Godkendt af styregruppen juni 2018

Bilag 1.1 til samarbejdsaftalen - 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 databeskyttelse.

Statsligt selvejende gymnasier har pligt til at have en DPO.

Forudsætninger og rammer for DPO'ens virke - DPO'ens relation til den dataansvarlige partnerskole

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

GF's DPO understøtter på bedste vis en god databeskyttelse hos partnerskole.

DPO'en referer direkte til rektor, men samarbejder med de dele af skolens organisation, som rektor anviser.

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

Ansvaret for at skolens behandlingen 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'ens side.

<u>Det er skolens (rektors) opgave at sikre, at nedenstående relation etableres som forudsætning for DPO'ens virke:</u>

Partnerskolen skal inddrage DPO'en "*rettidigt og tilstrækkeligt*" til at DPO'en 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'en indebærer, at skolen skal inddrage DPO'en forud[2] for skolens iværksættelse af en påtænkt behandling af personoplysning, ibrugtagning af nye funktioner i et it-system, udstedelse af nye retningslinjer til medarbejderne, mv.

[1] Jf. databeskyttelsesforordningens art. 38, stk. 1

[2] I praksis er der selvsagt mange behandlinger af personoplysninger, der allerede ér igangsat. Disse er også omfattet af DPO'ens rådgivning, men DPO'ens primære fokus er fremadrettet, jf. nærmere nedenfor i afsnittet om grundydelser og "DPO'ens prioritering af ressourcer".

2. Kravet om "*tilstrækkelig*" inddragelse af DPO'en indebærer, at skolen skal tage højde for DPO'ens bemærkninger, rådgivning og rapportering af en given situation.

Partnerskolen skal endvidere:

- 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 elevers vedkommende) og som led i opstart af ansættelsesforhold (for medarbejderes vedkommende).

Grundydelser: DPO-funktion

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

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 grundydelser:

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 **e**n 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 GF's databehandlerark)

Som grundydelse udfører DPO'en endvidere følgende for skolen:

1. Løbende feedback ifht. 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 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

2. DPO'en er kontaktpunkt for tilsynsmyndigheden (Datatilsynet) samt alle medarbejdere, elever (og deres værger) om alle spørgsmål om skolens behandling af personoplysninger og om udøvelse af deres rettigheder efter databeskyttelsesforordningen

3. DPO'en bistår skolen med at håndtere konkrete klagesager, som indbringes for Datatilsynet.

4. På skolens konkrete anmodning bistår DPO'en skolen med at håndtere sager om læk af

personoplysninger, herunder 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'en herom.

DPO'en udfører ikke følgende opgaver, idet DPO'en er afskåret herfra pga. sin uafhængighed:

- 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
- Beslutning om anmeldelse af læk til Datatilsynet og til de berørte registrerede personer

DPO'en prioriterer sine ressourcer på følgende måde:

1. Primært fokus på skolens fremadrettede, påtænkte aktiviteter vedr. databeskyttelse, herunder nye behandlinger, nye it-systemer, nye politikker, mv.
2. Fokus på de af skolens igangværende aktiviteter, som ud fra en risikovurdering konkret indebærer en højere risiko for brud på databeskyttelse – enten pga. mangler ved de it-systemer, der anvendes eller fordi der behandles følsomme personoplysninger
3. Fokus på igangværende aktiviteter, der ud fra en risikovurdering konkret indebærer lavere risiko for brud på databeskyttelse – enten fordi skolen har fuld kontrol over data på egen server eller fordi der er tale ikke-følsomme personoplysninger
4. I mindre grad fokus på afgrænsede behandlinger, fx kortvarig brug af apps som led i undervisning

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.