutiner har tagits fram.

3.2.1 Dataskyddsombudets bedömning och rekommendation

Organisationen för dataskydd (kontaktombuden, huvudkontaktombudets och dataskyddsombudets roller) ger goda förutsättningar för ett korrekt, effektivt och förvaltningsöverskridande arbete med hanteringen av personuppgifter och personuppgiftsincidenter.

Huvudkontaktombudets och kontaktombudens kontinuerliga arbete, i kombination med hanterade granskningar, personuppgiftsincidenter och utbildningssatsningar, bedöms ha höjt kunskapen om dataskyddsförordningen över lag i verksamheten.

Även förståelsen för vikten av att följa dataskyddsförordningen bedöms ha höjts. Detta arbete måste givetvis fortsätta. Verksamheterna har även i handling bekräftat att det finns en vilja att följa dataskyddsförordningen, till exempel genom verksamheternas pågående arbete med uppgiftsminimering och gallring av personuppgifter på sociala medier.

Remissinstanserna har i varierande omfattning anfört att chefer är engagerade i arbetet med personuppgifter. Utifrån den omfattande mängd personuppgifter kommunen hanterar, kommunens roll som myndighet och kommunens ansvar enligt dataskyddsförordningen, behöver chefer och ledningsgrupper vara ledande och delaktiga i arbetet med hanteringen av personuppgifter och personuppgiftsincidenter.

3.3 Vem beslutar om anmälan av personuppgiftsincidenter till tillsynsmyndigheten och vem fyller i anmälan

Enligt dataskyddsförordningen *ska den personuppgiftsansvarige nämnden* om möjligt inom 72 timmar anmäla en personuppgiftsincident till tillsynsmyndigheten, om det inte är osannolikt att personuppgiftsincidenten medför risk för personers rättigheter och friheter.[17]

Vem beslutar om anmälan av personuppgiftsincidenter till tillsynsmyndigheten

När en personuppgiftsincident anmälas till dataskyddsombudet lämnar dataskyddsombudet en rekommendation om incidenten ska anmälas till tillsynsmyndigheten. Frågan här gäller *vem* som därefter tar beslut om personuppgiftsincidenten ska anmälas till tillsynsmyndigheten.

- Kommunstyrelsen, byggnadsnämnden, miljö- och hälsoskyddsnämnden, tekniska nämnden, fastighetsnämnden har anfört att beslut om anmälan till tillsynsmyndigheten hanteras som verkställighet på förvaltningsnivå.
- Utbildningsnämnden samt kultur- och fritidsnämnden har anfört att ett ärende om anmälan till tillsynsmyndigheten har behandlats i den personuppgiftsansvariga nämnden.

[17] Art 33 dataskyddsförordningen.

- Socialnämnden har anfört att delegationsbeslut fattas om anmälan till tillsynsmyndigheten.

Vem fyller i anmälan av personuppgiftsincidenter till tillsynsmyndigheten

Anmälan till tillsynsmyndigheten fylls i på tillsynsmyndighetens hemsida, genom att en person, klickar i svar på, av tillsynsmyndigheten, ställda frågor.

- Kommunstyrelsen har anfört att den tjänsteman som bäst har kunskap om personuppgiftsincidenten fyller i anmälan.
- Byggnadsnämnden samt miljö- och hälsoskyddsnämnden har anfört att förvaltningschef får underteckna framställningar till andra myndigheter och att det är tänkbart att en anmälan fylls i gemensamt av förvaltningschefen, kontaktombud, administrativ chef och/eller den som upptäckt incidenten.
- Tekniska nämnden och fastighetsnämnden har anfört att förvaltnings- eller administrativ chef fyller i anmälan.
- Utbildningsnämnden samt kultur- och fritidsnämnden har anfört att den person som upptäckt incidenten, tillsammans med ansvarig chef eller kontaktombudet, fyller i anmälan.
- Socialnämnden har anfört att en av socialdirektören utsedd tjänsteperson fyller i anmälan.

3.3.1 Dataskyddsombudets bedömning

Vissa remissinstanser hanterar *beslutet*, om personuppgiftsincidenten ska anmälas till tillsynsmyndigheten, som verkställighet, medan andra remissinstanser tar beslut på delegation eller i nämnden. Remissinstanserna har olika rutiner för *vem* som fyller i anmälan till tillsynsmyndigheten på tillsynsmyndighetens hemsida.

Av vad remissinstanserna har uppgett saknas tydliga bestämmelser för vem som tar beslutet och vem som fyller i eventuell anmälan till tillsynsmyndigheten.

Bristen på bestämmelser och konkreta exempel från verkligheten visar på att det idag uppstår eller riskerar att uppstå en ytterst olycklig och tveksam hantering. Se nedan.

- En tjänsteperson har utfört, upptäckt eller varit delaktig i en personuppgiftsincident.
- Samma tjänsteperson beslutar om eventuell anmälan till tillsynsmyndighet som verkställighet. Detta alltså utan den personuppgiftsansvariga nämnden har gett en delegation och utan att nämnden får information om beslutet.
- Samma tjänsteperson fyller själv i anmälan av incidenten till tillsynsmyndigheten. Detta utan att objektivt kunna värdera incidenten, eftersom person själv utfört, upptäckt eller varit delaktig i den.

Även i det fall chefen är informerad, upplyst eller involverad i ovan hantering, bedöms hanteringen inte helt lämplig.

3.3.2 Dataskyddsombudets rekommendation

Vem beslutar om anmälan av personuppgiftsincidenter till tillsynsmyndigheten

Enligt dataskyddsförordningen *ska den personuppgiftsansvarige nämnden* anmäla en personuppgiftsincident till tillsynsmyndigheten, under de däri angivna förutsättningarna.[18]

Beslutet, huruvida kommunen ska anmäla en personuppgiftsincident till tillsynsmyndigheten, inrymmer både överväganden och bedömningar. Beslutet kan få betydande konsekvenser för kommunen, till exempel genom att tillsynsmyndigheten inleder tillsyn och kommunen tilldelas administrativa sanktionsavgifter. Under dessa förhållanden finns inte utrymme att betrakta beslutet som verkställighet, utan den personuppgiftsansvarige nämnden har att fatta beslutet.[19] Eftersom en personuppgiftsincident ska anmälas inom 72 timmar, sker beslutsfattandet lämpligen genom delegation till delegater på förvaltningen.[20] Jämför vidare med till exempel Stockholms stads[21] och Upplands-Bro kommuns[22] delegationsordningar.

Eftersom delegaten måste stå tillräckligt långt ifrån ärendet, för att kunna göra en objektiv bedömning av ärendet, kan det vara lämpligt att utse minst två delegater. Beslutet ska anmälas till nämnden.

Vem fyller i anmälan av personuppgiftsincidenter till tillsynsmyndigheten

Det är inte lämpligt att den tjänsteperson som själv utfört, upptäckt eller varit delaktig i incidenten, fyller i anmälan till tillsynsmyndigheten. Detta eftersom tjänstepersonen kan ha svårt att värdera incidenten på ett objektivt sätt. Den som fyller i anmälan till tillsynsmyndigheten bör stå tillräckligt långt ifrån ärendet, för att kunna fylla i anmälan till tillsynsmyndigheten på ett objektivt sätt.

Den närmsta chefen till den som utfört, upptäckt eller varit delaktig i incidenten, bör fylla i anmälan till tillsynsmyndigheten på tillsynsmyndighetens hemsida. Chefen ska stå tillräckligt långt ifrån ärendet för att kunna fylla i anmälan på ett objektivt sätt. I annat fall bör överordnad chef fylla i anmälan till tillsynsmyndigheten.

4 Sammanfattning

- Vad gäller den personuppgiftsansvariga nämndens hantering behöver kommunikationen mellan nämnden och förvaltningen bli bättre, mer aktuell och kontinuerlig för att den

[18] Art 33 dataskyddsförordningen.
[19] Jfr. prop. 2016/17:171 s. 382.
[20] Art 33 dataskyddsförordningen.
[21] Jfr. Stockholms stad, Delegationsordning för äldrenämnden, beslutad den 31 augusti 2021, ALD 2021/296, punkt 1.32.
[22] Jfr. Upplands-Bro kommun, kommunstyrelsens delegationsordning, beslutad den 16 mars 2022, KS 21/0529, punkten A 6.9.

personuppgiftsansvarige nämnden ska kunna bedömas ta sitt, enligt dataskyddsförordningen, ålagda ansvar. Detta innebär att nuvarande ordning måste ses över och ändras.

- Vad gäller verksamhetens hantering så visar huvudkontaktombudets och kontaktombudens arbete, i kombination med hanterade granskningar, personuppgiftsincidenter och utbildningsinsatser, att kunskapsnivån har höjts över lag i verksamheten. Chefer och ledningsgrupper behöver vara ledande och mer involverade i arbetet med personuppgifter. Detta innebär att nuvarande ordning måste ses över och ändras.
- Den personuppgiftsansvariga nämnden har att fatta beslutet om anmälan av personuppgiftsincidenten till tillsynsmyndigheten, eftersom beslutet kan få betydande konsekvenser för kommunen. Lämpligen utses minst två delegater på förvaltningen och beslutet ska anmälas till nämnden. Detta innebär att nuvarande ordning måste ses över och ändras.

  Närmsta chef till den som utfört, upptäckt eller varit delaktig i personuppgiftsincidenten bör fylla i anmälan till tillsynsmyndigheten, om chefen står tillräckligt långt ifrån ärendet för att kunna fylla i anmälan på ett objektivt sätt. I annat fall överordnad chef. Detta innebär att nuvarande ordning måste ses över och ändras.