Datum
2022-01-25

Jakob Söderbaum, DSO

Nuläget i gymnasie- och arbetsmarknadsnämndens 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 bland annat 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.

Gymnasie- och arbetsmarknadsnämnden har utsett Jakob Söderbaum till sitt dataskyddsombud. Dataskyddsombudet rapporterar enligt lagen (GDPR artikel 38.3) till högsta förvaltningsledningen.

Nuläget i huvudsak

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

I bilderna nedan 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 nämnden idag har kommit på vägen till full GDPR-efterlevnad, enligt dataskyddsombudets sammanvägda bedömning, visas med färgsättning:

- Grönt utgör en tillräckligt hög GDPR-efterlevnad.

[1] General Data Protection Regulation

- Gult markerar att det finns definierat vad som behövs och ett pågående arbete.
- Grått är aktiviteter som ännu inte har påbörjats.

Den första etappen ”Akut” (*Bild 1*) 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 1: det allra mest akuta för att bygga upp ett lagenligt dataskydd.

Den andra etappen ”Brådskande” (*Bild 2*) 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.

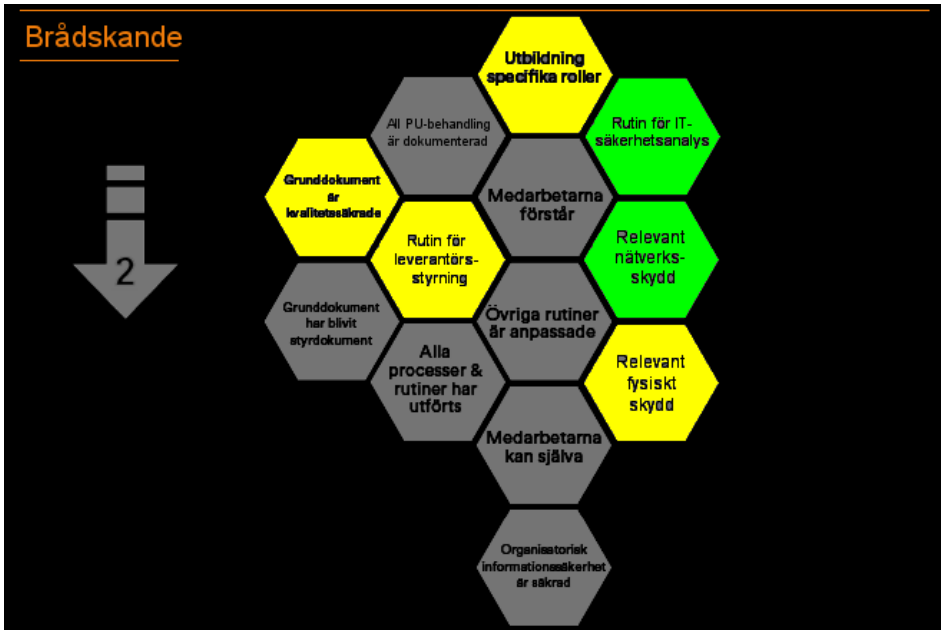

BILD 2: Det brådskande – vad som utöver det akuta i föregående bild förväntas vara klart idag givet det nuvarande rättsläget.

Den tredje etappen ”Kommande behov” (*Bild 3*) 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.

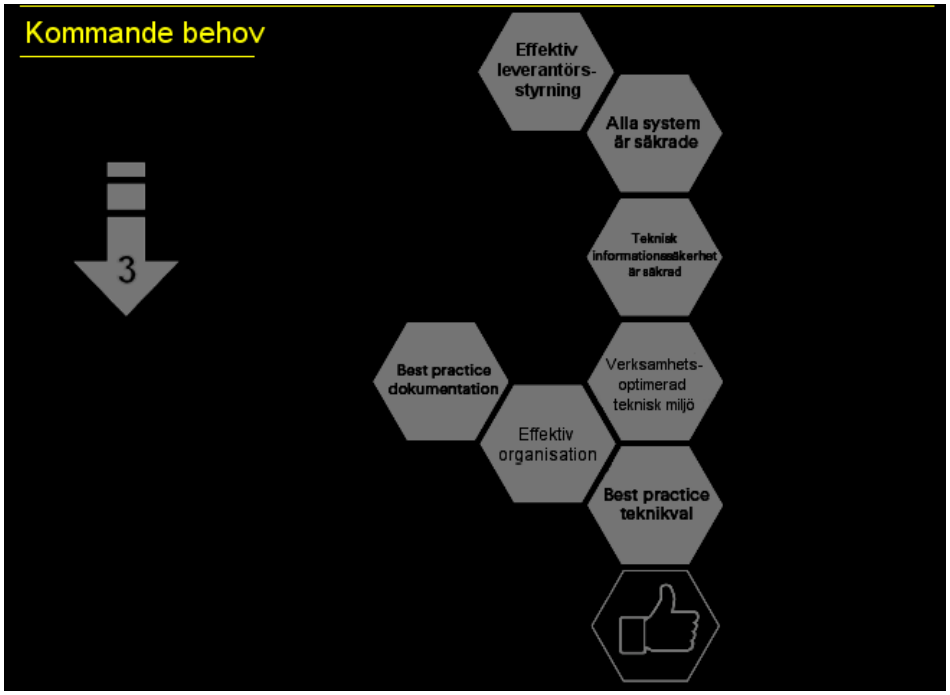

BILD 3: Kommande behov. För att efterleva dataskyddslagstiftningen fullt ut behöver även dessa aktiviteter fullföljas.

Utvecklingsarbete inom nämndens ansvarsområde

De viktigaste aktiviteterna för att bygga bort de mer betydande av bristerna i gymnasie- och arbetsmarknadsnämnden 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 4* motsvarar rubrikerna i hexagonerna i *Bild 2*. För att leva upp till lagens krav bedömer dataskyddsombudet det som lämpligt att gymnasie- och arbetsmarknadsnämnden förvaltningspersonal prioriterar dessa aktiviteter under den närmast överskådliga tiden – och helst ha dem klara senast vid slutet av 2022.

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 förvaltningen
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 interna Dataskyddspolicies
Grunddokument finns		Dokumenterade interna rutiner, regler och anvisningar rörande det huvudsakliga ifråga om hur nämndens 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 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 PUB-avtal som förvaltningen behöver ha är kvalitetssäkrade
Gallring + gallringsrutin		Relevanta rutiner för gallring finns beskrivna i förvaltningens informationshanteringsplan och efterlevs
Grunddokument är kvalitetssäkrade		Interna Dataskyddspolicies 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

Bild 4: nulägesbeskrivning av gymnasie- och arbetsmarknadsnämndens GDPR-utvecklingsarbete

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 kronor för personuppgiftsincidenter, beroende på typ av brott, dess omfattning och allvarlighetsgrad.

Gymnasie- och arbetsmarknadsnämnden uppvisar idag en mängd brister i relation till GDPR, varav många kan leda till böter vid granskning från IMY. Här sammanfattas de allvarligaste av dessa brister för gymnasie- och arbetsmarknadsnämndens del, som alltså var och en kan leda till höga böter:

- Ofullständigt register över personuppgiftsbehandlingar (artikel 30).
- Ofullständig uppfyllnad av dataskyddsförordningens artikel 5 (principer för behandling av personuppgifter), artikel 6 (att nämnden får och ska hantera uppgifterna) samt artikel 9 (särskilda krav avseende känsliga personuppgifter).
- Avsaknad av, eller ofullständig, information till registrerad om behandlingar (artikel 12) samt i förekommande fall inhämtning samtycke (artikel 7).
- Oklar förmåga att tillhandahålla registerutdrag (artikel 13-15).

- Bristande förmåga att upptäcka och hantera personuppgiftsincidenter (artikel 33-34).
- Bristande förmåga att inhämta säkerhetsgarantier från personuppgiftsbiträden samt ge dem instruktioner (artikel 28).
- Avsaknad av konsekvensbedömningar vid ny/ändrad behandling av personuppgifter.
- Bristande integritets- och dataskydd rörande molntjänster.

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 gymnasie- och arbetsmarknadsnämnden håller idag en dataskyddsorganisation på att implementeras och utbildas med stöd av dataskyddsombudet. Denna består av en dataskyddskoordinator på 50% av en heltid tillsammans med systemförvaltarna och vissa nyckelpersoner inom verksamheten. Till sitt stöd har dessa en process för personuppgiftsincidenthanteringen och en arbetsplan för utvecklingsarbetet som tagits fram av dataskyddsombudet.

Under 2021 har dataskyddsombudet hanterat följande volym av personuppgiftsincidenter hos gymnasie- och arbetsmarknadsnämnden:

Ansvarig nämnd	**Upptäckta sedan förra rapporten**	**Upptäckta totalt 2021**	**IMY-anmälda sedan förra rapporten**	**IMY-anmälda totalt 2021**
GAN	3	3	3	3
Totalt i kommunen:	***27***	***27***	***25***	***25***

Det är relativt få personuppgiftsincidenter som har upptäckts och anmälts inom gymnasie- och Arbetsmarknadsnämnden under 2021 – och även inom hela kommunen. Dataskyddsombudet bedömer att anledningen till att få personuppgiftsincidenter har identifierats inom gymnasie- och Arbetsmarknadsnämnden är att kunskapen om GDPR idag är låg inom förvaltningsorganisationen. Tydliga insatser för att öka kunskapen och efterlevnaden bör därför prioriteras under 2022 och 2023.