Datum
2022-01-25

Jakob Söderbaum, DSO
Diarienr KFN 2022/23

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. Den ställer krav på förändringar av merparten av befintliga processer, rutiner och riktlinjer för vardagsarbetet i alla organisationer som har verksamhet i EU.

Innehållet i GDPR var känt sedan 2016, i syfte att ge alla organisationer rimliga förutsättningar för att bygga upp en viss skyddsnivå, identifiera vad som saknas för att leva upp till de nya lagkraven, samt ta fram och börja följa en dokumenterad plan för hur bristerna steg för steg ska byggas bort. Inför att lagen skulle träda i kraft anlitade kommunen ett informations- och cybersäkerhetsföretag vilka bl.a. höll utbildning för medarbetare och genomförde workshops i mindre grupper. En förvaltningsövergripande GDPR-arbetsgrupp tillsattes som samordnade arbetet i kommunen.

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.

Kultur- och fritidsnämnden har utsett Jakob Söderbaum till sitt dataskyddsombud från och med den 22/2 2021. Jakob innehar uppdraget på 100% av en heltid, medan uppdraget dessförinnan innehades av medarbetare på 20-25% av en heltid och med andra huvudansvar. Dataskyddsombudet rapporterar enligt lagen (GDPR artikel 38.3) till högsta förvaltningsledningen.

Dataskyddsombudet har nu genomfört en granskning av nuläget avseende efterlevnaden av dataskyddslagstiftningen (där GDPR är den centrala lagen) inom samtliga av kommunens nämnder och förvaltningar, samt identifierat hur det viktigaste som saknas idag ska kunna byggas upp, och vad som är viktigast att få på plats först.

Dataskyddsombudet ser det som lämpligt att ha en Årsrapport som den här för var och en nämnd. Därutöver en aggregerad Delårsrapport till kommunstyrelsen, samt separata Delårsrapporter till var och en förvaltningsledning. I dessa rapporter kommer nulägesstatus beskrivas översiktligt, viss löpande statistik presenteras, huvudsakliga utvecklingsaktiviteter som genomförts att listas, och prioriterade utvecklingsområden att lyftas fram.

[1] General Data Protection Regulation

Nuläget i huvudsak

I dagsläget har kultur- och fritidsnämnden endast i begränsad utsträckning påbörjat det arbete som skulle ha varit klart när lagen trädde i kraft.

I *Bild 1* har dataskyddsombudet visualiserat de huvudsakliga aktiviteter som en organisation behöver genomföra för att leva upp till dataskyddslagstiftningen i allt väsentligt, sammanfogade i den ordning de bör genomföras där vissa steg behöver vara på plats innan ett annat steg kan tas. Hur långt kommunen idag har kommit på vägen till full GDPR-efterlevnad, enligt dataskyddsombudets sammanvägda bedömning, visas med färgsättning:

- Grönt utgör en tillräckligt hög GDPR-efterlevnad.
- Gult markerar att det finns definierat vad som behövs och ett pågående arbete.
- Grått är aktiviteter som ännu inte har påbörjats någonstans inom kommunen.

I *Bild 2-4* visas utvecklingsarbetets tre etapper i läsbar storlek.

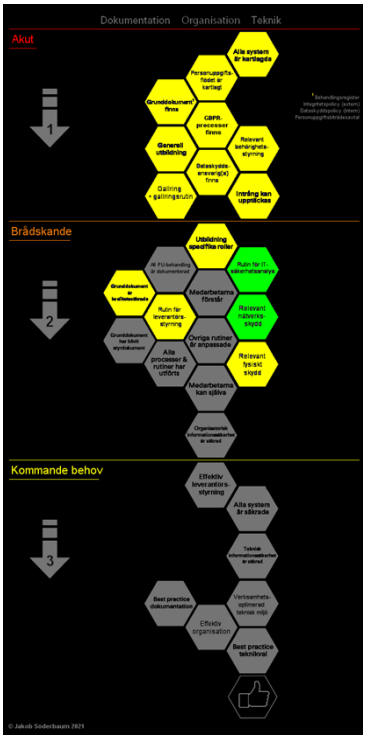

BILD 1: Vägen till full GDPR-efterlevnad, och hur långt kommunen hittills har kommit.

Den första etappen ”Akut” (*Bild 2*) är vad som skulle ha varit klart i alla nämnder och förvaltningar när lagen trädde i kraft. Här finns idag påbörjade aktiviteter inom alla områden, men ingenting håller en tillräcklig nivå och arbetet har bara påbörjats. Att göra klart detta utvecklingsarbete har högsta prioritet.

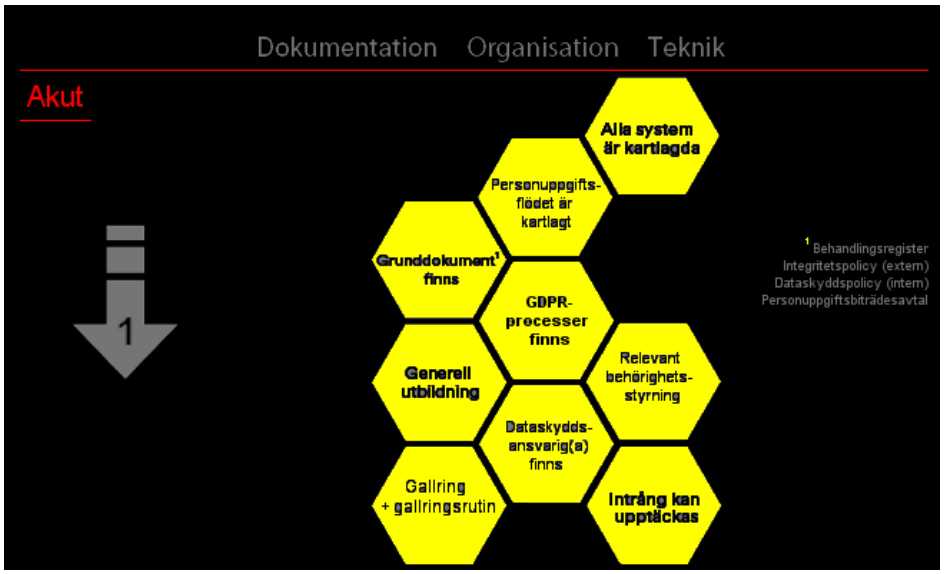

BILD 2: Det allra mest akuta för att bygga upp ett lagenligt dataskydd.

Den andra etappen ”Brådskande” (*Bild 3*) är vad som kan förväntas vara på plats i en organisation idag, när GDPR har gällt i 3,5 år. Kommunen har här vissa påbörjade aktiviteter, och två rubriker som håller en tillräcklig nivå.

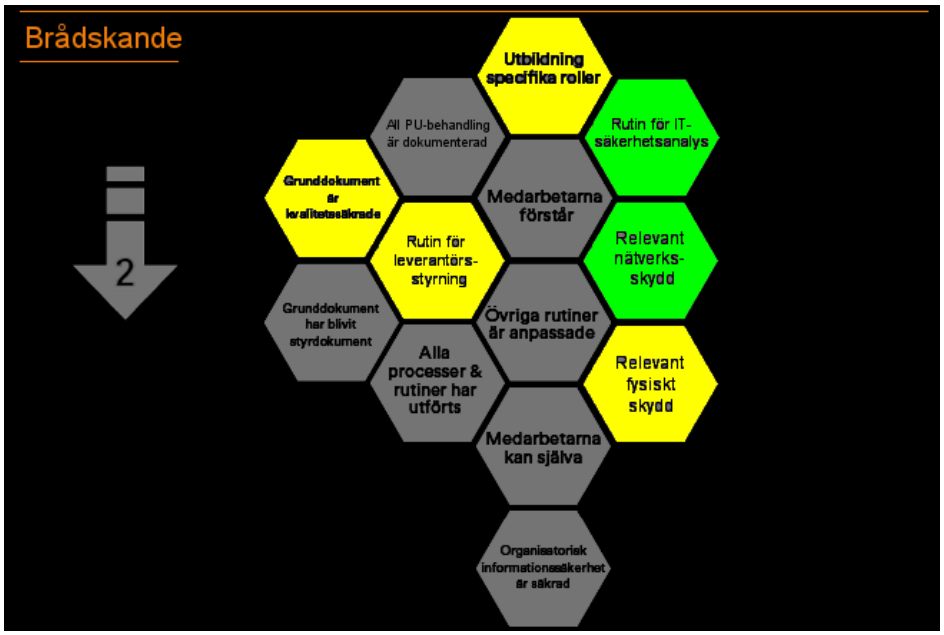

BILD 3: Det brådskande – vad som utöver det akuta i föregående bild förväntas vara klart idag givet det nuvarande rättsläget.

Den tredje etappen ”Kommande behov” (*Bild 4*) är aktiviteter som i framtiden behöver genomföras för att en organisation till slut – se symbolen ”tummen upp” längst ner i bilden – ska kunna anses uppfylla dataskyddslagstiftningen till 100 %.

För att leva upp till dataskyddslagstiftningens krav fullt ut måste alltså ett aktivt utvecklingsarbete pågå under flera år framöver i Huddinge kommun. Detta kräver resurser som idag inte har avsatts för dessa ändamål.

Utvecklingsarbete inom nämndens ansvarsområde

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

- Grönt = genomförd aktivitet
- Gult = påbörjad aktivitet
- Rött = ej påbörjad 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 kultur- och fritidsnämndens förvaltningspersonal prioriterar dessa aktiviteter under den närmast överskådliga tiden – och helst ha dem klara senast vid

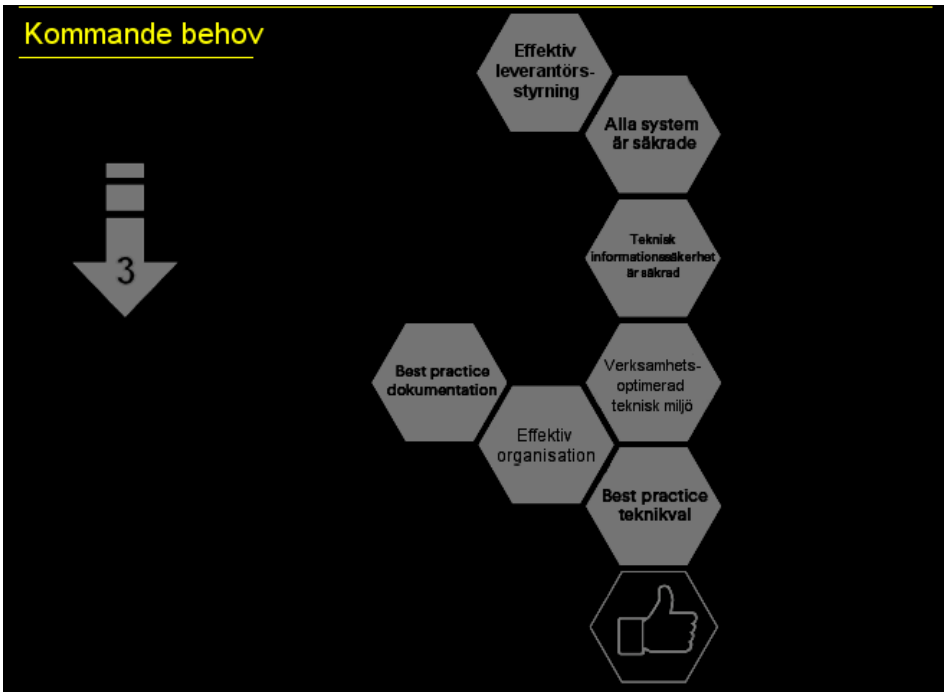

BILD 4: Kommande behov. För att efterleva dataskyddslagstiftningen fullt ut behöver även dessa aktiviteter fullföljas.

slutet av 2022.

BILD 5: Nulägesstatus i 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 GDPR-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-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.

Kultur- och fritidsnämnden uppvisar idag en mängd brister i relation till GDPR, varav många kan leda till böter vid granskning från IMY. Det är därför viktigt för det första att det finns en kunskap om GDPR hos alla medarbetare, vad som utgör en personuppgiftsincident, och om ansvaret när en sådan incident upptäcks. För det andra att förvaltningen har rutiner på plats för att kunna hantera de incidenter som upptäcks.

Inom kultur- och fritidsnämnden håller idag en dataskyddsorganisation på att implementeras och utbildas med stöd av dataskyddsombudet. Den består av en utredare och en IT-samordnare inom förvaltningens Stabs- och utvecklingsenhet. Till sitt stöd har dessa en process för personuppgiftsincidenthanteringen och en arbetsplan för utvecklingsarbetet som tagits fram av dataskyddsombudet. Det skulle dock behövas ytterligare resurser för att förvaltningen ska kunna ta fullt ansvar för både utvecklings- och incidenthanteringsarbetet.

Under 2021 har dataskyddsombudet hanterat följande volym av personuppgifts-incidenter hos kultur- och fritidsnämnden:

Ansvarig nämnd	**Upptäckta sedan förra rapporten**	**Upptäckta totalt 2021**	**IMY-anmälda sedan förra rapporten**	**IMY-anmälda totalt 2021**
KFN	0	0	0	0
Totalt i kommunen:	***27***	***27***	***25***	***25***

Inga personuppgiftsincidenter har upptäckts och anmälts inom kultur- och fritidsnämnden under 2021 – och det är även förvånansvärt få inom hela kommunen. Dataskyddsombudet bedömer att anledningen till att inga personuppgiftsincidenter har identifierats inom kultur- och fritidsnämnden, som är en i princip 100% digitaliserad förvaltning, är att kunskapen om GDPR idag är låg inom förvaltningsorganisationen. Många fler personuppgiftsincidenter skulle sannolikt upptäckas om all personal hade fått en kommunanpassad GDPR-utbildning. En sådan utbildning behöver direktupphandlas under 2022 (för hela kommunen), och i samband med det behöver det finnas någon inom förvaltningen som tar huvudansvar för incidenthanteringen. Denne bör också kunna ta ansvar för utvecklingsarbetet. Möjliga alternativ är att nyrekrytera, eventuellt till en roll med ansvar för flera nämnder och förvaltningar, eller att ta in en konsult. Allt detta talar för behov av en budgetjustering för 2023 och lämpligen även för 2022.