Datum
2023-01-17

Jakob Söderbaum, DSO
Diarienr VON 2023/77

Nuläget i vård- och omsorgsnämndens GDPR-efterlevnad

Inledning

Dataskyddsförordningen/GDPR[1] är en EU-lag som syftar till att skydda individens integritet och som trädde i kraft den 25 maj 2018. Syftet med GDPR är i korthet:

1) att reglera hur den mänskliga rättigheten till personlig integritet ska komma till uttryck i IT-samhället;
2) att placera makten över organisationers rätt att behandla personuppgifter i individens egna händer, och att ge individen ett antal specificerade rättigheter ifråga om sina personuppgifter;
3) att beivra all behandling av personuppgifter som inte uppfyller de ingående kraven enligt GDPR.

För att svara upp mot detta behöver alla organisationer i EU *för det första* bygga upp organisatoriska förutsättningar för att kunna tillgodose de registrerades rättigheter (däribland registerutdrag, radering och rättelse). *För det andra* bygga upp en grundläggande struktur för ansvarstagande bestående av dokumentation, organisatorisk respektive teknisk säkerhet och en dataskyddsorganisation som jobbar proaktivt med utveckling och reaktivt med incidenthantering. Denna grundläggande struktur behöver sedan vidareutvecklas över tid i riktning mot s.k. Privacy by design (kort sagt lätt att göra rätt och svårt att göra fel för medarbetarna), vi behöver känna till alla ”hål i rustningen” och ha ett pågående arbete för att fylla igen hålen. Det är i dessa hål, stora och små, som personuppgiftsincidenter kan inträffa och för det behöver vi ha en incidenthanteringsprocess för att anmäla inom 72 timmar, utreda vad som hänt, identifiera åtgärder, och besluta vilka åtgärder som ska genomföras och när.

Att inte kunna tillgodose de registrerades rättigheter, att inte ha de huvudsakliga delarna av den grundläggande strukturen för ansvarstagande på plats, eller att ha brister som kränker integriteten för eller utgör säkerhetshot mot registrerade individers personuppgifter, kan medföra sanktionsavgifter från Integritetsskyddsmyndigheten (IMY) på upp till 10 msek per brott. De viktigaste punkterna för att personuppgiftsansvariga i offentlig sektor ska undvika sanktionsavgifter, här med angivande av högsta sanktionsavgifter per specifikt GDPR-brott enligt Dataskyddslagen[2], är de följande:

- Uppfylla principerna i Artikel 5, lagligheten i Artikel 6 samt de särskilda kraven avseende känsliga personuppgifter i Artikel 9. (10 msek)

[1] General Data Protection Regulation
[2] Dataskyddslagen 6 kap 2 § 2 st.

- Ge information till registrerad om behandlingar samt i förekommande fall inhämta samtycke. (10 msek)
- Kunna tillhandahålla registerutdrag till den registrerade när denne begär detta. (10 msek)
- Ha ett inbyggt dataskydd samt säkerhet. (5 msek)
- Inhämta säkerhetsgarantier från personuppgiftsbiträden samt ge dem instruktioner. (5 msek)
- Föra ett register över behandlingar. (5 msek)
- Anmäla personuppgiftsincidenter till IMY. (5 msek)
- Genomföra konsekvensbedömningar. (10 msek)
- Ta hänsyn till dataskyddsombudets oberoende ställning. (5 msek)

Varje nämnd är, som det kallas i lagen, personuppgiftsansvariga och har därmed ett huvudansvar för GDPR-efterlevnaden både inom nämnden och dess förvaltning. Det åligger nämndens förvaltning att styra och leda arbetet för nämndens räkning, och att säkerställa att nämnden efterlever de lagar som gäller.

Vård- och omsorgsnämnden har i likhet med övriga nämnder utsett Jakob Söderbaum som dataskyddsombud, med uppdrag att kontrollera, granska, informera och ge motiverade rekommendationer angående efterlevnaden av dataskyddslagstiftningen inom förvaltningen å nämndens vägnar. Socialförvaltningen har ännu inte utsett någon dataskyddskoordinator av det slag som idag finns inom vissa andra förvaltningar (och som är normalt förekommande i kommuner av Huddinges storlek).

Under 2022 har dataskyddsombudet bl.a. genomfört följande aktiviteter av värde för alla nämnder:

- Kartlagt politikernas personuppgiftsbehandling
- Identifierat och utvärderat de huvudsakliga GDPR-relaterade riskerna i kommunen.
- Kvalitetssäkrat informationen om GDPR på Insidan.
- Kvalitetssäkrat informationen om GDPR på Huddinge.se.
- Direktupphandlat digital GDPR-utbildning.
- Medverkat till att definiera hur dataskyddsarbetet kommer in i PM3-modellen och stödobjektet för Säkerhet & lokaler.
- Medverkat i utredning av kommunens användande av och lämpliga förhållningssätt till amerikanska molntjänster.
- Genomfört utredning om möjligheter och konsekvenser ur GDPR-synvinkel inför att KS skulle bli ensam anställande myndighet i kommunen
- Stöttat arbetet med att utreda den ”stora incidenten” där toppen av isberget upptäcktes i mars, och där i princip all personals personuppgifter och väldigt många medborgares personuppgifter upptäcktes ligga helt öppet fördelat på flera olika digitala ytor. I december har den sista stora öppenheten stängts.

En årsrapport över allt dataskyddsombudets arbete under 2022 finns också, och har diarienummer KS-2022/3472.

Utvecklingsarbete inom nämndens ansvarsområde

Utvecklingsarbete under 2022 som fortsätter under 2023 handlar i huvudsak om följande:

- Verksamhetsarkitekt och verksamhetsutvecklare har i samarbete med dataskyddsombudet definierat detaljerna för hur ett gångbart behandlingsregister inom ramen för socialförvaltningens processregister i 2c8 bör se ut. Frågan om hur fort detta arbete kan tas i mål beror nu på utvecklingsledarna och processägarna inom SOF.

- Dataskyddsombudet har ett pågående projekt tillsammans med alla objektledare för att ta fram en fungerande GDPR-registerutdragsprocess för alla förvaltningar. Denna förväntas vara klar under Q1.

- Vård- och omsorgsnämndens nya ärendehanteringsprocess för personuppgiftsincidenter är i det huvudsakliga färdig. Ett systemstöd (Artvise) som förenklar delar av processen finns betalt och redo att börja användas inom alla förvaltningar, men socialförvaltningen har beslutat avvakta med implementeringen av denna. Det återstår också för medarbetare inom socialförvaltningen att kunna hantera alla sina personuppgiftsincidenter huvudsakligen självständigt så att medarbetarna bara behöver ta stöd av dataskyddsombudet i knäckfrågor och svårare bedömningar.

- Kommunstyrelseförvaltningen tecknar i januari 2023 avtal (med Visma Draftit) för en digital GDPR-utbildning för hela kommunen. Dataskydds-ombudet kommer i samråd med Biträdande förvaltningsdirektören och Enhetschefen för stöd och utveckling att planera genomförandet av denna utbildning för vård- och omsorgsnämndens medarbetare så att alla förhoppningsvis har genomgått den före semestern 2023.

- Verksamhetscontroller och upphandlare genomför för närvarande en inventering av PUB-avtal. Därefter kan dataskyddsombudet göra revision på alla befintliga avtal och etablera dem som eventuellt saknas idag inom vård- och omsorgsnämndens verksamhetsområden.

- Dataskyddsombudet håller på att revidera samtliga befintliga HKF:er och riktlinjer rörande dataskydd, och även ta fram ett flertal nya riktlinjer rörande dataskydd. Flertalet av dessa berör alla förvaltningar.

De viktigaste aktiviteterna för att bygga bort de mer betydande av bristerna i vård- och omsorgsnämndens integritets- och dataskydd beskrivs i följande färgsatta schema. Färgerna visar nulägesstatus:

- Grått = ej påbörjad aktivitet
- Gult = påbörjad aktivitet
- Ljusgrönt = nästan fullbordad aktivitet
- Grönt = genomförd aktivitet

Rubrikerna i vänsterkolumnen i *Bild 5* motsvarar rubrikerna i hexagonerna i *Bild 1* och flera i *Bild 2*. För att leva upp till lagens krav bedömer dataskyddsombudet det

som lämpligt att vård- och omsorgsnämndens förvaltningspersonal prioriterar dessa aktiviteter under den närmast överskådliga tiden – och helst ha dem klara senast vid slutet av 2023.

BILD 5: Nulägesbild av vård- och omsorgsnämndens GDPR-utvecklingsarbete

Område		Aktivitet
Alla system är kartlagda		Inventering av alla leverantörer av system och tjänster inom förvaltningen, vilka det har gjorts SSA på, och om förvaltningen har alla PUB-avtal man behöver
Dataskyddsansvarig(a) finns		Formellt utsedd(a) GDPR-ansvarig(a) i förvaltningen
Utbildning specifika roller		GDPR-ansvarig(a) har relevant GDPR-kunskap och verktyg
Dataskyddsansvarig(a) finns		Incidenthanteringsorganisation etablerad i den egna förvaltningen
Huvudprocesser finns		Incidenthanteringsprocess etablerad i förvaltningens incidenthanteringsorganisation
Personuppgiftsflödet är kartlagt		Huvudsaklig kartläggning av hur personuppgifter kommer in och behandlas inom förvaltningen har gjorts
Grunddokument är kvalitetssäkrade		Kvalitetssäkrat behandlingsregister för nämnden
Grunddokument finns		Val av leverantör för systemstöd till behandlingsregister
Huvudprocesser finns		Val av leverantör för systemstöd till incidenthantering
Generell utbildning		Val av leverantör för GDPR-utbildning
Huvudprocesser finns		Registerutdragsprocess etablerad i förvaltningen
Huvudprocesser finns		Processer för radering och rättelse etablerade i förvaltningen
Generell utbildning		Huvudsaklig GDPR-utbildning för kommuner genomförd för alla förvaltningens medarbetare
Grunddokument finns		Gap-analys ifråga om vad som finns och vad som ska finnas med i förvaltningens GDPR-rutiner, -regler och -anvisningar
Grunddokument finns		Dokumenterade rutiner, regler och anvisningar rörande det huvudsakliga ifråga om hur förvaltningens olika verksamheter får/bör behandla personuppgifter har upprättats
Utbildning specifika roller		Verksamhetsspecifik GDPR-utbildning genomförd för flertalet av förvaltningens medarbetare
Gallring + gallringsrutin		En huvudsaklig, systematisk GDPR-inriktad gallring har ägt rum i förvaltningen inför eller efter 25 maj 2018
Grunddokument finns		Alla PUB-avtal som förvaltningen behöver ha är på plats
Grunddokument är kvalitetssäkrade		Alla mallar och instruktioner för Samtycke som förvaltningen använder är kvalitetssäkrade
Relevant behörighetsstyrning		Inventering av alla behörigheter och licenser i alla system samt specificerande av vad som behöver förbättras
Relevant behörighetsstyrning		Felaktiga behörigheter har gallrats och GDPR-säkrade rutiner för behörighetsstyrning är dokumenterade och etablerade
Grunddokument är kvalitetssäkrade		Alla personuppgiftsbiträdesavtal som förvaltningen behöver ha är kvalitetssäkrade
Gallring + gallringsrutin		Relevanta rutiner för gallring finns beskrivna i förvaltningens informationshanteringsplan och efterlevs
Grunddokument är kvalitetssäkrade		GDPR-relaterade rutiner, regler och anvisningar har kvalitetssäkrats
All personuppgiftsbehandling är dokumenterad		Alla processer och rutiner där personuppgifter behandlas inom förvaltningen har GDPR-anpassats
Medarbetarna förstår		Enkät har genomförts bland medarbetarna som visar på tillräckligt god förståelse för GDPR

Incidenthantering inom nämndens ansvarsområde

De brister som en organisation har i sitt integritets- och dataskydd kan ge upphov till så kallade personuppgiftsincidenter, vilket betyder kränkningar av registrerade personers integritet som utgör brott enligt dataskyddslagstiftningen.

Den personuppgiftsansvarige har 72 timmar på sig att anmäla en personuppgifts-incident från det klockslag då en anställd inom kommunen fick kännedom om incidenten. Integritetsskyddsmyndigheten (IMY) kan utfärda böter på upp till 10 miljoner kr för personuppgiftsincidenter, beroende på typ av brott, dess omfattning och allvarlighetsgrad.

Under 2022 har dataskyddsombudet hanterat följande volym av personuppgifts-incidenter hos vård- och omsorgsnämnden:

Ansvarig nämnd	Upptäckta sedan förra rapporten	Upptäckta totalt 2022	IMY-anmälda sedan förra rapporten	IMY-anmälda totalt 2022
VON	2	3	2	3

Totalt i kommunen:	***18***	***43***	***13***	***38***

När den nyligen direktupphandlade digitala GDPR-utbildningen för alla kommunens anställda har genomförts inom socialförvaltningen, är det dataskyddsombudets förväntan att antalet upptäckta personuppgiftsincidenter kommer att öka inom förvaltningen. Det behöver då finnas personal med rätt kunskap och med tillräckligt med tid för att fånga upp och anmäla alla misstänkta personuppgiftsincidenter till Integritetsskyddsmyndigheten inom 72 timmar och i enlighet med kommunens ärendehanteringsprocess för personuppgiftsincidenter. Socialförvaltningen har för 2023 utsett sin Objektledare att samordna detta arbete.

Registrerades utövande av sina rättigheter

Följande antal begäranden har diarieförts hittills under 2022:

Nämnd	**Begäran om Registerutdrag**	**Begäran om Radering**	**Begäran om Rättelse**
VON	14	0	14
Totalt i kommunen:	***59***	***1***	***15***

Dataskyddsombudets rekommendationer för 2023

Dataskyddsombudets första rekommendation, som Säkerhetschefen instämmer i, är att det under 2023 ska finnas två dataskyddskoordinatorer per förvaltning, och så lär dataskyddsombudet dem det grundläggande. Det är också lämpligt att dessa medarbetare får en viss procent av en heltidstjänst angiven för det GDPR-relaterade arbetet (många jämförliga kommuner har flera heltidsanställda i denna roll). Ett förslag från Framtidsdirektören har varit att lägga utvecklingsarbetet på Objektledarna, vilket dataskyddsombudet tycker är en utmärkt idé.

Fr.o.m våren 2023 skulle varje förvaltning behöva jobba med att stänga personuppgiftsincident-ärenden (för socialförvaltningens del är det totalt 20 öppna ärenden sedan 2021). För att kunna göra detta behöver det utses en person (eller flera) i varje förvaltning som driver och samordnar ärendehanteringen, och så stöttar dataskyddsombudet den personen i hur detta ska göras. Detta förslag stöds av Säkerhetschefen. Socialförvaltningen har för 2023 utsett Mattias Ragnbäck att hantera detta.

Fr.o.m. Q2 2023 (efter att ett pågående projekt för att ta fram en fungerande process för detta väntas rulla i mål under Q1) behöver varje förvaltning kunna genomföra GDPR-registerutdrag. Ifråga om dessa bör en utsedd huvudansvarig inom respektive förvaltning samordna vad objektledarna ska leta upp i sina system baserat på de förfrågningar som inkommit. Dataskyddsombudet rekommenderar att denna samordningsuppgift ingår i förvaltningarnas dataskyddskoordinatorers arbetsuppgifter.