Cirkulæreskrivelse om Styrelsen for It og Lærings opgaver som databehandler i visse administrative systemer på undervisningsområdet

1. Indledning

1.1. Denne cirkulæreskrivelse er udarbejdet af Styrelsen for It og Læring under henvisning til databeskyttelsesforordningens artikel 28 om forholdet mellem aktører, der har en rolle som henholdsvis dataansvarlig og databehandler i relation til en behandling af personoplysninger.

På undervisningsområdet foretager Styrelsen for It og Læring på vegne af en række statslige institutioner, privat- og offentligt selvejende institutioner, private institutioner, kommuner og regioner behandling af personoplysninger i visse administrative systemer, som institutionerne er forpligtet til at benytte i henhold til:

- §§ 108, 109, 112, 114, 115, 116, 117 og 118 i "Bekendtgørelse om erhvervsuddannelser" for Praktikpladsen.dk og for EASY P
- § 5 i "Bekendtgørelse om prøver og eksamen i de almene og studieforberedende ungdoms- og voksenuddannelser" (BEK nr. 343 af 08/04/2016) for Netprøver
- § 4 i "Bekendtgørelse om udbetaling af bonus til private arbejdsgivere, der ansætter elever i erhvervsgrunduddannelse" (egu-bonusordningen) for EGU-Portalen
- § 13 i "Bekendtgørelse af lov om erhvervsuddannelser" for Elevplan og Digitale Uddannelsesaftaler
- § 61 i "Bekendtgørelse om erhvervsuddannelser" for Elevplan og Digitale Uddannelsesaftaler
- § 13 b i "Bekendtgørelse af lov om folkeskolen" for Elevplan og Digitale Uddannelsesaftaler
- §§ 2 d og 2 f i "Bekendtgørelse af lov om vejledning om uddannelse og erhverv samt pligt til uddannelse, beskæftigelse m.v." (vejledningsloven) for Elevplan og Digitale Uddannelsesaftaler
- § 18 i "Bekendtgørelse af lov om kombineret ungdomsuddannelse" for KUU-Portalen
- §§ 11, 23, 24, 25, 36 og 37 i "Bekendtgørelse om uddannelsesparathedsvurdering, uddannelsesplaner og procedurer ved valg af ungdomsuddannelse" for Optagelse.dk
- § 2 i "Bekendtgørelse om digital kommunikation ved ansøgning om optagelse på videregående uddannelse" for Optagelse.dk

Vilkårene for anvendelse af systemerne er de samme for statslige institutioner, privat- og offentligt selvejende institutioner, private institutioner, kommuner og regioner, der efter aftale med Styrelsen for It og Læring har valgt at benytte systemerne.

Det drejer sig om følgende systemer:

- Easy A
- Easy F
- Easy P
- EGU-Portalen
- Elevplan.dk og Digitale Uddannelsesaftaler
- KUU-Portalen
- Netprøver
- Optagelse.dk
- Praktik+
- Praktikpladsen.dk
- SkoleKom
- Viseffekt.dk

1.2. Styrelsen for It og Læring er databehandler for den behandling, som sker ved brug af de anførte administrative systemer, jf. punkt 1.1., da styrelsens behandling af personoplysninger i disse systemer alene sker til institutionernes formål og på institutionernes vegne, hvorved institutionerne er dataansvarlige for behandlingen af oplysningerne.

1.3. Efter databeskyttelsesforordningens artikel 28, stk. 3, skal en databehandlers behandling være reguleret af en kontrakt eller andet retligt bindende dokument i henhold til EU-retten eller medlemslandenes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, og der fastsætter:

1. Genstanden for og varigheden af behandlingen
2. Behandlingens karakter og formål
3. Typen af personoplysninger og kategorierne af registrerede
4. Den dataansvarliges forpligtelser og rettigheder

1.4. Det er på denne baggrund, at Styrelsen for It og Læring i nærværende cirkulæreskrivelse angiver, hvordan Styrelsen for It og Læring kan behandle personoplysninger i de administrative systemer, jf. punkt 1.1, som Styrelsen for It og Læring stiller til rådighed for institutionerne, og hvor Styrelsen for It og Læring foretager databehandlingen på vegne af institutionerne til institutionernes formål.

Cirkulæreskrivelsen er gældende for alle institutioner, som anvender de nævnte systemer, og fastsætter de rettigheder og forpligtelser, som finder anvendelse, når Styrelsen for It og Læring foretager behandling af personoplysninger på vegne af den enkelte institution til institutionens formål.

Cirkulæreskrivelsen er herved det retlige dokument, som er krævet i databeskyttelsesforordningens artikel 28, stk. 3.

1.5. Oplysninger om Styrelsen for It og Lærings behandling i de enkelte administrative systemer, herunder behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varigheden af behandlingen i de enkelte administrative systemer fremgår af hjemmesiden for Styrelsen for It og Læring (www.viden.stil.dk).

1.6. Cirkulæreskrivelsen frigør ikke Styrelsen for It og Læring for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

1.7. De enkelte institutioner er som led i deres efterlevelse af databeskyttelsesforordningens regler forpligtet til at gøre sig bekendt med indholdet af cirkulæreskrivelsen og følge den i forbindelse med behandling af personoplysninger ved hjælp af disse systemer.

2. Anvendelsesområde

2.1. Herved fastsættes bestemmelser om den behandling, som Styrelsen for It og Læring kan foretage i de under pkt. 1.1. anførte administrative systemer på undervisningsområdet, hvor systemerne stilles til rådighed for institutionerne af Styrelsen for It og Læring som databehandler, og hvor institutionerne er forpligtet til at gøre brug af de administrative systemer, jf. de hjemmelsgrundlag, der er angivet i punkt 1.1, eller efter aftale med Styrelsen for It og Læring har valgt at gøre brug af systemerne.

2.2. Styrelsen for It og Læring må ikke behandle personoplysninger i de under punkt 1.1. anførte administrative systemer til andre formål og opgaver, end det fremgår af denne cirkulæreskrivelse.

3. Den dataansvarliges forpligtelser og rettigheder

3.1. Som bruger af systemerne er den enkelte institution ansvarlig for den behandling af personoplysninger, som finder sted i forbindelse med anvendelsen af det enkelte system, sker inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

3.2. Den dataansvarlige institution har derfor både rettighederne og forpligtelserne til at træffe beslutning om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

3.3. Den enkelte institution er blandt andet ansvarlig for, at der er en hjemmel til behandling af de personoplysninger, som institutionen registrerer og behandler i systemerne, samt at kunne dokumentere en gyldig behandlingshjemmel, eksempelvis hvis hjemlen er baseret på et samtykke fra den registrerede, jf. databeskyttelsesforordningens artikel 7 om betingelser for samtykke.

4. Databehandlerens adgang til behandling af personoplysninger

4.1. Styrelsen for It og Læring må kun behandle de personoplysninger, som den enkelte institution lægger ind i systemet i overensstemmelse med reglerne i nærværende cirkulæreskrivelse, medmindre behandlingen kræves i henhold til EU-retten eller medlemsstaternes nationale ret, som Styrelsen for It og Læring er underlagt; I så fald underretter Styrelsen for It og Læring den dataansvarlige institution om dette retlige krav inden behandlingen, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. databeskyttelsesforordningens artikel 28, stk. 3, litra a.

4.2. Styrelsen for It og Læring varetager på vegne af de dataansvarlige institutioner opgaven med videregivelse af data fra de administrative systemer til brug for udførelse af statistiske eller videnskabelige undersøgelser, jf. databeskyttelseslovens § 10, når den rekvirerende aktør efter lovgivningen har hjemmel og de fornødne tilladelser til, at videregivelse af personoplysninger til sådanne formål kan ske. Den dataansvarlige institution skal således ikke anmode Styrelsen for It og Læring om videregivelse hertil i hvert enkelt tilfælde.

5. Fortrolighed

5.1. Styrelsen for It og Læring sikrer, at kun de personer, som aktuelt i styrelsen er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den enkelte institution. Adgangen til oplysningerne skal straks lukkes ned, hvis autorisationen fratages eller udløber.

5.2. Styrelsen for It og Læring autoriserer de personer, for hvem det er nødvendigt at have adgang til personoplysningerne i det relevante administrative system for at kunne opfylde de forpligtelser, som Styrelsen for It og Læring har over for den enkelte institution.

5.3. Styrelsen for It og Læring sikrer, at de personer, der i styrelsen er autoriseret til at behandle personoplysninger på vegne af den enkelte institution, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

5.4. Styrelsen for It og Læring skal efter anmodning fra den dataansvarlige institution kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

6.1. Styrelsen for It og Læring iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, som passer til disse risici.

6.2. Ovenstående forpligtelse indebærer, at Styrelsen for It og Læring skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

a) Pseudonymisering og kryptering af personoplysninger
b) Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester
a) Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
b) En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed

7. Anvendelse af underdatabehandlere

7.1. Styrelsen for It og Læring er berettiget til at anvende underdatabehandlere i tilknytning til de omhandlede systemer.

7.2. Ved anvendelse af underdatabehandlere er Styrelsen for It og Læring ansvarlig for at efterleve kravene i databeskyttelsesforordningens artikel 28. Styrelsen for It og Læring er herefter bl.a. forpligtet til:

- Alene at anvende underdatadatabehandlere, der kan stille de fornødne garantier for, at de gennemfører de passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandling opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder,
- At sikre, at der foreligger en gyldig underdatabehandleraftale mellem Styrelsen for It og Læring og en eventuel underdatabehandler.

7.3. Styrelsen for It og Læring skal på styrelsen hjemmeside (www.viden.stil.dk) give oplysning om underdatabehandlere for de enkelte administrative systemer.

Styrelsen for It og Læring skal endvidere på anmodning fra en institution oplyse om, hvorvidt oplysningerne behandles af underdatabehandlere. Underdatabehandleraftalen og eventuelle senere ændringer hertil sendes – efter den enkelte institutions

anmodning herom - i kopi til institutionen, som herigennem har mulighed for at sikre sig, at der er indgået en gyldig aftale mellem Styrelsen for It og Læring og underdatabehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til institutionen.

7.4. Styrelsen for It og Læring sørger for at pålægge underdatabehandlere de samme databeskyttelsesforpligtelser, som dem, der er fastsat ved denne cirkulæreskrivelse, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.

7.5. Styrelsen for It og Læring er således ansvarlig for – igennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som Styrelsen for It og Læring selv er underlagt efter databeskyttelsesreglerne og denne cirkulæreskrivelse.

7.6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Styrelsen for it og Læring fuldt ansvarlig over for den dataansvarlige institution for opfyldelsen af underdatabehandlerens forpligtelser.

8. Overførsel af oplysninger til tredjelande eller internationale organisationer

8.1. Styrelsen for It og Læring må alene overføre (overlade, videregive samt intern anvendelse) til tredjelande eller internationale organisationer til brug for styrelsens opgaveløsning i forhold til institutionerne, medmindre sådan overførsel kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Styrelsen for It og Læring er underlagt; i så fald underretter Styrelsen for It og Læring den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. databeskyttelsesforordningens artikel 28, stk. 3, litra a.

8.2. Styrelsen for It og Læring er ansvarlig for iagttagelsen af kravene i databeskyttelsesforordningens kapitel V, hvis der sker en sådan overførsel af personoplysninger til tredjelande eller internationale organisationer.

9. Bistand til den dataansvarlige institution

9.1. Styrelsen for It og Læring bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige institution ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af institutionens forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder, som er fastlagt i databeskyttelsesforordningens kapitel 3.

Dette indebærer, at Styrelsen for It og Læring så vidt muligt skal bistå den dataansvarlige institution i forbindelse med, at institutionen skal sikre overholdelsen af nedenstående regler i databeskyttelsesforordningen:

- Oplysningspligten ved indsamling af personoplysninger hos den registrerede, jf. artikel 13
- Oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede, jf. artikel 14
- Den registreredes indsigtsret, jf. artikel 15
- Retten til berigtigelse, jf. artikel 16
- Retten til sletning (»retten til at blive glemt«), jf. artikel 17
- Retten til begrænsning af behandling, jf. artikel 18
- Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling, jf. artikel 18
- Retten til indsigelse, jf. artikel 21

9.2. Styrelsen for It og Læring bistår den dataansvarlige institution med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for Styrelsen for It og Læring som databehandler, jf. databeskyttelsesforordningens art 28, stk. 3, litra f. Dette indebærer, at Styrelsen for It og Læring under hensynstagen til behandlingens karakter skal bistå den enkelte institution i forbindelse med, at institutionen skal sikre overholdelsen af:

a) Forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen.
b) Forpligtelsen til at anmelde brud på persondatasikkerheden til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer, efter at den enkelte institution er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
c) Forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

d) Forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
e) Forpligtelsen til at høre Datatilsynet inden behandling, hvis en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den enkelte institution for at begrænse risikoen.

10. Underretning om brud på datasikkerhed til Datatilsynet

10.1. Styrelsen for It og Læring underretter uden unødig forsinkelse den enkelte institution efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Styrelsen for It og Læring eller en eventuel underdatabehandler.

10.2. Styrelsen for It og Læring er ansvarlig for efterlevelsen af databeskyttelsesforordningens artikel 33 om anmeldelse af brud på persondatasikkerheden til Datatilsynet. Dette gælder dog ikke, hvis der er tale om et brud på personsikkerheden, som skyldes den enkelte institutions egen uberettiget anvendelse af systemet. Den enkelte institution er således selv ansvarlig for efterlevelsen af databeskyttelsesforordningens artikel 33 om anmeldelse af brud på persondatasikkerheden til Datatilsynet, hvis et brud på persondatasikkerheden skyldes institutionens egen uberettiget anvendelse af systemet.

10.3. I overensstemmelse med cirkulæreskrivelsens afsnit 9.2, litra b, skal Styrelsen for It og Læring under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for styrelsen – bistå den enkelte institution med at foretage anmeldelse af bruddet til Datatilsynet, hvis institutionen efter cirkulæreskrivelsens afsnit 10.2. er ansvarlig for at foretage anmeldelsen til Datatilsynet. Det kan betyde, at Styrelsen for It og Læring bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarlige institutions anmeldelse til Datatilsynet:

a) Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
b) Sandsynlige konsekvenser af bruddet på persondatasikkerheden
c) Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

11. Sletning og tilbagelevering af oplysninger

11.1. Personoplysningerne opbevares i de administrative systemer hos Styrelsen for It og Læring i de nedenfor angivne tidsperioder:

- Personoplysninger i EASY A slettes 1 år efter systemets udfasning i 2019.
- Personoplysninger i EASY F og EASY P slettes ikke af hensyn til sikring af dokumentation for uddannelsesaftaler og uddannelsesbevis.
- Personoplysninger i EGU-Portalen og KUU-Portalen af relevans for elevens uddannelsesforløb opbevares i 4 år. Dog slettes elevers notater og porteføljer efter en kort karensperiode når eleverne har fået status ”gennemført” eller ”afbrudt”.
- Personoplysninger i Elevplan og Digitale Uddannelsesaftaler af relevans for dokumentation af elevfravær opbevares i op til 1 år. Data af relevans for dokumentation af elevers opnåede kompetencer slettes ikke. Øvrige personoplysninger, herunder opgavebesvarelser, opbevares i op til 5 år.
- Personoplysninger i Netprøver slettes 12 måneder efter oprettelse fra 2019.
- Personoplysninger i Optagelse.dk slettes en gang årligt.
- Personoplysninger i Praktik+ indlæses fra EASY P og slettes ikke automatisk af styrelsen.
- Personoplysninger i Praktikpladsen.dk slettes ikke automatisk af styrelsen, men kan slettes af eleven selv.
- Personoplysninger i SkoleKom slettes automatisk når en bruger ikke har været logget på SkoleKom i 12 måneder.
- Personoplysninger i Viseffekt.dk slettes ikke automatisk af styrelsen. Brugeren kan selv slette sine baggrundsoplysninger i mindst et halvt år efter brugeren har indtastet oplysningerne. En senere sletning af brugeroplysningerne foretages af STIL efter anmodning fra brugeren eller den dataansvarlige på vegne af brugeren.

11.2. Ved ophør af tjenesterne vedrørende behandling af forpligtes Styrelsen for It og Læring til, efter den dataansvarlige institutions valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige institution, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

12. Tilsyn og revision

12.1. Styrelsen for It og Læring stiller alle oplysninger, der er nødvendige for at påvise styrelsens overholdelse af databeskyttelsesforordningens artikel 28 og reglerne i denne cirkulæreskrivelse, til rådighed for den dataansvarlige institution og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller anden revisor, som er bemyndiget af den dataansvarlige institution.

12.2. Styrelsen for It og Læring skal én gang årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart om databehandlerens overholdelse af reglerne i denne cirkulæreskrivelse med tilhørende bilag. Der er mellem parterne enighed om, at der kan anvendes følgende typer af revisionserklæringer: ISAE3000.

Styrelsen for It og Læring sender på anmodning fra en dataansvarlig institution snarest muligt efter indhentelsen kopi af revisionserklæringen til den enkelte institution til orientering.

12.3. Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem Styrelsen for It og Læring. Styrelsen for It og Læring skal én gang årligt indhente en revisionserklæring fra en uafhængig tredjepart om underdatabehandlerens overholdelse af styrelsens databehandleraftale med den pågældende. Der er mellem parterne enighed om, at der kan anvendes ISAE3000 eller tilsvarende revisionserklæringer.

Styrelsen for It og Læring sender på anmodning fra en dataansvarlig institution snarest muligt kopi af revisionserklæringen til den enkelte institution til orientering.

12.4. Styrelsen for It og Læring er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges institutions og Styrelsen for It og Lærings faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til Styrelsen for It og Lærings fysiske faciliteter mod behørig legitimation.

13. Orientering af den anden part

Styrelsen for It og Læring og de dataansvarlige institutioner orienterer hinanden om væsentlige forhold, der har betydning for de behandlinger og systemer, der er omfattet af denne cirkulæreskrivelse.

14. Ikrafttræden

Denne cirkulæreskrivelse træder i kraft den 25. maj 2018.

Styrelsen for It og Læring den 24. maj 2018

Jakob Harder