Datum
2023-02-17

Jakob Söderbaum, DSO
Diarienr KFN-2023/50

Nuläget i kultur- och fritidsnämndens 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.
4) 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 säkerhet och teknisk säkerhet, samt en dataskyddsorganisation som jobbar både proaktivt och reaktivt. Denna grundläggande struktur behöver sedan vidareutvecklas och förstärkas över tid, och varje förvaltning behöver känna till alla sina ”hål i rustningen” och ha ett pågående arbete för att fylla igen hålen. Det är i dessa hål, stora och små, som s.k. personuppgiftsincidenter kan inträffa och för det behöver förvaltningen ha en incidenthanteringsprocess för att anmäla inom 72 timmar, utreda vad som hänt, identifiera åtgärder, och besluta vilka åtgärder som ska genomföras och när. Dataskyddsrisker är enligt lagstiftaren viktigare än många andra risker i en myndighet. Därför finns *för det tredje* en särskild roll – dataskyddsombudet – för att hjälpa den personuppgiftsansvarige att ta kontroll över dessa risker. Denna roll är obligatorisk för alla myndigheter att ha, och lagstiftaren har även gett den specificerade arbetsuppgifter och en oberoende ställning.[2]
5) Att myndigheter kan tillgodose de registrerades rättigheter, har de huvudsakliga delarna av den grundläggande strukturen för ansvarstagande på plats, kan visa att de har tagit kontroll över risker och har förmåga att bemöta säkerhetshot mot registrerade individers personuppgifter, har av lagstiftaren ansetts viktigt. Av det skälet anges direkt i Dataskyddslagen

[1] General Data Protection Regulation
[2] Dataskyddsombudets roll, ställning och arbetsuppgifter framgår av GDPR artiklar 38 och 39.

vissa GDPR-brott som var för sig kan rendera sanktionsavgifter från Integritetsskyddsmyndigheten (IMY) på upp till 5 mkr respektive 10 mkr för myndigheter.[3]

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

Kultur- och fritidsnämnden 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. Kultur- och fritidsförvaltningen har för närvarande en dataskyddskoordinator.

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 http://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 kommunstyrelsen 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.

Nämndens förra årsrapport har diarienummer KFN 2022/23.

Utvecklingsarbete inom nämndens ansvarsområde

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

[3] Dataskyddslagen 6 kap 2 § 2 st.

- Dataskyddsombudet har ett pågående projekt tillsammans med alla objektledare[4] för att ta fram huvudsakliga behandlingsregister för alla förvaltningar. Inom kultur- och fritidsförvaltningen väntas det nya behandlingsregistret bli klart under Q1.

- 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.

- Kultur- och fritidsnämndens nya ärendehanteringsprocess för personuppgiftsincidenter är i det huvudsakliga färdig, och ett systemstöd (Artvise) som förenklar delar av processen håller på att testköras i samarbete mellan dataskyddsombudet, förvaltningens dataskyddskoordinator, och förvaltningens objektledare. Det återstår också för medarbetare inom Kultur- och fritidsförvaltningen att kunna hantera alla sina personuppgifts-incidenter huvudsakligen självständigt så att medarbetarna bara behöver ta stöd av dataskyddsombudet i knäckfrågor och svårare bedömningar.

- Kommunstyrelseförvaltningen har i januari 2023 tecknat avtal (med Visma Draftit) för en digital GDPR-utbildning för hela kommunen. Dataskyddsombudet kommer i samråd med kultur- och fritidsdirektören att planera genomförandet av denna utbildning för förvaltningens medarbetare så att alla förhoppningsvis har genomgått den före sommarsemestern 2023.

- Verksamhetscontroller och upphandlare genomför för närvarande en inventering av personuppgiftsbiträdesavtal[5]. Därefter kan dataskyddsombudet göra revision på alla befintliga avtal och etablera dem som eventuellt saknas idag inom kultur- och fritidsnämndens verksamhetsområden.

- Dataskyddsombudet håller på att revidera samtliga befintliga HKF:er och riktlinjer[6] 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 kultur- och fritidsnämndens integritets- och dataskydd beskrivs i nulägesbilden nedan. Färgerna visar nulägesstatus:

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

[4] Objektledare är en roll i Huddinge kommuns styr och samverkansmodell för digitalisering som baseras på PM3-modellen. Rollen innehas av utsedda tjänstemän med kunskap om IT-system och den verksamhet som objektet stödjer. Officiell rollbeskrivning finns här: https://insidan.huddinge.se/download/18.7e2b0b5917a0f70aec78ca1/1625034841889/PM3_MODELLBESKRIVNING_2021%20(1).pdf

[5] De avtal som nämnden i egenskap ofta behöver ha med leverantörer för att säkerställa att nämnden tar sitt ansvar när leverantören (personuppgiftsbiträdet) behandlar personuppgifter som nämnden (den personuppgiftsansvarige) ansvarar för.

[6] Dessa är kommunens fastställda styrdokument. HKF = Huddinge Kommuns Författningssamling.

BILD 1: Nulägesbild av kultur- och fritidsnämndens 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.

Under 2022 har dataskyddsombudet hanterat följande volym av personuppgifts-incidenter hos kultur- och fritidsnämnden:

Ansvarig nämnd	Upptäckta sedan förra rapporten	Upptäckta totalt 2022	IMY-anmälda sedan förra rapporten	IMY-anmälda totalt 2022
KFN	1	2	1	1
Totalt i kommunen:	***18***	***43***	***13***	***38***

När den nyligen direktupphandlade digitala GDPR-utbildningen för alla kommunens anställda har genomförts inom kultur- och fritidsförvaltningen, 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.

Registrerades utövande av sina rättigheter

Följande antal begäranden har inkommit hittills under 2022:

Nämnd	**Begäran om Registerutdrag**	**Begäran om Radering**	**Begäran om Rättelse**
KFN	0	0	0
Totalt i kommunen:	***99***	***1***	***15***

Dataskyddsombudets rekommendationer för 2023

Fr.o.m våren 2023 behöver varje förvaltning jobba med att stänga personuppgiftsincident-ärenden (för kultur- och fritidsnämndens del är det totalt bara ett sådant ärende öppet). 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. Dataskyddsombudet har sedan tidigare tagit fram en kvalitetssäkrad och fungerande process för kommunens personuppgiftsincidenthantering. Dataskyddsombudet rekommenderar att förvaltningens dataskyddskoordinator(er) får hantera denna arbetsuppgift, och får särskild tid avsatt av sin(a) chef(er) för detta arbete.

Fr.o.m. Q2 (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 minst en utsedd huvudansvarig inom respektive förvaltning samordna vad objektledarna ska leta upp i sina system baserat på de registerutdragsförfrågningar som inkommit. Dataskyddsombudet rekommenderar att denna samordningsuppgift ingår i dataskyddskoordinatorernas arbetsuppgifter.