Bilag 1.1 til samarbejdsaftalen

DPO- og udvidet datasikkerhedssamarbejde

Baggrund

Styregruppen oprettede pr. 1. januar 2017 et datasikkerhedssamarbejde. Den europæiske databeskyttelsesforordning stiller krav om, at offentlige myndigheder og institutioner udpeger en DPO. Partnerskolerne har anmodet Gymnasiefællesskabet om at løfte skolernes DPO opgave. DPO'en skal være uafhængig og skal være i stand til at udøve uvildig rådgivning. Partnerskolerne kan som led i 1 af de 3 minimums-samarbejdsområder bede Gymnasiefællesskabet om at varetager den lovpligtige DPO funktion og deltage i det udvidede datasikkerhedssamarbejde (compliance-arbejde og risikovurderingsarbejdet samt opfølgning på databehandlerne).

Opgaver og ydelser for datasikkerhedssamarbejdet og DPO-funktionen

Datasikkerheds- og DPO-samarbejdet består af følgende ydelser:

- DPO-funktionens kontrol- og rådgivningsydelser i medfør af GDPR
- GDPR implementeringsfunktion, der bistår partnerskolerne med compliance-arbejdet, herunder med risikovurderinger (forudsætter lokale implementeringer), ajourføring af risikovurderinger, analyser af behovet for databehandleraftaler samt med indgåelse af databehandleraftaler, stramning af eksisterende databehandleraftaler, kontrol med databehandleraftaler mv.

Teamet indgår i tæt samarbejde med partnerskolernes lokale datasikkerhedstovholdere/GDPR-teams.

DPO-funktionen og datasikkerhedssamarbejdets implementeringsfunktion er adskilte funktioner og samarbejder efter behov.

Som led i Datasikkerheds- og DPO-samarbejdet tilbyder Gymnasiefællesskabet blandt andet:

- Sparring og samarbejde med skolernes ledelser mhp. overholdelse af persondatareglerne
- Rådgivning af skolerne på alle niveauer
- Netværksinitiering for skolernes gdpr-tovholdere
- Støtte til skolerne ved forespørgsler om de registrerede personers rettigheder
- Udvikling/videreudvikling af retningslinjer, værktøjer og politikker til brug for de konkrete arbejdsgange i skoledriften, der indebærer behandling af persondata
- Kontakt med samarbejdspartnere og relevante myndigheder i og uden for sektoren
- Understøttelse af skolerne i opgaven med at kunne dokumentere datasikkerheden
- Fortolkning af regler og konkretisering af "hvad man må gøre" med persondata
- Rådgivning til skolernes overvejelser om datasikkerhed ved indkøb og implementering af it-systemer
- Rådgivning til skolerne vedr. model til – *samt konkret bistand i forbindelse med* - gennemgang, indgåelse og håndhævelse af databehandleraftaler samt løbende opfølgning på behandlingssikkerheden hos databehandlerne.
- Rådgivning af skolerne vedr. digitale og manuelle sletterutiner (afklaring af behov, metode, og bud på fastlæggelsen af administrative arbejdsgange, der understøtter sletteopgaven på en så ressource-besparende og sikker måde som muligt).

Skolerne modtager vejledning og individuel rådgivning i, hvordan de kan leve op til kravene. Gymnasiefællesskabet afholder løbende kurser/netværk-indsatser, målrettet skolernes behov.

Skolerne modtager endvidere en række skabeloner og vejledninger, som de kan vælge at hente inspiration i, f.eks. om medarbejderes persondata, elevers persondata, skolernes studievejledning,

generelle retningslinjer osv. Derudover modtager skolerne f.eks. formuleringer til ansættelsesbreve, velkomstbreve og besvarelse af anmodninger om indsigt i- eller sletning af egne personoplysninger. Gymnasiefællesskabet har blandt andet udarbejdet en komplet skoledatasikkerhedshåndbog.

DPO-funktionen rådgiver den dataansvarlige skole og overvåger og bistår skolerne med at efterleve reglerne om databeskyttelse. Hvad der konkret ligger i denne opgave afhænger af den enkelte skoles situation, behov og prioriteringer, hvorfor DPO-funktionen er i tæt kontakt med den enkelte skole om indholdet af rådgivningsopgaven.

Implementeringsfunktionen bidrager til skolernes praktiske implementering af tiltag og driftsopgaver, som DPO-funktionen i medfør af GDPR alene må rådgive om. Dermed sikres kravene i GDPR om, at DPO-funktionen skal være uafhængig og skal udøve kontrol men ikke må udøve kontrol af eget arbejde. Samtidig sikres det, at skolerne får den praktisk assistance til udførelse af implementeringsopgaver, som der kan være forskellige og driftsmæssige behov for.

Kollektiv ordning hvor der ydes bistand med:	DPO- funktionen bidrager med følgende:
A. Risikovurderinger (forudsætter lokale implementeringer) samt ajourføring af risikovurderinger B. Analyser af behovet for databehandleraftaler samt bistand til indgåelse af databehandleraftaler og stramning af eksisterende databehandleraftaler, C. Kontrol med databehandleraftalerne, herunder løbende tilsyn med databehandlere f.eks. assistance til at indhente og gennemgå revisionserklæringer mv., der leveres af eksterne databehandlere D. Bistand med at leverandører får slettet forældede data i overensstemmelse med databehandleraftaler samt ved ophør af brug af værktøjer mv. **Funktionen bidrager også med:** E. Udarbejdelse, tilpasning af redskaber, skabeloner mv, herunder opdatering af skoledatasikkerhedshåndbogen	1. Rådgivning af dataansvarlige og hjælp til organisationens efterlevelse af de databeskyttelsesretlige regler. 2. Stå til rådighed for ledelsen, ansatte, elever (og værger) vedrørende spørgsmål om databeskyttelse 3. Udarbejdelse og tilpasning af data-politikker 4. Konkret undervisning, dialog, besvarelse af spørgsmål, tolkning af regler og udtalelser, vejledning 1. Løbende feedback ifht. skolens efterlevelse af de databeskyttelsesretlige regler i organisationen, 2. Overvågning (kontrol) og kvalitetssikring af, at forudsætninger for skolens lovlige behandling af personoplysninger er til stede, herunder at: ✓ Skolen har politikker om databeskyttelse (og disse er er kendt af de relevante medarbejdere, de ajourføres løbende og de påses overholdt fra ledelses side) ✓ Skolen uddanner sit personale i databeskyttelse ✓ Skolen har oplysningskampagner ✓ Skolen har overblik over hvem, der er ansvarlig for hvad i organisationen ✓ Skolen indhenter og gennemgår revisioner af fx studieadministrative systemer og øvrige væsentlige it-systemer, der leveres af eksterne databehandlere ✓ Skolen løbende gennemfører en aktiv vurdering af, hvilke sikkerhedsforanstaltninger (tekniske og organisatoriske), som skal anvendes for at begrænse risici i forhold til de registreredes rettigheder og interesser 3. DPO-funktionen er kontaktpunkt for tilsynsmyndigheden (Datatilsynet). 4. DPO-funktionen bistår skolen med at håndtere konkrete klagesager, som indbringes for Datatilsynet. 5. På skolens konkrete anmodning bistår DPO-funktionen skolen med at håndtere sager om sikkerhedsbrud/-læk af personoplysninger, herunder bistand til at foretage anmeldelse af læk til Datatilsynet og evt. også til de berørte registrerede personer. Det er skolen selv, der beslutter, om der skal ske anmeldelse til Datatilsynet og til de registrerede personer. Skolen rådfører sig med DPO-funktionen herom.

	DPO- funktionen er f.eks. afskåret fra at udføre følgende opgaver pga. sin uafhængighed i medfør af GDPR-reglerne: 1. Håndtering af registrerede personers anmodning om indsigt i egne oplysninger, sletning mv. 2. Mindre praktiske eller almindelige driftsopgaver eller driftsmæssige spørgsmål knyttet til opsætning af it-systemer 3. Beslutning om anmeldelse af læk til Datatilsynet og til de berørte registrerede personer 4. Løbende tilsyn med og kontrol af databehandlere

Forudsætninger og rammer for DPO-funktionens virke

GF's DPO-funktion er den dataansvarlige partnerskoles *rådgiver*, som partnerskolen kan og skal inddrage i alle spørgsmål om databeskyttelse på skolen[1].

GF's DPO-funktion skal *overvåge*, at persondatalovgivningen overholdes hos partnerskolen og skal på bedste vis understøtte en god databeskyttelse hos partnerskolen.

DPO-funktionen refererer direkte til rektor/ledelsen, og samarbejder med de dele af skolens organisation, som rektor anviser herunder datasikkerhedstovholderen/GDPR-teamet på skolen.

Det er dog ledelsen, som på baggrund af DPO-funktionens afrapportering og rådgivning afgør, om en påtænkt eller igangværende behandling, systemanvendelse, medarbejderinstruks eller lign., ud fra en risikovurdering kan iværksættes eller opretholdes.

Ansvaret for, at skolens behandling af personoplysninger sker efter reglerne, påhviler skolen, som dataansvarlig institution. Det er også skolen, som sanktioneres, hvis reglerne ikke overholdes, også selvom dette skyldes ukorrekt rådgivning fra DPO-funktionens side.

Det er skolens (rektors) opgave at sikre, at nedenstående forhold etableres som forudsætning for DPO-funktionens virke:

Partnerskolen skal inddrage DPO-funktionen "*rettidigt og tilstrækkeligt*" til, at DPO-funktionen har reel mulighed for at yde skolen rådgivning om, hvorvidt skolens brug af persondata, it-systemer, databehandlere samt skolens handleplaner og databeskyttelsespolitikker lever op til databeskyttelsesreglerne.

1. Kravet om "rettidig" inddragelse af DPO-funktionen indebærer, at skolen skal inddrage DPO-funktionen forud for skolens iværksættelse af en påtænkt behandling af personoplysning, ibrugtagning af nye funktioner i et it-system, udstedelse af nye retningslinjer til medarbejderne, mv.
2. Kravet om "*tilstrækkelig*" inddragelse af DPO-funktionen indebærer, at skolen skal tage højde for DPO-funktionens bemærkninger, rådgivning og rapportering af en given situation.

Partnerskolen skal endvidere:

- Offentliggøre kontaktoplysninger for DPO-funktionen på sin hjemmeside samt meddele oplysningerne til Datatilsynet.
- Oplyse de registrerede personer om DPO-funktionens kontaktoplysninger i skolens standardorienteringer om behandling af personoplysninger, som fx typisk gives i forbindelse med skolestart i 1.g. (for elevers vedkommende) og som led i opstart af ansættelsesforhold (for medarbejderes vedkommende).

[1] Dette fremgår direkte af databeskyttelsesforordningens art. 38, stk. 1. Datatilsynets vejledning om databeskyttelsesrådgivere kan læses her https://www.datatilsynet.dk/regler-og-vejledning/databeskyttelsesraadgivere-dpoer