Cirkulæreskrivelse om fælles dataansvar for visse administrative systemer, som stilles til rådighed af Styrelsen for It og Læring

1. Indledning

1.1. Denne cirkulæreskrivelse er udarbejdet af Styrelsen for It og Læring under henvisning til databeskyttelsesforordningens artikel 26 om fælles dataansvar.

Styrelsen for It og Læring er ansvarlig for at levere en række administrative systemer på undervisningsområdet, som statslige institutioner, privat- og offentligt selvejende institutioner, private institutioner, kommuner og regioner er forpligtet til at benytte i henhold til:

- §§ 4 og 5 i "Almen eksamensbekendtgørelsen" for XPRS
- §§ 15, 20, 22 i "AVU-loven" for XPRS
- §§ 18 a og 28 i "Bekendtgørelse af lov om arbejdsmarkedsuddannelserne m.v." for Efteruddannelse.dk og Viskvalitet
- §§ 14 og 19 f i "Bekendtgørelse af lov om folkeskolen" for PrøveAdministrationsSystemet
- §§ 11 og 18 i "Bekendtgørelse af lov om godtgørelse og tilskud til befordring ved deltagelse i erhvervsrettet voksen- og efteruddannelse" for Efteruddannelse.dk
- § 15 i "Bekendtgørelse om åben uddannelse og tilskud til arbejdsmarkedsuddannelser m.v." for Efteruddannelse.dk
- § 29 i "Bekendtgørelse om arbejdsmarkedsuddannelserne" (AMU-bekendtgørelsen) for Viskvalitet
- § 2 i "Bekendtgørelse om folkeskolens prøver" for Folkeskolens Prøver
- §§ 45, 48 i "Lov om de gymnasiale uddannelser" for XPRS

Vilkårene for anvendelse af systemerne er de samme for statslige institutioner, privat- og offentligt selvejende institutioner, private institutioner, kommuner og regioner, der efter aftaler vælger at benytte systemerne.

Det drejer sig om følgende systemer:

- EfterUddannelse.dk
- Ordblindetesten
- PrøveAdministrationsSystemet (PAS)
- Folkeskolens Prøver (FP)
- Viskvalitet
- XPRS

Oplysning om data i de enkelte administrative systemer fremgår af hjemmesiden for Styrelsen for IT og Læring (www.viden.stil.dk).

1.2. Efter databeskyttelsesforordningens artikel 26 er der tale om et fælles dataansvar, når to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling af persondata. Dette er tilfældet for de anførte administrative systemer på undervisningsområdet, som leveres af Styrelsen for It og Læring i henhold til det under punkt 1.1. angivne hjemmelsgrundlag.

1.3. Når der er tale om et fælles dataansvar, skal de fælles dataansvarlige ifølge databeskyttelsesforordningens artikel 26, stk.1, på en gennemsigtig måde fastlægge deres respektive ansvar for overholdelse af forpligtelserne i henhold til forordningen, navnlig hvad angår udøvelse af den registreredes rettigheder og deres respektive forpligtelser til at fremlægge de oplysninger, der er omhandlet i databeskyttelsesforordningens artikel 13 (oplysningspligt ved indsamling af personoplysninger hos den registrerede) og artikel 14 (oplysningspligt hvis personoplysninger ikke er indsamlet hos den registrerede) ved hjælp af en ordning imellem dem, medmindre og i det omfang de dataansvarliges respektive ansvar er fastlagt i EU-ret eller medlemsstaternes nationale ret, som de dataansvarlige er underlagt.

Det er på denne baggrund, at Styrelsen for It og Læring ved retsregler i nærværende cirkulæreskrivelse angiver, hvordan dataansvaret er udmøntet i de systemer, som styrelsen stiller til rådighed for institutionerne. Cirkulæreskrivelsen er gældende for alle institutioner, som anvender de nævnte systemer.

1.4. 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 deres behandling af personoplysninger ved hjælp af disse systemer.

2. Anvendelsesområde

2.1. Herved fastsættes bestemmelser om ansvarsfordelingen mellem Styrelsen for It og Læring og de institutioner, der anvender de administrative systemer på undervisningsområdet, som stilles til rådighed af Styrelsen for It og Læring efter det under punkt 1.1. angivne hjemmelsgrundlag.

Personoplysninger, som institutionerne behandler i disse systemer, bliver også behandlet, herunder indsamlet, til formål hos Styrelsen for It og Læring, fordi Styrelsen for It og Læring har behov for oplysningerne til en viderebehandling, som styrelsen foretager uden instruks fra institutionerne.

Styrelsen for It og Læring indsamler institutionernes data fra en række systemer til fx administrative formål, tilsyn, kontrol og statistikformål, complianceanalyser og lignende. Denne viderebehandling sker til Styrelsen for It og Lærings egne formål og med Styrelsen for It og Læring som ene dataansvarlig, og viderebehandlingen af oplysningerne er derfor ikke omfattet af cirkulæreskrivelsen.

2.2. Det væsentligste indhold af den ordning, der fastsættes i denne cirkulæreskrivelse, skal gøres tilgængeligt for de personer, der registreres oplysninger om, jf. databeskyttelsesforordningens artikel 26, stk. 2.

2.3. Den registrerede kan, uanset ordningens udformning, udøve sine rettigheder i medfør af databeskyttelsesforordningen med hensyn til og over for den enkelte dataansvarlige, jf. databeskyttelsesforordningens artikel 26, stk. 3.

2.4. Ved institutionernes anvendelse af de angivne systemer, som stilles til rådighed af Styrelsen for It og Læring, foreligger der et fælles dataansvar. Ved vurderingen heraf er der bl.a. lagt vægt på, at de behandlinger af personoplysninger, som finder sted i systemet, sker til begge parters formål og med fælles hjælpemidler (systemet).

3. Overordnet ansvarsfordeling

3.1. Som bruger af systemerne er den enkelte institution bl.a. ansvarlig for den behandling af personoplysninger, som finder sted i forbindelse med anvendelsen af de enkelte systemer, herunder korrekt indsamling og registrering af oplysninger. Den enkelte institution er også i vidt omfang ansvarlig for udøvelsen af den registreredes rettigheder.

3.2. Som ansvarlig myndighed for systemerne er Styrelsen for It og Læring bl.a. ansvarlig for at foretage passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene for behandlingen i de forskellige systemer.

4. Principper og behandlingshjemmel

4.1. Den enkelte institution er ansvarlig for, at der er en hjemmel til behandling af de personoplysninger, som institutionen registrerer og behandler i systemerne.

4.2. Den enkelte institution er også ansvarlig for 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.

4.3. Den enkelte institution og Styrelsen for It og Læring er hver især ansvarlige for at overholde principperne for behandling af personoplysninger samt god databehandlingsskik, i det omfang at reglerne finder anvendelse på den pågældendes ansvarsområder i henhold til cirkulæreskrivelsen.

5. Den registreredes rettigheder

5.1. Den enkelte institution er ansvarlig for sikringen af de registreredes rettigheder gennem iagttagelse af nedenstående regler i databeskyttelsesforordningen:

- Oplysningspligt ved indsamling af personoplysninger hos den registrerede, jf. artikel 13,
- Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede, jf. artikel 14,
- Den registreredes indsigtsret, jf. artikel 15,
- Ret til berigtigelse, jf. artikel 16,
- Ret til sletning (retten til at blive glemt), jf. artikel 17,
- Ret til begrænsning af behandling, jf. artikel 18,

- Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling, jf. artikel 19.
- Ret til indsigelse mod en behandling, jf. artikel 21.

5.2. Den enkelte institution er ansvarlig for egne data og ansvarlig for behandlingen af anmodninger eller henvendelser fra de registrerede om de forhold, der er nævnt i punkt 5.1.

5.3. Hvis Styrelsen for It og Læring modtager en anmodning eller henvendelse fra en registreret person om forhold, der er nævnt i punkt 5.1., og som vedrører en anden institution, jf. punkt 5.2., sendes denne til besvarelse hos den relevante institution snarest muligt.

5.4. Styrelsen for It og Læring er ansvarlig for at bistå institutionerne i det omfang, at dette er relevant og nødvendigt for, at institutionerne kan efterleve deres forpligtelser over for de registrerede.

6. Dokumentation for overholdelse af Databeskyttelsesforordningen

6.1. Den enkelte institution er ansvarlig for, under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med databeskyttelsesforordningen. Foranstaltningerne skal om nødvendigt revideres og ajourføres, jf. databeskyttelsesforordningens artikel 32.

6.2. Foranstaltningerne for Styrelsen for It og Læring skal, hvis det står i rimeligt forhold til behandlingsaktiviteterne, omfatte implementeringen af passende databeskyttelsespolitikker, jf. databeskyttelsesforordningens artikel 24, stk. 2.

6.3. Styrelsen for It og Læring er ansvarlig for iagttagelse af reglen om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i databeskyttelsesforordningens artikel 25.

6.4. Den enkelte institution er ansvarlig for at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at institutionens behandling af oplysningerne er i overensstemmelse med databeskyttelsesforordningen, jf. databeskyttelsesforordningens artikel 24, stk. 1. Dette kan eksempelvis indebære udarbejdelse af procedurer for anmodninger om indsigt eller opfyldelse af oplysningspligten.

7. Anvendelse af databehandlere og underdatabehandlere

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

7.2. Ved anvendelse af databehandlere og eventuelle 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 databehandlere, 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 databehandleraftale mellem Styrelsen for It og Læring og databehandleren, og
- At sikre, at der foreligger en gyldig underdatabehandleraftale mellem databehandleren og en eventuel underdatabehandler.

7.3. Styrelsen for It og Læring skal på anmodning fra en institution oplyse om, hvorvidt oplysningerne behandles af databehandlere og evt. underdatabehandlere.

7.4. Hvis oplysningerne behandles af databehandlere og evt. underdatabehandlere, kan Styrelsen for It og Læring efter anmodning fra institutionerne oplyse om indholdet af aftalerne.

8. Fortegnelse

8.1. Styrelsen for It og Læring er ansvarlig for at iagttage kravet i databeskyttelsesforordningens artikel 30 om fortegnelser over behandlingsaktiviteter. Dette indebærer, at Styrelsen for It og Læring fører fortegnelser over de behandlingsaktiviteter, som foretages i de pågældende systemer.

8.2. Styrelsen for It og Læring orienterer institutionerne om indholdet af ovennævnte fortegnelser.

8.3. Den enkelte institution skal – eventuelt på baggrund af indholdet i fortegnelserne hos Styrelsen for It og Læring – udarbejde egne fortegnelser over de af aftalen omhandlede behandlingsaktiviteter.

9. Behandlingssikkerhed

9.1. Styrelsen for It og Læring er ansvarlig for at iagttage kravet i databeskyttelsesforordningens artikel 32 om behandlingssikkerhed. Dette indebærer, at Styrelsen for It og Læring skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici. Dette skal ske under hensynstagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Dette indebærer, at Styrelsen for It og Læring skal foretage en risikovurdering og herefter gennemføre foranstaltninger for at begrænse de identificerede risici.

9.2. Den enkelte institution er forpligtet til at gennemføre relevante sikkerhedsforanstaltninger, som knytter sig til institutionens anvendelse af systemerne, herunder f.eks. foranstaltninger i forbindelse med den fysiske sikkerhed.

10. Anmeldelse af brud på persondatasikkerheden til Datatilsynet

10.1. Styrelsen for It og Læring er ansvarlig for efterlevelsen af databeskyttelsesforordningens artikel 33 om anmeldelse af brud på persondatasikkerheden til Datatilsynet.

10.2. Den enkelte institution er dog ansvarlig for efterlevelsen af databeskyttelsesforordningens artikel 33 om anmeldelse af brud på persondatasikkerheden til Datatilsynet, hvis et brud på persondatasikkerheden skyldes egen uberettiget anvendelse af systemet.

11. Underretning om brud på persondatasikkerheden til den registrerede

11.1. Styrelsen for It og Læring er ansvarlig for iagttagelsen af databeskyttelsesforordningens artikel 34 vedrørende underretning om brud på persondatasikkerheden til den registrerede.

11.2. Den enkelte institution er ansvarlig for iagttagelsen af databeskyttelsesforordningens artikel 34 om underretning til den registrerede om brud på persondatasikkerheden, hvis et brud på persondatasikkerheden skyldes egen uberettiget anvendelse af systemet. I et sådant tilfælde er Styrelsen for It og Læring forpligtet til at bistå institutionen med oplysninger, som er nødvendige for, at institutionen kan overholde sine forpligtelser over for den registrerede.

12. Konsekvensanalyse vedrørende databeskyttelse og forudgående høring

12.1. Styrelsen for It og Læring er ansvarlig for iagttagelsen af kravet i databeskyttelsesforordningens artikel 35 om konsekvensanalyse vedrørende databeskyttelse. Dette indebærer, at Styrelsen for It og Læring forud for behandlingen skal foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger, hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

12.2. Styrelsen for It og Læring er ligeledes forpligtet til at iagttage kravet i databeskyttelsesforordningens artikel 36 om forudgående høring af tilsynsmyndigheden, når kravet om høring finder anvendelse.

13. Overførsel af personoplysninger til tredjelande eller internationale organisationer

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

13.2. Den enkelte institution er ansvarlig for iagttagelsen af kapitel V, hvis overførslen af personoplysninger til et tredjeland eller en international organisation sker i forbindelse med institutionens anvendelse af systemet/på institutionens foranledning.

14. Klager

14.1. Styrelsen for It og Læring er ansvarlig for behandling af eventuelle klager fra registrerede, hvis klagerne omhandler overtrædelse af bestemmelser i databeskyttelsesforordningen, hvor Styrelsen for It og Læring efter denne cirkulæreskrivelse er ansvarlig.

14.2. Den enkelte institution er ansvarlig for behandling af eventuelle klager fra registrerede, hvis klagerne omhandler overtrædelse af bestemmelser i databeskyttelsesforordningen, hvor institutionen efter denne cirkulæreskrivelse er ansvarlig.

14.3. Hvis en institution eller Styrelsen for It og Læring modtager en klage, som rettelig bør behandles af den anden part, sendes klagen til den dataansvarlige snarest muligt.

14.4. Hvis en institution eller Styrelsen for It og Læring modtager en klage, hvor en del af klagen rettelig bør behandles af den anden part, sendes denne del af klagen til besvarelse hos denne part snarest muligt.

14.5. Den registrerede skal, i forbindelse med en institutions eller Styrelsen for It og Lærings oversendelse af en klage eller en del heraf til den anden part, oplyses om det væsentligste indhold af nærværende cirkulæreskrivelse.

15. Orientering af den anden part

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

16. Ikrafttræden

Denne cirkulæreskrivelse træder i kraft den 25. maj 2018.

Styrelsen for It og Læring den 24. maj 2018

Jakob Harder