Årsrapport dataskydd 2021 för kommunstyrelsen

Diarienummer	Senast uppdaterad	Beslutsinstans	Ansvarig processägare
20220121:024	2022-01-21	Dataskyddsombud	Dataskyddsombud

Dokumentets syfte

Dokumentet syftar till att redovisa hur det gått med behandlingen av personuppgifter och dataskydd under år 2021.

Dokumentet gäller för

Dokumentet gäller för hela kommunens verksamhet.

Innehållsförteckning

1. Inledning

I denna rapport redovisar dataskyddsombudet hur det gått med behandlingen av personuppgifter och dataskydd under år 2021. I rapporten redovisas dataskyddsarbetet såsom till exempel uppgifter om statistik, tillsyn, granskningar, personuppgiftsincidenter, registerutdrag, sanktionsavgifter, skadestånd, årsberättelse och fortsatt planering.

Det är nämnden som är ansvarig för sin behandling av personuppgifter.

2. Gällande rätt

En personuppgift är i regel en upplysning om en person, som kan leda till att personen 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.[1]

Personuppgifter ska enligt lagstiftningen i korthet

- behandlas 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,
- ska behandlas på ett säkert sätt.[2]

I kommunen är den aktuella nämnden personuppgiftsansvarig för sin behandling av personuppgifter. Den personuppgiftsansvarige (nämnden) ansvarar för och ska kunna visa att lagstiftningen efterlevs.[3]

Behandlingen av personuppgifter är endast laglig om det finns en rättslig grund för behandlingen.[4]

3. Dataskyddsorganisation

Under hösten har dataskyddsorganisationen börjat arbeta efter en ny ordning. Dataskyddsorganisation uppdaterades formellt den 1 december 2021. Ändringarna rör framförallt dataskyddsombudets arbetsuppgifter och införandet av ett huvudkontaktombud. Dataskyddsorganisation ser nu ut som följande.[5]

- Utöver kontaktombuden, som finns på varje avdelning eller enhet som arbetar proaktivt och operativt med dataskyddsfrågor, finns nu också ett huvudkontaktombud (kommunstyrelsens kontaktombud). Huvudkontaktombudet arbetar främst, utöver sina arbetsuppgifter som kontaktombud, med proaktiva och operativa åtgärder som att ge

[1] Jfr. art 4 dataskyddsförordningen.
[2] Jfr. art 5 dataskyddsförordningen.
[3] Art 5 dataskyddsförordningen.
[4] Art 6 dataskyddsförordningen.
[5] Läs mer i Anvisning organisation för säkerhet och dataskydd, KS 2021/0474, daterad den 1 december 2021.

råd och hålla utbildning samt att samordna kommunens nätverk för kontaktombud.

- Dataskyddsombudet arbetar främst reaktivt med granskning av efterlevnaden av dataskyddslagstiftningen, konsekvensbedömningar och personuppgiftsincidenter.

4. Register för behandlingar

Varje nämnd måste ha ett register över personuppgiftsbehandlingar som beskriver de behandlingar som sker inom nämndens personuppgiftsansvar. Verksamheten ansvarar för att hålla registret aktuellt. Registret sker i systemstödet Draftit.

Kommunstyrelsen har i sitt register 155 antal behandlingar av personuppgifter**.**

5. Personuppgiftsincidenter

En personuppgiftsincident är en incident som leder till obehörigt röjande eller åtkomst till personuppgifter. Det kan också röra sig om oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter.[6] Det kan till exempel vara att någon skickat en e-post med känsliga personuppgifter utan kryptering till en annan e-postadress än den som slutar på @danderyd.se, eller att någon anställd får del av personuppgifter i onödan, som personen inte behöver för sitt arbete och utanför dennes behörighet.

Personuppgiftsincidenter upptäcks vanligen

- av verksamheten,
- av dataskyddsombudet i samband med granskning eller kontakt med verksamheten eller
- av kommunens systemleverantörer.

Om en personuppgiftsincident inträffar ska den anmälas till dataskyddsombudet. Dataskyddsombudet utreder incidenten vidare i samråd med verksamheten. Dataskyddsombudet gör en rekommendation 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.[7]

Om en nämnd har flera personuppgiftsincidenter kan det tala för att verksamheten har god kännedom om dataskyddslagstiftningen, och att verksamheten med stöd i denna kunskap 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

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

personuppgifter, eller att personuppgiftsincidenter inte upptäcks eller anmäls i den utsträckning som det enligt lag krävs.

Kommunstyrelsen har haft tio (10) personuppgiftsincidenter under år 2021. Av dessa har dataskyddsombudet rekommenderat att tre (3) personuppgifts-incidenter anmälts till tillsynsmyndigheten.

Nedan redovisas några personuppgiftsincidenter:

- Vid dataskyddsombudets granskning av kommunens kamerabevakning av parkeringsplatsen på Vendevägen kontrollerades om kommunen följde tillsynsmyndighetens förbehåll i tillståndet för kamerabevakningen. Dataskyddsombudet identifierade flera avvikelser. Kommunen hade även lämnat ut en film som visade ett område med personer som kommunen inte haft tillstånd att bevaka, till en annan myndighet. Verksamheten agerade skyndsamt på dataskyddsombudets rekommendationer. Ärendet anmäldes till tillsynsmyndigheten, som nu har skrivit av ärendet.
- En anställds personnummer noterades på en beställning via kommunens e-tjänst, utan att det fanns något skäl till det. Eftersom felet rättades till omgående bedömde dataskyddsombudet att personuppgiftsincidenten inte behövde anmälas till tillsynsmyndigheten.
- Vid byte från ett system till ett annat riskerades en viss typ av ärenden att gå förlorade, utan att det fanns stöd i dokumenthanteringsplanen för det. Eftersom verksamheten hade tid för att flytta över ärendena bedömde dataskyddsombudet att personuppgiftsincidenten inte behövde anmälas till tillsynsmyndigheten. Verksamheten arbetar fortfarande med att förhindra att någon information ska gå förlorad.
- En sökväg i personalsystemet medförde att 110 chefer kunde se personuppgifter om 1475 anställda och 350 visstidsanställda, och namnet på deras barn. Felet anmäldes och skulle åtgärdas i mars, men bestod i oktober 2021. Dataskyddsombudet rekommenderade anmälan till tillsynsmyndigheten och andra förebyggande åtgärder. Felet är nu åtgärdat.
- I en rapport från ronderande väktare nämndes en minderårig individ med namn, telefonnummer och misstanke om brott. Rapporten skickas till ett tiotal anställda på kommunen. Dataskyddsombudet rekommenderade anmälan till tillsynsmyndigheten och andra förebyggande åtgärder liksom att den registrerade skulle informeras. Väktarbolaget har fastställt nya rutiner för att inte sprida information på detta sätt i framtiden.

6. Planerad granskning av rutiner för behandling av personuppgifter

Dataskyddsombudet har i december 2021 påbörjat en granskning av strukturen för dataskyddsarbetet i respektive förvaltning/nämnd. Syftet med granskningen är att utreda om kommunen följer dataskyddslagstiftningen

utifrån kommunens rutiner för behandling av personuppgifter och personuppgiftsincidenter. Utgångspunkten för granskningen är att god struktur i dataskyddsarbetet förbättrar förutsättningarna för en korrekt behandling av personuppgifter.

Svaren kommer ge god insyn i hur behandling av personuppgifter och personuppgiftsincidenter går till i kommunen. Förvaltningarna ska inkomma med svar senast den 14 februari 2022.

Utöver den kommungemensamma granskning som det redogjorts för ovan kommer kommunstyrelsens användning av samtycke som rättslig grund att granskas år 2022. Detta eftersom kommunstyrelsen påvisat brister i behandlingen av personuppgifter med samtycke som rättslig grund vid dataskyddsombudets granskning år 2020.

7. Reaktiva granskningar

Dataskyddsombudet kan på eget initiativ initiera granskning av efterlevnaden av dataskyddslagstiftningen. 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 tillsynsmyndigheten informeras.[8]

Dataskyddsombudet har under år 2021 utfört sex (6) reaktiva granskningar i kommunstyrelsens verksamhet.

Nedan redovisas några granskningar:

- Granskning av e-post till anställda med statistik om hur den anställde använder sin arbetstid och vilka kollegor den anställda har mest kontakt med. Verksamheten har nu stoppat utskicket av e-posten. Granskningen pågår.
- Granskning av kamerabevakning. Se under personuppgiftsincident.
- Granskning av kommunens avtal med leverantör för friskvårdshantering. Dataskyddsombudet konstaterade en risk för att personuppgifter skulle kunna komma att överföras till tredje land och lämnade även andra rekommendationer. Verksamheten fick till stånd ett nytt avtal med leverantören. Ärendet avslutades.
- Granskning av kommunens mediabank för kommunikation utifrån om det finns rättslig grund för behandling av personuppgifterna.

[8] Jfr. art 38 dataskyddsförordningen.

Verksamheten har med stöd av huvudkontaktombudet gått igenom och gallrat foton. Ärendet pågår.

- Granskning av upphandling av nytt lönesystem. I upphandlingen hade kravställts att informationen skulle lagras inom Europa. Det avgörande för otillåten tredjelandsöverföring är emellertid om leverantören faller under tredje lands lag, som möjliggör ett otillåtet utlämnande av information i strid med dataskyddslagstiftningen. Ärendet pågår.

8. Tillsyn

Tillsynsmyndigheten har inte under år 2021 genomfört någon tillsyn eller annonserat någon kommande tillsyn hos någon av kommunens verksamheter eller 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.[9]

Kommunstyrelsen har fått fyra (4) förfrågningar om registerutdrag under år 2021.

10. Administrativa sanktionsavgifter

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

Tillsynsmyndigheten har inte påfört någon administrativ sanktionsavgift på kommunen under år 2021.

11. Skadestånd

Varje person som lidit skada till följd av en överträdelse av dataskyddslagstiftningen ska ha rätt till ersättning (skadestånd). Varje personuppgiftsansvarig som medverkat till behandling i strid med dataskyddslagstiftningen ska ansvara för skadan. [12]

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

Kommunstyrelsen har inte fått in någon begäran om skadestånd för felaktig behandling av personuppgifter under år 2021.

12. Händelser under år 2021

- Dataskyddsombudet föredrog sin granskningsrapport gällande samtliga personuppgiftsansvarigas (nämnders) användning av samtycke som rättslig grund för ledningsgruppen. Separata rapporter för respektive personuppgiftsansvarig levererades till respektive förvaltningschef.
- I samverkan med kontaktombuden och informationssäkerhets-samordnaren inventerade dataskyddsombudet de arbetsprocesser och moment som idag existerar för det dagliga dataskyddsarbetet, bland annat processen för registerutdrag och upplägg för arbetsmöten. Processerna uppdaterades och arbetet effektiviserades ytterligare.
- Statistiken för personuppgiftsincidenter från kvartalsrapporterna år 2020 visade att mängden rapporteringar minskat med över 50 %. Dataskyddsombudet genomförde en utbildningskampanj för förvaltnings- och avdelningschefer på förvaltningarna gällande upptäckt, utredning och åtgärder vid personuppgiftsincidenter. Statistik från kvartalsrapporter år 2021 visade sedan att utbildningskampanjen givit resultat och antalet incidentrapporter ökade därefter. Emellertid rapporteras personuppgiftsincidenter fortfarande ofta efter 72 timmar från att de upptäcks, vilket är oförenligt med art 33 dataskyddsförordningen. Detta har varit ett av skälen till den pågående granskningen av personuppgiftsansvarigas hantering av personuppgifter och personuppgiftsincidenter.
- Under hösten 2021 utnämndes ett nytt dataskyddsombud. Det tidigare dataskyddsombudet har tagit rollen som huvudkontaktombud.
- Organisation för dataskyddsarbetet har uppdaterats, se avsnittet om organisation. Genom att dataskyddsombudet och huvudkontaktombudet uppdrag har renodlats, har det frigjort utrymme och dataskyddsarbetet blivit mer effektivt. Det har till exempel lett till att verksamheten i större utsträckning får operativt stöd på förvaltningsnivå, men också att antalet granskningar av dataskyddsombudet ökat. Personuppgiftsincidenterna har ökat.
- Dataskyddsorganisationen har tagit initiativ till nya rutiner vad gäller kommunens upphandlingar. Vid varje upphandling ska verksamheten svara på några frågor, för att på ett snabbt sätt kunna identifiera om upphandlingen medför några betänkligheter utifrån dataskyddslagstiftningen och i så fall förebygga dessa. Förvaltningens kontaktombud ska även bli informerade när det pågår en upphandling som rör behandling av personuppgifter.

13. Planering för år 2022

- Dataskyddsombudet planerar fortsatt granskning av kommunens användning av samtycke som rättslig grund. Detta kommer gälla de nämnder som haft påvisade brister i användningen av samtycke som rättslig grund år 2020, se vidare information i bilagan. Även tillsynsmyndigheten har utlovat att granskningar av myndigheters användning av samtycke som rättslig grund kommer att ske framöver.
- Huvudkontaktombudet kommer spela in och uppdatera utbildningsfilmerna på kommunens intranät om dataskydd.
- Kontaktombudens roll ska renodlas, bli mer operativ och framträdande på förvaltningarna. Kontaktombuden ska bli informerade om verksamheten upphandlar något som rör behandling av personuppgifter.
- Dataskyddsombudet har tagit initiativ till att dataskyddsorganisationen ska vara representerad i den planerade analysgruppen för kommunens fortsatta digitaliseringsarbete.