DANSK OPLYSNINGS FORBUND

Info om behandling af personoplysninger og databeskyttelsesforordningen

Marts 2018

Ny Østergade 7, 1. sal
4000 Roskilde
Tlf. 70 20 60 20
www.danskoplysning.dk
post@danskoplysning.dk

Indhold

Indledning

Når EU's databeskyttelsesforordning (officielt: *Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger mv. (databeskyttelsesforordningen).*) den 25. maj 2018 afløser den danske persondatalov, er der en række regler som virksomheder skal overholde og – ikke mindst – dokumentere, at de overholder.

For at hjælpe skolerne med at overholde de kommende regler, har vi i DOF udarbejdet dette skriftlige materiale, som i skrivende stund består af flere dokumenter:

- Info om behandling af personoplysninger (dette dokument)
- Bilag: Fortegnelse over behandlingsaktiviteter
- Bilag: Persondatapolitik
- Bilag: Intern adgang til data-tjeklisten
- Bilag: Persondatasikkerhed-tjeklisten
- Bilag: Skolens databehandlere-tjeklisten
- Bilag: Databehandleraftale

På nuværende tidspunkt arbejder Folketinget og Justitsministeriet på en ny dansk databeskyttelseslov, som kan have indflydelse på forordningens fortolkning. Vores infomateriale samt de tilhørende dokumenter skal derfor betragtes som dynamiske dokumenter, som med stor sandsynlighed vil blive opdateret i løbet af året.

Det er naturligvis frivilligt for skolerne, om de vil bruge dette materiale og vores anbefalinger, men det kan ikke undgås, at skolerne på et eller andet tidspunkt bliver nødt til at forholde sig til de nye regler og krav.

For flere informationer om databeskyttelsesforordningen henviser vi til Datatilsynets hjemmeside: www.datatilsynet.dk.

Hvad er personoplysning?

Personoplysning er enhver form for information, der kan henføres til fysiske personer.

Der er to hovedtyper af personoplysninger med relevans for aftenskolernes virke: Følsomme personoplysninger og Almindelige personoplysninger.

Følsomme personoplysninger:

Race, etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger, seksuelle forhold, seksuel orientering.

Almindelige personoplysninger:

Alle personoplysninger som ikke er følsomme eller ikke relateres til oplysninger om strafbare forhold.

F.eks.: økonomi, skat, gæld, sygedage, CV, navn, adresse, telefonnr., fødselsdato, stilling, familieforhold, bil, ansættelsesdato osv. Personbilleder anses også som værende en alm. personoplysning.

CPR

CPR-nr. er ikke omfattet af forordningen og her gælder det samme regler som hidtil. Da CPR ikke hører under kategorien ”Følsomme oplysninger”, kan det jf. Persondatalovens §11 behandles, hvis det følger af lov eller bestemmelser fastsat i henhold til lov. Dette gælder f.eks. kommunale krav om CPR på udenbys deltagere eller CPR-krav omfattet af skattelovgivningen.

CPR må også gerne behandles, hvis den registrerede har givet sit udtrykkelige samtykke hertil.

Behandling af personoplysninger i aftenskolerne

Hvad er Behandling?

Begrebet ”behandling” omfatter enhver form for håndtering af personoplysninger. Det er først og fremmest elektronisk behandling af oplysninger, der er omfattet af reglerne. Det kan f.eks. være indsamling, registrering, systematisering, opbevaring, søgning, brug, videregivelse eller sletning af oplysninger.

Det betyder bl.a., at en virksomhed eller privat person, der kun stiller en server (computer) til rådighed, som oplysningerne opbevares på, også foretager en behandling af oplysningerne ved at opbevare dem.

Behandling kan også være offentliggørelse af oplysninger på en hjemmeside eller registrering af oplysninger i et IT- administrationssystem.

Hvornår må skolen behandle personoplysninger?

Regler om behandlinger er i princippet ret skønsmæssige, og det er i det sidste ende op til skolen selv at vurdere, om skolen har ret til at behandle (bestemte) personoplysninger.

Hovedreglen er dog:

- At der skal foreligge *saglige formål* med behandlingen.

Derudover anses behandlingen for lovlig (jf. Artikel 6) hvis ét af følgende er gældende (forkortet jf. relevans for aftenskoler):

a) Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.
b) Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.
c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
…
f) Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

Selvom samtykke (pkt. a) kan virke som den nemme måde at få behandlingshjemmel, er det for de fleste aftenskolens aktiviteter overflødig, idet behandlingen i langt de fleste tilfælde hører under pkt. b – opfyldelse af kontrakt (f.eks. kursustilmelding), samt pkt. f – interesseafvejning, hvor skolens saglige formål med behandlingen vejer tungere end evt. modstående hensyn til den registrerede.

Registrering af deltagere relateres nemlig til eksplicitte krav i Folkeoplysningsloven og de kommunale retningslinjer og er nødvendigt for at kunne administrere aktiviteter, herunder tilmeldinger, faktureringer, tilskudsafregning mm.

Samtykke kan dog bruges i visse tilfælde, hvor ovenstående ikke er dækkende. Det kan f.eks. være ved udsendelse af nyhedsbreve, åbne spørgeskemaer, indsamling af ekstra personoplysninger mm. Se mere om samtykke senere i artiklen.

For undervisere og skolens personale er det pkt. c, som er relevant, idet det relateres til f.eks. skattelovgivningen og skatteindberetning.

Formål med behandlingen kan med fordel specificeres i skolens persondatapolitik (se bilaget forslag til Persondatapolitik), som skal offentliggøres på skolens hjemmeside.

Hvilke personoplysninger må skolen behandle?

Hovedreglen her er:

- At behandlingen begrænses til de personoplysninger, som er *nødvendige* for at opfylde *formålet*.

Her er det tale om reglen om dataminimimering, som skal sikre, at virksomheden kun har adgang til de personoplysninger, som sagligt er nødvendige for at levere ydelsen og efterleve lovgivningen.

Folkeoplysningsloven og de kommunale retningslinjer omtaler normalt følgende personoplysninger, som skolerne med sikkerhed må behandle: navn og efternavn, adresse, fødselsdato, telefonnummer, kommunal tilknytning (herunder handlekommune, betalingskommune, opholdskommune), CPR-nr. for udenbys deltagere mm.

For at kunne levere ydelsen (f.eks. kursusmateriale, informationer om et hold, tilmelding, aflysning mm.) kan det også være nødvendigt med en e-mailadresse og mobiltelefonnummer.

Derudover kræver kommuner i nogle tilfælde, at skolen indsamler Tro og Love-erklæringer (handicaperklæringer), som kan indeholde yderligere personoplysninger, herunder følsomme personoplysninger.

Behandling af alle disse personoplysninger, som enten har hjemmel i lovgivningen (inkl. de kommunale krav) eller er nødvendige for konkret levering af ydelsen, er lovlige jf. pkt. b og f i forordningens artikel 6.

I forhold til undervisere og skolens personale kan personoplysninger også inkludere CPR, ansættelsesforhold, løn mm. med hjemmel i skattelovgivningen. Som noget særligt skal der også indhentes børneattester for undervisere, der har med børn og unge under 15 år at gøre.

Skolen skal dog være opmærksom på, om der indsamles yderligere informationer, som skolen ikke umiddelbart har behandlingshjemmel til. I nogle tilfælde kan man bruge samtykke, mens det i andre tilfælde er bedst at stoppe med at behandle disse unødvendige oplysninger. Et eksempel kan være indsamling af CPR-nr., selvom det ikke er påkrævet i lovgivningen, eller informationer om ens køn, arbejdsforhold mm., selvom dette ikke er nødvendigt for kursusdeltagelse.

Hvor længe må skolen opbevare personoplysningerne?

Som udgangspunkt skal personoplysningerne slettes eller anonymiseres, når de ikke længere er nødvendige for opfyldelsen af det formål, som de oprindeligt er indsamlet til. Det er dog op til skolen selv at vurdere, hvornår det er.

Her skal man være opmærksom på, at modtagelse af tilskud jf. Folkeoplysningsloven berettiger kommuner til at udføre kontrol med tilbagevirkende kraft, samt at Bogføringsloven kræver opbevaring af regnskabsmaterialet i 5 år. Det betyder i praksis, at personoplysningerne passivt kan opbevares i maksimalt 5 år.

Hvordan skal skolen opbevare personoplysningerne?

Opbevaring og behandling af personoplysninger skal foregå betryggende og med et passende niveau af sikkerhed og privatlivsbeskyttelse. Det betyder bl.a.:

- **Det er kun betroede personer med saglige formål, der kan have adgang til personoplysninger.**
  Her skal man vurdere, om f.eks. en skoles bestyrelse har et sagligt formål med at få indsigt i deltagernes personoplysninger, eller om de kan nøjes med at have adgang til statistiske data (se bilaget Intern adgang til data-tjeklisten).
- **Sikkerhed skal være i orden.**
  I praksis betyder det, at pc'er og andre elektroniske medier, hvor der opbevares personoplysninger, skal beskyttes med stærke password, antivirus og firewall, at kommunikation via hjemmesider skal være krypteret osv. (se bilaget Persondatasikkerhed-tjeklisten)
  Ved sikkerhedsbrud skal bestemte regler og retningslinjer følges. Se senere i artiklen.
- **Lav databehandleraftaler**
  Når man outsourcer opbevaring af personoplysninger til en tredje part (f.eks. hostingvirksomhed eller cloud-baserede løsninger), skal der underskrives en databehandleraftale (se bilaget Databehandleraftale), som bekræftelse for, at udbyderen kan garantere den nødvendige sikkerhed.

Sikkerhedsniveauet skal i praksis afspejle den konkrete risiko for, at oplysningerne stjæles, mistes, eller behandles ulovligt.

Hvad skal deltagere informeres om?

Databeskyttelsesforordningen giver de registrerede en række rettigheder om forskellige aspekter af behandlingen af personoplysninger. Formålet er at skabe åbenhed omkring behandlingen af personoplysninger. Disse rettigheder er:

- **Retten til at modtage oplysning om en behandling af sine personoplysninger (*oplysningspligt*).**
  Den registrerede (f.eks. deltageren) skal gøres opmærksom på, at der behandles personoplysninger om vedkommende. Den registrerede har ret til at vide, hvem dataansvarlig er, hvad formålet med behandlingen er, hvem modtager oplysningerne mm.
- **Retten til at få indsigt i sine personoplysninger (*indsigtsret*).**
  Den registrerede kan kræve at få indsigt i de oplysninger om den pågældende selv, som skolen behandler. Dette gøres ved at udlevere en udskrift eller en elektronisk kopi af oplysningerne.
- **Retten til at få urigtige personoplysninger berigtiget (*retten til berigtigelse*).**
  Hvis der behandles forkerte oplysninger om en person, kan den pågældende bede om at få oplysningerne rettet.
- **Retten til at få sine personoplysninger slettet (*retten til at blive glemt*).**
  I visse tilfælde har den registrerede ret til at få egne personoplysninger slettet. Det kan f.eks. være, hvis oplysningerne ikke længere er nødvendige til at opfylde de formål, hvortil de blev indsamlet, eller hvis et samtykke trækkes tilbage. Skolen kan dog fortsætte med at behandle oplysningerne, hvis der er et lovligt grundlag – f.eks. kommunalt krav om passiv opbevaring af data eller af hensyn til kravene i bogføringsloven.
- **Retten til at gøre indsigelse**
  Den registrerede har ret til at gøre indsigelse mod, at personoplysninger anvendes til bl.a. direkte markedsføring og profilering. Dette anser vi ikke som relevant for aftenskoler.
- **Retten til at flytte sine personoplysninger (*dataportabilitet*).**
  Den registrerede har ret til at modtage personoplysninger om sig selv i et struktureret, almindeligt anvendt og maskinlæsbart format. Selvom det nok ikke er relevant for aftenskolerne, så kan en deltager i princippet bede skolen om at få overført egne personoplysninger til en anden skole.

Hvis en person henvender sig til skolen med hensyn til en eller flere af ovenstående rettigheder, skal henvendelsen besvares senest en måned efter, den er modtaget. Besvarelse og opfyldelse af disse rettigheder skal være kortfattet, letforståeligt og i klart og enkelt sprog.

Hvad er Dataansvarlig og Databehandler?

Databeskyttelsesforordningen introducerer to hovedbegreber: Dataansvarlig og Databehandler.

Jf. Databeskyttelsesforordningens art. 4, nr. 7 og nr. 8 defineres Dataansvarlig som: ”*en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger*.”

Og en Databehandler som: ”*en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne*”.

Selvom sondringen mellem disse to begreber ikke er entydig, så er rollefordelingen ret essentiel, idet det er den Dataansvarlige, der primært har ansvar for, at persondatabehandlingen lever op til reglerne i databeskyttelsesforordningen.

En aftenskole har brug for at registrere deltagernes data (navn, adresse, fødselsdato osv.) for at kunne foretage en kursustilmelding og opkrævning – både ved lov (folkeoplysningsloven, skatteloven og de kommunale bestemmelser) og som nødvendigt for at levere en ydelse (kursus). Skolen råder hermed over et klart *formål* med behandlingen af personoplysninger samt viden om, *hvordan* oplysningerne skal behandles. Skolen er derfor den Dataansvarlige.

Når aftenskolen bruger elektroniske hjælpemidler (programmer, cloud løsninger, apps osv.) til registrering og opbevaring af persondata, og disse hjælpemidler er outsourcet til (hostet af) en anden virksomhed, så vil denne virksomhed agere databehandler.

Når aftenskolen bruger DOFPro, VuptiWeb, Lønbehandling mm., som udvikles, hostes og ejes af Dansk Oplysnings Forbund, så har skolen rollen som Dataansvarlig og DOF som Databehandler.

Som dataansvarlig kan aftenskolen uddelegere visse beslutninger til skolens databehandler (DOF), f.eks. hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe den nødvendige datasikkerhed. Der kan også gives en generel godkendelse til at benytte underdatabehandlere.

For at lovliggøre denne rolleopdeling mellem Dataansvarlig og Databehandler er det nødvendigt med at lave en *databehandlingsaftale*. Denne aftale vil indeholde klare retningslinjer for, hvordan Databehandleren skal behandle (opbevare) aftenskolens persondata. At en anden virksomhed er databehandler betyder bl.a., at virksomheden ikke må behandle aftenskolens persondata til egne eller andre formål som ikke er aftalt med skolen.

Se DOF’s databehandleraftale mellem DOF og DOF’s aftenskoler i bilaget Databehandleraftale. Se også bilaget Skolens databehandlere-tjeklisten.

Fortegnelser over behandlingsaktiviteter

Dataansvarlig og Databehandleren skal i visse tilfælde føre en fortegnelse over deres behandling af personoplysninger. Det er pt. stadigvæk lidt uklart, om foreningerne er underlagt dette krav, men da fortegnelsen i bund og grund er et lille dokument, som i klart sprog beskriver, hvordan personoplysningerne konkret behandles, er det vores anbefaling, at skolerne fører en intern fortegnelse.

Fortegnelsen indeholder konkrete informationer om, hvem dataansvarlig er, hvad formål med behandlingen er, hvilke personer og personoplysninger behandles mm. I bund og grund skal fortegnelsen ses som en vigtig og lettilgængelig dokumentation for skolens overholdelse af databeskyttelsesforordningen.

Skolen skal dog sørge for at vedligeholde fortegnelsen og naturligvis følge de beskrevne principper.

Vi har (se bilaget Fortegnelser over behandlingsaktiviteter) udarbejdet to eksempler på fortegnelser, som skolen kan bruge, som de er, eller som inspiration til skolernes egne fortegnelser. Fortegnelser skal naturligvis afspejle skolens virkelighed.
Som supplement til fortegnelsen har vi også udarbejdet en datasikkerheds-tjekliste (bilaget Persondatasikkerhed-tjeklisten).

Bortset fra at fortegnelsen skal foreligge skriftligt og elektronisk, så er der ingen yderligere formkrav. Fortegnelsen kan derfor være et alm. tekstdokument, Excel regneark, et skema osv.

Fortegnelsen er et internt dokument, og det er kun, når Datatilsynet anmoder om det, at fortegnelsen skal udleveres.

Samtykke

Vi anbefaler generelt, at skolerne ikke bruger samtykker, medmindre det er absolut nødvendigt. Som beskrevet ovenfor, så har skolerne allerede behandlingshjemmel for de fleste af skolens aktiviteter.

Men i nogle tilfælde og efter grundige overvejelser kan det være nødvendigt med at formulere og indhente samtykke. Et eksempel kunne være tilmelding til nyhedsbrev eller offentliggørelse af underviserens billede på skolens hjemmeside. I praksis kan man give samtykke til behandling af personoplysninger, uanset hvilke oplysninger det drejer sig om.

Der er dog nogle regler vedr. samtykker, som vi hurtigt vil gennemgå her:

Tidspunkt

Et samtykke skal indhentes, før databehandlingen finder sted.

Form

Et samtykke kan både afgives mundtligt, skriftligt og digitalt. Skolen skal dog kunne bevise, at der er givet samtykke. Det er nemlig skolen som den dataansvarlige, der har bevisbyrden.

Normalt vil man indhente samtykke ved at placere et afkrydsningsfelt eller knap på hjemmesiden, hvor besøgende skal klikke på "Ja" for at komme videre. IT-Systemet skal kunne registrere tidspunktet og formen (f.eks. 11-12-2017 23:00, Hjemmesiden).

Tilbagekaldelse

Den registrerede skal på et hvilket som helst tidspunkt kunne trække sit samtykke tilbage på en enkel og lettilgængelig måde. Det skal være lige så let at tilbagekalde sit samtykke som at give det, men det er ikke et krav, at tilbagekaldelse skal ske på samme måde, som samtykke oprindeligt er givet. Det er et krav, at den registrerede, inden samtykke gives, skal oplyses om, at samtykket kan tilbagekaldes.

I praksis betyder det, at tilbagekaldelse skal ske på tilnærmelsesvist samme måde som det er afgivet og med ligeså meget/lidt besvær. Samtykke givet via en mail kan f.eks. tilbagekaldes via en mail. Samtykke givet ved et "ok" på en hjemmeside kan tilbagekaldes ved et klik på en (men ikke nødvendigvis samme) hjemmeside. Det er f.eks. ikke lovligt at give "flueben" samtykke og så kræve, at den kun kan tilbagekaldes ved at ringe til kontoret.

Tilbagekaldelse af samtykke vedrører kun den fremtidige behandling af den registreredes oplysninger og har ingen indflydelse på behandlingen, inden samtykket er tilbagekaldt. Hvis behandlingen af oplysninger alene hviler på det afgivne samtykke, bør oplysningerne slettes (idet opbevaring sidestilles med behandling).

Oplysningerne kan godt behandles (gemmes), efter samtykke er tilbagekaldt, hvis det sker på et andet lovligt grundlag. Det kan f.eks. være bogføringspligt, hvor informationerne skal gemmes i en periode.

Frivilligt

Et samtykke skal være frivilligt. Det er tale om reelt og frit valg, så længe et nægtet samtykke ikke medfører negative konsekvenser.

Et samtykke anses ikke for at være givet frivilligt, hvis f.eks. tilmelding til et kursus afhænger af samtykke, selvom et sådant samtykke ikke er nødvendigt for kursusdeltagelse. Et godt eksempel er samtykke til nyhedsbrev i forbindelse med

kursustilmeldingen. Sådan et samtykke bør være frivillig og ikke betinge selve tilmeldingen.

Et andet eksempel kan være offentliggørelse af undervisernes billeder på hjemmesiden, hvilket kræver et samtykke. Samtykket vil ikke være frivilligt, hvis undervisere får oplyst, at det kan have negative ansættelsesrelaterede konsekvenser, hvis de siger nej.

Specifikt

Et samtykke skal være specifikt med en præcis angivelse af formålene med behandlingen af personoplysninger.

Hvis en indhentning af oplysninger via samtykke tjener flere formål, skal skolen indhente særskilt samtykke for hvert enkelt formål. Et samtykke for skolens nyhedsmail kan f.eks. ikke bruges som et samtykke til modtagelse af nyhedsmails fra forbundet. I praksis kan det klares ved, at man har flere afkrydsningsfelter i tilmeldingsformularen, eller at man laver en samlet erklæring, hvor den registrerede kan markere, til hvilke formål oplysningerne må behandles.

Informeret

Af samtykketeksten skal det klart og tydeligt fremgår, hvad der gives samtykke til. Derudover skal skolen som minimum informere den registrerede om:

- Den dataansvarliges (skolens) identitet (Navn, Adresse, kontaktinfo, CVR mm.).
- Formål med behandlingen (f.eks. deltagelse i konkurrencen).
- Hvilke oplysninger der behandles (Navn, e-mail mm.)
- Hvilken behandling der finder sted.
- Info om tilbagekaldelse (hvordan det kan ske).

Utvetydig viljestilkendegivelse og passivitet

Utvetydig viljestilkendegivelse betyder, at det givne samtykke ikke må give anledning til tvivl, og at det er et produkt af en aktiv handling fra den registreredes side. Passivitet f.eks. i form af på forhånd afkrydsede felter eller inaktivitet på hjemmesiden kan ikke betragtes som utvetydig viljestilkendegivelse, og kan derfor ikke udgøre et samtykke.

Utvetydig viljestilkendegivelse kan f.eks. være underskrift på et dokument, aktiv afkrydsning af et felt på hjemmesiden, klik på ”Send” i et skema, hvis det klart fremgår, at klik på ”Send” er lige med samtykke.

Brud på persondatasikkerheden

Som noget nyt i Danmark, så vil der efter 25. maj 2018 gælde to generelle forpligtelser:

1. Forpligtelse at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet).
2. Forpligtelse at underrette de registrerede i tilfælde af brud på persondatasikkerheden.

Se venligst bilaget Brud på persondatasikkerheden for uddybende forklaring.

Yderligere informationer kan indhentes i Datatilsynets Vejledning om håndtering af brud på persondatasikkerheden (februar 2018), samt lovteksten i databeskyttelsesforordningens kapitel IV, afdeling 2 og afsnittene 5.11. og 5.12. i betænkning nr. 1565/2017 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning.