

Indledning

Denne rapport er udarbejdet med henblik på at informere FGU institutionernes ledelser om status på implementering og overholdelse af databeskyttelsesreglerne - som fastlagt i EU-Databeskyttelsesforordningen (i det efterfølgende benævnt som GDPR) (EU 2016/679) samt i de danske vedtagne bestemmelser om samme (Databeskyttelsesloven nr. 502 af 23/05/2018).

Baggrunden

FGU-sektoren blev formelt etableret i august 2019, hvorefter denne nye selvejende organisation skulle finde sine ben at stå på. De enkelte institutioner havde forskellige udgangspunkter i forhold til GDPR, hvor nogle havde arbejdet med det i andre sammenhænge, og andre havde ikke de store erfaringer med arbejdet. Erfaringerne fra det tidligere arbejde blev benyttet som afsæt for arbejdet med GDPR i det nye FGU-regi, hvor det var relevant.

FGU Danmark indgik i foråret 2020 aftale med revisionsfirmaet BDO om rådgivning og assistance i forbindelse med implementering af de i EU-persondataforordningen anførte krav til persondatabeskyttelse på de 27 FGU-institutioner.

FGU Danmark fik i juli 2020 tildelt et ekstra driftslignende tilskud fra Børne- og Undervisningsministeriet, som bl.a. dækker udgifterne forbundet med aftalen med BDO.

Arbejdet blev igangsat med, at der blev udpeget en kontaktperson for hver FGU-skole til projektet, der indledningsvist deltog i et seminar. Herefter blev der nedsat en tværgående projektgruppe bestående af seks medarbejdere fra FGU-institutionerne, som har samarbejdet med BDO om at udarbejde generiske dokumenter til alle institutionerne, der efterfølgende tilretter disse til lokale forhold efter behov.

Materialet omfatter:

- fortegnelser over behandlingsaktiviteter
- risikovurderinger på de programmer institutionerne anvender
- politikker
- procedurebeskrivelser.

Aftalen med BDO afsluttedes med virtuelle møder med hver enkelt FGU-institution ultimo 2020/primo 2021, hvor de udarbejdede materialer præsenteredes.

For at sikre en stærk forankring af GDPR-implementeringen hos alle medarbejdere, blev det i efteråret 2020 besluttet at indgå samarbejde med firmaet Moch om gennemførelse af en virtuel uddannelse inden for GDPR og cybersikkerhed.

I tillæg til aftalen med BDO blev det ligeledes besluttet i ultimo 2020, at man, inden for rammeaftalen med BDO, ville gennemføre en Phishingkampagne rettet mod alle medarbejdere i på de 27 FGU-institutioner. Denne kampagne vil blive afviklet med flere udsendelsesbølger hen over sommeren og efteråret i 2021, som skal bidrage til at sikre medarbejdernes opmærksomhed på egen indsats i forhold til at sikre institutionen imod sikkerhedsbrud.

GDPR-implementeringsprojektet

Starten på implementeringsprojektet var en række korte workshops med deltagelse fra næsten alle institutioner.

Det blev på disse workshops hurtigt klart, at institutionerne arbejder meget homogent i forhold til det daglige arbejde med persondatabehandling samt i forhold til brug af systemer, selv om der er små variationer fra institution til institution.

GDPR-kravene er de samme til hver enkelt institution uanset valg af systemer som f.eks. office-platform, hvor nogle benytter Google og andre Microsoft samt andre værktøjer som f.eks. de studieadministrative systemer Uddata+ eller FGU-planer, og derfor kunne det konstateres, at hvis opgaven skulle løses inden for den forventede tidsramme, så måtte arbejdet organiseres anderledes end ét lokalt GDPR-implementeringsprojekt pr institution.

Efter en kort dialog mellem BDO, sekretariatet i FGU Danmark og styregruppen bestående af institutionsudvalget, blev det besluttet at følge BDO's anbefalinger og organisere det kommende arbejde omkring en central projektgruppe, med repræsentanter fra institutioner på tværs af landet.

Deltagerne til projektgruppen blev udvalgt på baggrund af deres kvalifikationer, samt lysten til at deltage i det videre arbejde.

Med dette udgangspunkt blev der sammensat en særdeles effektiv og velfungerende projektgruppe bestående af følgende:

- Maria Moeslund Madsen fra FGU Nordvest
- Stine Johanne Kierkegaard fra FGU HLSS
- Inge Rasmussen fra FGU Hovedstaden
- Klaus Gunnar Jensen fra FGU Hovedstaden
- Kent Rose fra FGU Midt- og Østsjælland
- Dennis Kristian Gravgaard fra FGU Sydøstjylland
- Ivan Sommer fra BDO Revisionselskab

Med baggrund i rollen som facilitator og projektleder på opgaven har BDO's repræsentant Senior Manager Ivan Sommer udtalt: *Jeg vil gerne give stor ros til projektgruppen for både engagement og kvalitet i det arbejde der blev lavet. Det har været i sandhed været i særklasse.*

Resultatet af projektgruppens arbejde består af et generisk sæt masterdokumenter, der er den nødvendige dokumentation for, hvordan den enkelte institution overholder kravene fra databeskyttelsesforordningen. Hver enkelt institution skal blot lave nogle få lokale tilretninger for, at dokumentet kan omsættesbliver retvisende i forhold til dagligdagen i den enkelte institution.

Selv om Corona-pandemien forsøgte at lægge hindringer i vejen, blev arbejdet alligevel udført og klart til forventet tid, således at resultatet kunne præsenteres for de enkelte institutioner på virtuelle Teamsmøder.

I forbindelse med præsentationen af masterdokumenterne fik institutionerne instruktion om, hvordan materialet forventes at blive anvendt samt hvor og hvordan, det bør gemmes.

Samlingen af masterdokumenter består af:

- Fortegnelser over behandlingsaktiviteter i forbindelse med elever

- Fortegnelser over behandlingsaktiviteter i forbindelse med medarbejdere
- Risikovurderinger af de anvendte systemer. I de tilfælde, hvor flere systemer dækker de samme behandlingsaktiviteter, er der lavet en fælles risikovurdering og institutionen skal blot slette det ikke relevante.
- Procedurebeskrivelse til dokumentation af, hvordan medarbejderne udfører de daglige arbejdsprocesser i forbindelse med persondatabehandlingerne.
- Politikker for hhv. databeskyttelse og underretning om indsamling af data, samt it-politik, mailpolitik, privatlivspolitik samt slettepolitik.

Awareness kursus

Som led i forankringen af implementeringsarbejdet skal alle medarbejdere uddannes inden for GDPR og Cybersikkerhed for herigennem at understøtte de organisatoriske sikkerhedsforanstaltninger, der er et krav fra forordningen.

Projektgruppen har sammen med sekretariatet vurderet forskellige udbydere af løsninger til denne opgave og valget faldt på Moch, der i en kombination af pris, produkt og fleksibilitet var klart bedre end de øvrige virksomheder, hvorfor der blev indgået en 3-årig aftale med dem.

Det har desværre vist sig, at det faktuelle indhold i kurserne ikke helt har levet op til, hvad der blev lovet fra Moch. Et enkelt kursus omkring god forvaltningsskik viste sig at ligge så langt fra det lovede produkt, at det kun 48 timer efter lanceringen blev det taget ud af drift og medarbejdernes adgang deaktiveret. Der arbejdes pt på at finde en ny løsning til erstatning herfor, idet emnet er vurderet til at være vigtigt for alle medarbejdere i FGU-sektoren.

Yderligere har der beklageligvis været en række uforudsete hændelser og uregelmæssigheder i kurset, der har skabt forvirring og frustrationer hos medarbejderne. Der arbejdes intenst med leverandøren for at sikre, at de fremadrettet lever op til det lovede produkt.

Endelig skal der lyde et stort tillykke til alle medarbejdere hos FGU Sydvestsjælland der er 100 pct. i mål på uddannelsen inden for både Cyber og GDPR sporet, skarpt forfulgt af FGU Nordvest og FGU HLSS. Det flotte resultat i FGU Sydvestsjælland er præmieret med kage til personalet.

Resten af FGU-institutionerne ligger i gennemsnit med en gruppe på mellem 30 pct´. – 60 pct. af medarbejderskaren, der på nuværende tidspunkt endnu ikke er gået i gang med uddannelsen.

Den fælles DPO

FGU Danmarks Direktør- og Rektorkollegium besluttede på et seminar den 3.-4. september 2020 at gå sammen om en fælles DPO-funktion. Det blev besluttet, at FGU Danmarks sekretariat varetog opgaven frem til årsskiftet 2020/2021 med assistance fra BDO, hvorefter der skulle ansættes en fælles DPO tilknyttet sekretariatet.

26 af de 27 FGU-institutioner er gået sammen om det fælles GDPR-arbejde, herunder en DPO, som er ansat pr. 1. juni 2021 for en 3-årig periode. Udgifterne forbundet hermed dækkes af de enkelte FGU-institutioner og en del af sekretariatet. DPO'en vil også skulle varetage få andre opgaver end DPO-opgaven.

Den fælles DPO's funktion er at understøtte, rådgive, vejlede og overvåge, at den dataansvarlige (FGU-institutionen) overholder reglerne i databeskyttelsesforordningen, samt er denne kontaktled til - og skal samarbejde med - Datatilsynet.

DPO'ens arbejde indebærer bl.a. følgende opgaver:

- Underrette og rådgive organisationen og de ansatte om databeskyttelse
 - o Konkret rådgivning om beskyttelse af personoplysninger i organisationen samt overvejelser og beslutninger om, hvordan compliance sikres ifm.
 - Organisationens indkøb af nyt it-system
 - Kravspecifikationer til leverandører
 - Udarbejdelse af organisationens data-politikker
 - Iværksættelse af behandling af personoplysninger
 - Overvejelser om, hvorvidt en given behandling af personoplysninger overholder de generelle behandlingsregler
 - o Stå til rådighed for ansatte samt ledelsen i organisationen vedrørende spørgsmål om databeskyttelse
 - o Rådgivning ifm. udarbejdelse af organisationens konsekvensanalyser
 - o Modtage underretning om og rådgive organisationen ifm. Brud på persondatasikkerheden
- Overvåge overholdelsen af de databeskyttelsesretlige regler i organisationen
 - o Overvåge organisationens politikker og databeskyttelse, uddannelse af personale i databeskyttelse, oplysningskampagner, fordeling af ansvar og revisioner
- Rådgivning ifm. udarbejdelse af organisationens konsekvensanalyser
- Samarbejde med Datatilsynet på vegne af organisationen
- Være kontaktpunkt for Datatilsynet angående spørgsmål om behandling af personoplysninger for de personer, der behandles oplysninger om

Plan for 2021

Den kommende periode i resten af 2021 vil der være følgende fokusområder for DPO'en, hvor planen i udgangspunktet ser således ud:

- o DPO'en kommer snarest rundt til alle institutioner og vil sammen med ledelsen og den lokale GDPR-ansvarlige at gennemgå status for implementeringen af det generiske mastermateriale og samtidig få identificeret ønsker til den videre uddannelse af de lokale GDPR-ansvarlige, samt indsamle information om, hvad der især ønskes støtte til.
I samme forbindelse indsamles indgåede databehandlertaftaler, for efterfølgende at kunne iværksætte udførelse af tilsynsopgaven på institutionernes vegne.
- o Etablering af et vidensbibliotek omkring GDPR-forhold, der skal være tilgængelig for alle de institutioner, der er med i samarbejdet om den fælles DPO-funktion.
Opbygningen er endnu ikke endelig, hvorfor der indtil videre vil være mulighed for at sende ønsker og forslag til indhold og struktur til iso@fgu.dk
I udgangspunktet overvejes følgende struktur:
 - o Spørgsmål/svar omkring GDPR fra organisationen (*Spørgehjørnet*)
 - o Pixiebog, der på let tilgængelig vis forklarer forordningen, samt vejledninger
 - o Databehandlertaftaler og resultaterne af tilsyn med samme
 - o Logbog over sikkerhedsbrud

Det er endnu ikke fast besluttet, hvilket værktøj der skal anvendes til vidensbiblioteket, men udgangspunktet vil blive Microsoft Teams, som alle har adgang til, hvorfor opgaven med at skabe indhold, kan gå i gang omgående. Det bliver igen de institutioner, der samarbejder omkring DPO-funktionen, der vil få adgang.

- Trin to af uddannelsespakken, der også er en del af den rammeaftale vi har med BDO, bliver iværksættelse af en Phishing kampagne, hvor vi vil lokke mailbrugerne til at afgive deres personlige oplysninger. Denne kampagne er tæt på at have stabelafløb for første udsendelse.
- På sekretariatets webside, vil vi informere om FGUs håndtering af GDPR-implementeringen, der er ganske unik i sammenligning med den offentlige sektor i øvrigt, hvor vi med en effektiv centralisering og styring har sparet den enkelte institution for mange timers arbejde og vil kunne gøre det fremover også i forhold til de praktiske opgaver der skal udføres hvert år fremover, samt dele generiske og almene informationer om emnet.
- Opbygning af et DPA-team, hvor deltagerne i samarbejde med DPO'en lægger planen for hvordan uddannelse, støtte, hjælp, bidrag etc bedst opfylder behovet og sikrer at den enkelte DPA bliver klædt på med de nødvendige kompetencer.
(DPA: Data Protection Assistant eller GDPR ansvarlig)

Målet er at have en DPA på hver enkelt institution og indenfor en 3 årig periode at få opbygget et egentligt DPO team, der kan sikre personafhængighed ved f.eks. sygdom, ferie og andet fravær i forhold til håndtering af sikkerhedsbrud og således sikre at der altid er en DPO klar til at spille bolden i enhver krisesituation.

- Etablering af en DPO mailboks, hvortil man kan sende alt vedr. GDPR. Denne mailboks tænkes at blive administreret af alle deltagerne i DPA-teamet.
- De ovenstående opgaver vil indgå i et årshjul, der synliggør hvornår de enkelte områder er i fokus og dette årshjul kommer til at ligge tilgængeligt sekretariatets webside.
- Yderligere vil DPO'en som del af funktionen indgå i DPO netværk hos f.eks. Statens IT, STIL etc, hvor det er vigtigt at FGU har en stemme og desuden bidrage i forhold til IT og informationssikkerhed.

Ivan Sommer



DPO – FGU Danmark

M: iso@fgu.dk

T: 2782 7300