



## Bilag 1.1 til samarbejdsaftalen

Opdateret april 2018

### Gymnasiefællesskabets DPO-funktion

#### Baggrund

Den europæiske databeskyttelsesforordning stiller krav om, at offentlige myndigheder og institutioner udpeger en DPO. Dette skal senest ske fra den 25. maj 2018. "DPO" er en forkortelse af "Data Protection Officer" – på dansk: "databeskyttelsesrådgiver".

DPO-funktionen er element i databeskyttelsesforordningens fokus på "ansvarlighed" og "dokumentation" i forhold til overholdelse af databeskyttelsesreglerne. Den dataansvarlige institution har pligt til at inddrage DPO'en i et omfang, der er såkaldt "tilstrækkeligt og rettidigt" til at DPO'en kan vurdere, om institution prioriteringer, planer, politikker og praksis lever op til databeskyttelsesreglerne.

Det kan fx være som led i de generelle overvejelser og beslutninger om, hvordan man overholder databeskyttelsesreglerne fx ved formulering af retningslinjer til medarbejderne, ved vurdering af om en behandling kræver samtykke fra den registrerede person eller ej, ved overvejelser om datasikkerheden i it-systemer eller ved ibrugtagning af nye it-platforme, hvor der kan være særlig risiko for manglende beskyttelse af personoplysninger.

DPO'en medvirker på den måde til, at den dataansvarlige institution har styr på, hvilke personoplysninger der behandles og hvordan behandlingen sker.

Den dataansvarlige institution har pligt til at tage højde for DPO'ens vurdering af en given situation. Dette medfører dog ikke, at DPO'en overtager selve ansvaret for, at behandlingen af personoplysninger sker i overensstemmelse med reglerne. I sidste ende er det den dataansvarlige institution, der skal overholde reglerne og som selv afgør, om en bestemt behandling ud fra en risikovurdering kan iværksættes eller opretholdes samt med hvilke hjælpemidler. Det er også den dataansvarlige institution, som sanktioneres, hvis reglerne ikke overholdes, også selvom dette skyldes ukorrekt rådgivning fra DPO'ens side.

DPO'en er uafhængig og refererer direkte til den dataansvarlige institutions øverste ledelse.

#### Generelt om Gymnasiefællesskabets DPO-funktion

Gymnasiefællesskabets DPO-funktion<sup>1</sup> rådgiver de deltagende partnerskoler om de databeskyttelsesretlige regler og understøtter på bedste vis en god databeskyttelse hos den dataansvarlige partnerskole.

Styregruppen har besluttet, at alle partnerskoler automatisk deltager i DPO-samarbejdet.

#### Grundydelse: DPO-funktion

DPO'en rådgiver den dataansvarlige skole og bistår skolen med at efterleve reglerne om databeskyttelse.



Hvad der konkret ligger i denne opgave afhænger af den enkelte skoles situation, behov og prioriteringer, hvorfor DPO'en er i tæt kontakt med den enkelte skole om indholdet af rådgivningsopgaven.

Skolerne kan trække på følgende grundydelse:

1. Konkret undervisning, dialog, besvarelse af spørgsmål, tolkning af regler og udtalelser, vejledning
2. Udarbejdelse og tilpasning af redskaber, politikker og skabeloner til brug for skolens medarbejdere
3. Gennemgang af databehandleraftaler og it-kontrakter med henblik på at vurdere, om brugen af en konkret it-ydelse rummer en risiko i forhold til de registrerede personers rettigheder
4. Løbende bistand til risikovurdering af skolens it-set up (herunder årlig indhentning af revisionserklæringer fra de databehandlere, der fremgår af skema i Bilag 1)

Som grundydelse udfører DPO'en endvidere følgende for skolen:

5. Løbende feedback af skolens efterlevelse af de databeskyttelsesretlige regler i organisationen, herunder kvalitetssikring med at følgende forudsætninger for skolens lovlige behandling af personoplysninger er til stede:
  - Skolen har politikker om databeskyttelse (og disse 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 gennemfører løbende en aktiv vurdering af, hvilke sikkerhedsforanstaltninger (tekniske og organisatoriske) som skal anvendes for at begrænse risici i forhold til de registreredes rettigheder og interesser
6. DPO'en er kontaktpunkt for tilsynsmyndigheden (Datatilsynet) samt alle medarbejdere, elever (og deres værgere) om alle spørgsmål om skolens behandling af personoplysninger og om udøvelse af deres rettigheder efter databeskyttelsesforordningen
7. DPO'en bistår skolen med at håndtere konkrete klagesager, som indbringes for Datatilsynet.
8. DPO'en bistår skolen med at håndtere konkrete sager om læk af personoplysninger

DPO'en bistår ikke med følgende opgaver:

- Håndtering af registrerede personers anmodning om indsigt i egne oplysninger, sletning mv.
- Mindre praktiske eller almindelige driftsopgaver eller driftsmæssige spørgsmål knyttet til opsætning af it-systemer
- Udarbejdelse af konkrete databehandleraftaler
- Behandling af personoplysninger, der finder sted i overensstemmelse med interne regler, som den dataansvarlige skole har fastsat

For at DPO'en kan udføre sit arbejde, og de registrerede personer let kan komme i kontakt med DPO'en, skal skolen:

- Offentliggøre kontaktoplysninger for DPO'en på sin hjemmeside samt meddele oplysningerne til Datatilsynet
- Oplyse de registrerede personer om DPO'ens kontaktoplysninger i skolens standardorienteringer om behandling af personoplysninger, som typisk gives ifbm. skolestart i 1.g. (for elevernes vedkommende) og som led i opstart af ansættelsesforhold (for medarbejderen vedkommende).



## Opgaver som ikke er indeholdt i grundydelsen

Konkret bistand med databeskyttelsesmæssige overvejelser og tiltag (fx databeskyttelse gennem design og standardindstillinger) i forbindelse med implementering af nye it-programmer af større *omfang*.

DPO'en kan ikke for nuværende indestå for om skolers cloud-løsninger samt skolers indgåede IT-kontrakter med multi-internationale selskaber (fx Microsoft og Google) lever op til lovgivningen.

DPO'en kan i disse situationer alene yde rådgivning med afsæt i Datatilsynets vejledninger, anbefalinger og afgørelser.

Skoler må i disse situationer forvente, at skulle søge ekstern ekspertrådgivning.