VEJLEDNING TIL FRIE SKOLER

BESKYTTELSE *af* PERSONDATA

2. udgave

Danmarks Private Skoler grundskoler & gymnasier
efterskolerne
FRISKOLERNE
Højskolerne
Foreningen af Kristne Friskoler

Denne vejledning er 2. udgave af de frie skoleforeningers vejledning til skolerne om beskyttelse af persondata.

Danmarks Private Skoler
grundskoler & gymnasier

efterskolerne

FRISKOLERNE

HØJSKOLERNE

Foreningen af
Kristne Friskoler

Redaktion:
Dzenana Causevic og Peter Højgaard Pedersen (Dansk Friskoleforening), Thomas Sørensen og Nicolas No Richter (Danmarks Private Skoler), Viggo Mellerup (Foreningen af Folkehøjskoler i Danmark), Mette Hjort-Madsen (Efterskoleforeningen)

Redaktionen er afsluttet i juni 2019

Illustrationer: Stig Spangsberg
Forside, design og grafisk tilrettelæggelse: Signe Bjerregaard, Kabus

INDHOLD

1

Indledning

Databeskyttelsesloven stiller krav til skolens it og organisation

I maj 2018 trådte EU's forordning om beskyttelse af persondata[1] i kraft. Forordningen har medført øgede krav til it- og databehandlingssikkerhed i institutioner og virksomheder, ligesom borgerne har fået styrkede rettigheder ift. egne oplysninger.

I Danmark er forordningens regler indarbejdet i Databeskyttelsesloven[2].

De frie skoleforeninger udarbejdede den første udgave af denne vejledning i efteråret 2017. Hensigten var at støtte skolerne i arbejdet med at sikre overholdelse af de nye regler i den daglige administration.

Forordningen og Databeskyttelsesloven har nu været i kraft i et års tid. Datatilsynet har siden udgivet en række supplerende vejledninger, som er indarbejdet i denne opdaterede udgave af vejledningen.

I denne vejledning anvendes begrebet persondatareglerne for det samlede regelsæt.

Det er skoleforeningernes vurdering, at de fleste skoler siden forordningens ikrafttrædelse har arbejdet med overholdelse af reglerne ift. oplysningspligt og samtykke. Mange skoler har også taget stilling til sletning af oplysninger om elever og medarbejdere. Undervisningsministeriets seneste undersøgelse af skolernes overholdelse af de nye regler viser også, at administrationerne i stort omfang har styr på reglerne. Men der er fortsat usikkerhed ifm. medarbejdernes behandling af elevernes data, herunder brug af gratis APPs.

Skolerne har som dataansvarlige pligt til at sikre, at oplysninger om elever og medarbejdere ikke utilsigtet fortabes, forringes, misbruges eller bringes til uvedkommendes kendskab. Det kræver gode it-løsninger med gennemtænkte og sikre arbejdsgange.

Vi har endnu ikke haft konkrete klagesager, som er blevet afgjort i Datatilsynet. Kommer sådanne sager i fremtiden, kan afgørelserne få betydning for fortolkningen af reglerne. I så fald kan retningslinjerne i denne vejledning blive justeret.

(1) EU General Data Protection Regulation (2016/679)
(2) Lov nr. 502 af 23. maj 2018.

1.1 Ændringer siden første udgave og status på databeskyttelse

De væsentligste tilføjelser og rettelser i vejledningen omhandler følgende temaer:

- CPR-nummer er en særlig oplysningskategori, som det kræver lovhjemmel eller samtykke at behandle.
- Alle virksomheder har pligt til at anvende 'sikker mail', hvis de behandler følsomme eller fortrolige personoplysninger, herunder CPR-nummer, via mail.
- Krav til databehandleraftaler: Hvem skal skolen have databehandleraftaler med, og hvad skal aftalerne indeholde?
- Krav til risiko- og konsekvensanalyser (ikke lovpligtigt for frie skoler).

1.2 Persondatareglerne kort fortalt

Det er vigtigt at understrege, at det er en stor og krævende opgave at sikre overholdelse af reglerne om databeskyttelse. Det betyder, at opgaven skal have ledelsens bevågenhed, og at ledelsen bør involvere sig løbende i arbejdet.

Persondatareglerne stiller en række krav til skolerne, som bl.a. handler om overblik og dokumentation. Det vil sige, at I skal have overblik over hvilke data, I behandler på skolen, og hvordan I behandler dem. Overblikket skal I dokumentere skriftligt og opbevare på skolen.

Hvis I undervejs i forløbet finder nogle områder, hvor I ikke lever op til kravene, f.eks. fordi I ikke har fået samtykke til behandling af oplysningerne, eller jeres it-sikkerhed er for dårlig, så skal I udbedre dette.

Reglerne om databeskyttelse er en god anledning til at løbe jeres arbejdsgange og it-systemer igennem for at tjekke, om noget kan gøres smartere eller mere sikkert. Afhængig af udgangspunktet kan det kræve en væsentlig indsats og nye investeringer i stabile og sikre it-systemer.

Endelig er det en god ide, når man leder efter leverandører af it-services, at holde øje med, om leverandøren lever op til forordningens krav til databehandlere og herunder, at de er villige til at overholde de krav, som Datatilsynet stiller til databehandleraftaler.

Læs mere her:
www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/

1.3 Fire-trinsmodel

I korte træk anbefaler skoleforeningerne en Fire-trinsmodel i arbejdet med at sikre, at skolen lever op til kravene i persondatareglerne:

1 Gennemgå og registrér datastrømme på skolen: Hvilke oplysninger behandler I, og hvordan behandler I dem? I denne sammenhæng er det vigtigt, at I også har blik for, om der er oplysninger, som indebærer en særlig høj risiko for de registrerede. Det vil oftest være følsomme oplysninger om helbred og/eller rent private forhold som f.eks. skilsmisse, misbrug, overgreb, etc. Registreringen kaldes en fortegnelse og skal opbevares på skolen.

2 Gennemgå skolens databehandlingssystemer, både fysiske og digitale, og indgåede aftaler om databehandling (skab overblik over leverandører og tjenester på it-området). Vurdér om I har tilstrækkelige sikkerhedsforanstaltninger i alle led af behandlingen. Sørg for at få indgået de fornødne databehandleraftaler, hvis de ikke allerede er indgået.

3 Identificér de områder, hvor I evt. ikke lever op til kravene i persondatareglerne og sørg for at udbedre dette.

4 Udarbejd en databeskyttelsespolitik. En databeskyttelsespolitik er en skriftlig beskrivelse af skolens praksis og retningslinjer for behandling af persondata, herunder om indgåelse af databehandleraftaler. Ofte giver det mening at formulere en ekstern politik til hjemmesiden, som suppleres af en intern medarbejderinstruks om databeskyttelse.

Når dokumentationen er udarbejdet og samlet i en databehandlingsrapport for skolen, stiller persondatareglerne krav om, at bestyrelsen årligt forholder sig til, om skolen stadig overholder kravene. Det er derfor en god idé at skrive temaet på bestyrelsens årshjul.

Skoleforeningerne har udarbejdet et værktøj, Persondatamappen, hvor skabeloner og inspiration til alle nødvendige elementer i dokumentationskravet er indarbejdet. Filen (Excel) findes på skoleforeningernes hjemmesider.

1.4 Læsevejledning

Denne vejledning er udarbejdet i samarbejde mellem de frie skoleforeninger i Danmark. Den er bygget op som et opslagsværk, hvor skolerne kan finde centrale begreber i persondatareglerne med principielle og konkrete eksempler på korrekt databehandling.

Afsnittet om begreber er struktureret efter begrebernes væsentlighed og indbyrdes sammenhæng, så det både kan læses samlet og enkeltvis.

Afsnittene om beskyttelse af hhv. medarbejderes og elevers personoplysninger er opbygget kronologisk; fra ansøgning over ansættelse/optagelse til personen forlader skolen igen. Her findes konkrete eksempler og anvisninger på god praksis.

Som bilag til vejledningen findes et værktøj i Excelformat 'Persondatamappen' til brug for bl.a. datastrøms-analyse på skolen og dokumentationsoverblik samt skabeloner til udformning af samtykkeerklæringer til elever/forældre og medarbejdere. Værktøjet kan findes på skoleforeningernes hjemmesider, hvor man bl.a. også kan finde formuleringsforslag til samtykke og oplysningspligt.

1.5 Afgrænsning af vejledningens anvendelsesområde

Denne vejledning vurderer ikke konkrete systemløsninger ift. persondatareglerne. Alle skolens aftaler med leverandører og samarbejdspartnere ift. behandling af personoplysninger skal være omfattet af databehandleraftaler. Hvorvidt konkrete systemer, software eller andre løsninger overholder persondatareglerne, bør leverandøren medvirke til at dokumentere. Vi anbefaler derfor, at man vælger en leverandør, som kan dokumentere overholdelse af kravene, særligt vedr. it-sikkerhed.

2

Persondatareglernes begreber

I dette afsnit kan du finde definitioner på en række centrale begreber i persondatareglerne.

2.1 Den registrerede

Den registrerede er den person, som personoplysningerne er knyttet til. På en skole vil det f.eks. være elever eller studerende, medarbejdere, forældre, samarbejdspartnere, mv. Hvis en person er under 18 år, er det forældremyndighedsindehaveren/-haverne, der skal give samtykke til behandling af oplysninger på den registreredes vegne. Dog bør og kan børn og unge i nogle tilfælde selv give samtykke til behandling af deres personoplysninger. Se nærmere herom i afsnit 4.2.

2.2 Dataansvarlig

Den dataansvarlige er en fysisk eller juridisk person, som f.eks. en virksomhed eller en skole, der behandler personoplysninger (såsom indsamling, registrering og videregivelse) om sine ansatte og elever, m.fl. Det er den dataansvarlige, der har ansvaret for, at personoplysningerne behandles i overensstemmelse med persondatareglernes krav, og at eventuelle databehandlere, som behandler oplysninger på den dataansvarliges vegne, overholder relevante krav til sikkerhed, mv.

Skolen har som dataansvarlig pligt til at udforme og beskrive tilstrækkelige it- og organisatoriske sikkerhedsforanstaltninger, så data ikke utilsigtet fortabes, misbruges eller kommer til uvedkommendes kendskab. Eksempler på formuleringer vedr. forretningsgange og interne retningslinjer til inspiration for denne beskrivelse kan hentes i værktøjet 'Persondatamappe' under fanebladet it- og organisatoriske sikkerhedsforanstaltninger.

2.3 Databehandler

En dataansvarlig kan overlade det til en anden at udføre den praktiske behandling af personoplysninger på sine vegne.

En databehandler kendetegnes ved kun at behandle personoplysninger på vegne af (efter instruks fra) en dataansvarlig. Det er således den dataansvarlige, der bestemmer hvilket formål, databehandlingen skal tjene og hvilke hjælpemidler, der må anvendes til behandlingen.

Databehandleren behandler aldrig personoplysninger til egne formål og må derfor ikke bruge de

tilgængelige oplysninger til andet end udførelsen af opgaven for den dataansvarlige. Det betyder, at den dataansvarlige (Skolen) er ansvarlig for behandlingen hos databehandleren. Herunder skal den dataansvarlige sikre sig, at databehandleren overholder persondatareglerne, herunder til it-sikkerhed. Den dataansvarlige skal også jævnligt føre kontrol med databehandlerens overholdelse af kravene. Forordningen kræver, at der indgås en databehandleraftale med alle databehandlere, hvor betingelserne for samarbejdet er beskrevet, jf. afsnit 2.8.

I praksis kan en databehandler f.eks. være en virksomhed, som varetager en skoles it-systemer. En databehandler kan også være en udbyder af et webhotel, der hoster hjemmesider for andre, eller et inkassobureau, som får oplysninger fra en dataansvarlig med henblik på inddrivelse af gæld.

Datatilsynet har i sin vejledning om databehandlere fastslået, at revisorer, der udfører almindelige revisionsopgaver for skolen, ikke er databehandlere, men selvstændige dataansvarlige. Det samme gælder f.eks. rejsebureauer eller andre virksomheder, der sælger en ydelse til skolen, men ikke handler efter instruks.

Skolen indberetter en række oplysninger i statslige systemer, f.eks. optagelse.dk, og deler oplysninger om elever via UNI-login. Styrelsen for It og Læring (STIL) har udarbejdet en liste med oversigt over systemansvaret for alle de fællesoffentlige systemer. Der er systemer, hvor skolen er dataansvarlig, og systemer hvor STIL er dataansvarlig, og tilfælde hvor ansvaret er delt. UNI-login er skrevet ind i bekendtgørelsen om dataansvar og er dermed undtaget fra kravet om databehandleraftale.

Se bekendtgørelsen her:
www.retsinformation.dk/Forms/R0710.aspx?id=209148

2.4 Personoplysninger

En personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person (elev, forældre, ansat, samarbejdspartner mv.).

Personen skal direkte eller indirekte kunne identificeres gennem oplysninger, som er særlige for personens identitet, som f.eks. navn, CPR-nummer, adresse eller online-identifikatorer som f.eks. IP-adresser.

Billeder fra tv-overvågningsudstyr er også persondata, som derfor er reguleret ved persondatareglerne. TV-overvågning er selvstændigt reguleret i lov om tv-overvågning.

Persondataloven skelner mellem tre kategorier af personoplysninger:

- **ALMINDELIGE OPLYSNINGER** er f.eks. navn, adresse, stilling, indkomst og formueforhold, civil stand, sygedage, tjenstlige forhold, eksamen, ansøgning, CV, strafbare forhold, væsentlige sociale problemer, andre rent private forhold, som f.eks. bortvisning fra jobbet. Disse er oplysninger, som man må behandle, hvis man har fået personens samtykke hertil, eller skolen har et sagligt og lovligt formål til behandling af oplysningerne.

- **FORTROLIGE OPLYSNINGER** er almindelige oplysninger man skal være særlig påpasselig med og som i udgangspunktet ikke må offentliggøres. Primært kan nævnes CPR-nummer som kun må behandles, hvis det kræves af loven, eller der foreligger samtykke. I tillæg hertil er der nogle almindelige oplysninger, som efter omstændighederne bør regnes som fortrolige. Det kan være strafbare forhold, formueforhold, rent interne familieforhold, mv.

- **FØLSOMME OPLYSNINGER**, er information om personen, som det ifølge forordningen er ***forbudt at registrere***. Det gælder racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, samt medlemskab af faglige organisationer og helbredsmæssige og seksuelle forhold.

  – Det er kun lovligt at behandle følsomme oplysninger, hvis der er tale om et helt specifikt formål, og personen har givet ***udtrykkeligt samtykke*** til behandling. Se mere om behandlingen af følsomme oplysninger for hhv. medarbejdere og elever nedenfor.

2.5 Behandling

Behandling er ***enhver håndtering af oplysninger***; dvs. alle de måder skolen behandler oplysninger på. Behandling er altså enhver indsamling, registrering, systematisering, opbevaring, ændring, søgning, transmission, videregivelse, sammenstilling, samkøring, blokering, sletning eller tilintetgørelse af oplysninger. Det er f.eks. registrering af ansøgere til ventelister, overførsel af oplysninger til optagelse.dk, udbetaling af løn, registrering af sygefravær, og oplysninger som personen selv indtaster på en hjemmeside.

Persondatareglerne gælder for ***alle typer af elektronisk og manuel behandling af personoplysninger*** i registerform. Det gælder bl.a. oplysninger i e-mails, indtastning i registre og økonomisystem, systemoverførsler til f.eks. optagelse.dk eller andre databaser, fysiske breve, notater fra telefonsamtaler, mv.

2.5.1 GENERELLE KRAV TIL BEHANDLING

Persondatareglerne opstiller en række generelle krav til behandling af personoplysninger. Oplysningerne skal:

- Behandles lovligt, rimeligt og på en gennemsigtig måde ift. den registrerede.
- Indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles uden særlig grund.
- Være korrekte og om nødvendigt ajourførte. Urigtige oplysninger skal slettes.
- Opbevares på en sådan måde, at man ikke kan identificere den registrerede i længere tidsrum, end det er nødvendigt til at varetage formålet med registreringen.
- Opbevares med den fornødne sikkerhed mod, at oplysningerne bliver stjålet, fortabes eller misbruges, dvs. hændeligt eller ved et uheld kommer til uvedkommendes kendskab.

2.5.2 FORMÅL MED BEHANDLINGEN

Behandlingen af personoplysninger er ***lovlig***, når den registrerede har givet sit samtykke til behandling af sine personoplysninger, ELLER mindst ét af følgende ***formål*** er opfyldt:

- Behandling er nødvendig af hensyn til opfyldelse af en ***aftale eller en kontrakt***, som den registrerede er part i. På en skole er det f.eks. en aftale om optagelse af en elev og vilkårene herfor.
- Behandling er nødvendig for at overholde en retlig forpligtigelse, som påhviler den dataansvarlige. En ***retlig forpligtelse*** er f.eks. den lovbestemte indberetning af årselevtal til Styrelsen for Undervisning og Kvalitet (STUK).
- Behandling er nødvendig for at ***beskytte den registreredes eller en anden fysisk persons vitale interesser***, som f.eks. i tilfælde med underretninger til kommunen om mistrivsel eller fare for barnets udvikling. Her er både tale om en retlig forpligtelse og hensyn til barnets vitale interesser.
- Behandling er nødvendig af hensyn til ***udførelse af en opgave i samfundets interesse*** eller som henhører under offentlig myndighedsudøvelse. Det gælder f.eks. indberetninger til Danmarks Statistik, som i øvrigt også er hjemlet i lov.
- Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en ***legitim interesse***, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder går forud herfor. Et sådant tilfælde kan f.eks. være oversendelse af en restance til et inkasso-firma.
- Behandling af ***følsomme oplysninger*** er ifølge persondatareglerne i udgangspunktet forbudt. Behandling må kun finde sted i særlige tilfælde, og kræver at der er et helt specifikt formål med behandlingen og at der foreligger et udtrykkeligt samtykke, hvor formålet med behandlingen fremgår.

2.6 Samtykke

Personen, hvis oplysninger bliver behandlet og opbevaret, skal give samtykke hertil. Samtykket kan når som helst trækkes tilbage. Samtykket er ikke længere gyldigt, hvis formålet med behandlingen af oplysninger ændrer sig, eller der slet ikke er et formål længere.

Samtykket skal være en tydelig tilkendegivelse af, at vedkommende er indforstået med behandlingen og opbevaringen. Samtykket skal være ***skriftligt*** og skal desuden være:

- ***Tydeligt adskilt fra den øvrige tekst***
  Må eksempelvis ikke være skjult som en del af teksten, skrives med småt eller lignende.

- ***Være frivilligt***
  Der skal være et reelt frit valg til afgivelse af samtykke. En aftale/kontrakt må ikke være betinget af afgivelse af samtykke til behandling af oplysninger, som ikke er nødvendige.

- ***Specifikt***
  Det skal specificeres hvilke oplysninger, der gives samtykke til behandling af.

- ***Informeret***
  Der skal gives oplysninger om, hvad samtykket indebærer, og om retten til at tilbagekalde sit samtykke.

- ***Utvetydigt/udtrykkeligt***
  Der må ikke kunne være tvivl om, hvorvidt der er afgivet samtykke til behandling af de specifikke oplysninger. Hvis man anmoder om samtykke til behandling af følsomme oplysninger, skal de specifikke formål med indsamlingen af hver enkelt oplysning fremgå af samtykket.

2.7 Den registreredes rettigheder

Den registrerede har en række rettigheder, som udmønter sig i forpligtelser for den dataansvarlige. Det vil sige, at skolen aktivt skal foretage en række handlinger for, at disse rettigheder kan siges at være opfyldt.

2.7.1 OPLYSNINGSPLIGT VED INDSAMLING AF PERSONOPLYSNINGER HOS DEN REGISTRERETE

Oplysningspligten, dvs. pligten til at oplyse personen om behandlingen af personoplysninger, er forskellig afhængigt af, om oplysningerne kommer fra personen selv eller en tredjepart. Oplysningspligten i de tilfælde, hvor oplysningerne indhentes hos tredjepart, behandles i afsnit 2.7.2.

Hvis skolen indsamler personoplysninger om en person fra personen selv, skal skolen på det tidspunkt, hvor oplysningerne indsamles, oplyse den registrerede om en række forhold.

Skoleforeningerne har udarbejdet to skabeloner til hhv. elever/forældre og medarbejdere med følgende elementer, som skolen skal oplyse om:

- Identitet på og kontaktoplysninger på skolen og eventuelle repræsentanter.

- Formålene med den behandling, som personoplysningerne skal bruges til og det retlige grundlag for behandlingen, f.eks. hvis behandlingen er nødvendig for at opfylde en kontrakt.

- De legitime interesser, som skolen eller en tredjepart forfølger, f.eks. hvis skolen videregiver oplysninger til kommunen i forbindelse med en underretning eller til et inkassofirma til brug for indkrævning af restancer.

- Eventuelle modtagere eller kategorier af modtagere af personoplysninger.

- Hvor skolen har tænkt sig at overføre personoplysninger til et tredjeland (land uden for Europa), f.eks. en rejsearrangør i udlandet.

- Det tidsrum, hvori personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier der anvendes til at fastlægge dette tidsrum.

- Retten til at anmode skolen om indsigt i, berigtigelse eller sletning af personoplysninger eller begrænsning af behandling (blokering) i en periode.

- Retten til at trække et samtykke tilbage på ethvert tidspunkt.

- Om meddelelse af personoplysninger er lovpligtigt eller et krav iht. en kontrakt, herunder betingelser for at indgå en kontrakt. Desuden skal der oplyses om konsekvenserne ved ikke at give disse oplysninger.

- Hvis skolen har tænkt sig at bruge oplysningerne til andet formål end det, hvortil de er indsamlet, skal dette andet formål oplyses.

– GDPR I PRAKSIS –

Samtykke eller oplysning?

Samtykke til behandling af oplysninger skal indhentes, når der ikke findes anden lovhjemmel til skolens behandling af oplysningen. Det gælder særligt elevernes helbredsoplysninger og deling af billeder på internettet.

Hvis man allerede har en hjemmel til behandlingen, f.eks. opbevaring af oplysninger i fem år med henvisning til bekendtgørelser om regnskab og revision, er det tilstrækkeligt at oplyse den registrerede om det på tidspunktet for indsamlingen. Her er det altså ikke nødvendigt at bede om samtykke til opbevaringen.

Hvis man indsamler CPR-nummer i forbindelse med indskrivning på skolens venteliste, skal der indhentes samtykke med det samme, da der ikke er lovkrav om brug af CPR-nummer i forbindelse med ventelister.

Hvornår gælder der ikke oplysningspligt?
Hvis den registrerede allerede er bekendt med oplysningerne, f.eks. via bestemmelser i aftalevilkårene. Her gælder det dog, at man hellere må oplyse en gang for meget end en gang for lidt. Skolen skal også være opmærksom på, at samtykket ikke 'gemmes væk' f.eks. i bilag til en optagelsesskrivelse.

2.7.2 OPLYSNINGSPLIGT – NÅR PERSONOPLYSNINGER IKKE ER INDSAMLET HOS DEN REGISTRERETE

Hvis skolen ikke indsamler personoplysninger om en person fra personen selv, men oplysningerne kommer fra f.eks. en børnehave, en kommunal sagsforvaltning eller andre, skal skolen oplyse om de samme forhold som ovenfor. Derudover skal skolen give oplysning om:

- De berørte kategorier af personoplysninger, f.eks. hvorvidt det er almindelige oplysninger eller følsomme oplysninger, som skolen har modtaget om den registrerede.

- Hvilken kilde personoplysningerne kommer fra, og eventuelt hvorvidt de stammer fra offentligt tilgængelige kilder.

Det er et krav i loven, at skolen oplyser om behandlingen indenfor en rimelig frist efter indsamlingen af personoplysningerne og senest indenfor en måned.

Hvis skolen skal bruge personoplysningerne til at kommunikere med den registrerede, skal skolen opfylde sin oplysningspligt senest på tidspunktet for den første kommunikation med den registrerede, eller når personoplysningerne skal videregives første gang til en anden modtager.

Hvornår gælder der ikke oplysningspligt?
Ved indsamling hos andre end den registrerede gælder oplysningspligten ikke, hvis den registrerede allerede er bekendt med oplysningerne, men derudover har skolen heller ikke oplysningspligt såfremt:

- At det viser sig umuligt eller vil kræve en uforholdsmæssig stor indsats, f.eks. hvis skolen ikke kan finde frem til kontaktoplysninger på den registrerede. Et eksempel kan f.eks. være en forælder uden dansk CPR-nr., som er flyttet til udlandet.

– GDPR I PRAKSIS –

Opfyldelse af oplysningspligten

For at oplysningspligten er overholdt, skal oplysningerne formidles til den registrerede i et letforståeligt sprog, på en nem tilgængelig og gennemsigtig måde. Man må ikke gemme oplysningerne bag en lang række af links eller ved på fysisk kopi at henvise til et websted, som læseren ikke kan tilgå fra dokumentet.

Mange skoler har digitale tilmeldingsværktøjer, hvor forældre kan tilmelde sig en venteliste eller søge om optagelse på skolen med det samme. Her kan man f.eks. opfylde oplysningspligten ved, at systemet 'tvinger' folk til at scrolle gennem beskrivelsen, eller man kan indsætte de væsentligste elementer i teksten og herefter en 'klik-boks' sammen med et link til skolens databeskyttelsespolitik, hvor skolens behandling og den registreredes rettigheder er beskrevet mere udførligt.

- Hvis indsamling eller videregivelse er udtrykkeligt fastsat i lovgivningen.

- Hvis personoplysningerne skal forblive fortrolige som følge af tavshedspligt, herunder lovbestemt tavshedspligt. Et eksempel kan f.eks. være oplysninger om overgreb mod en elev begået af en tredjepart.

2.7.3 INDSIGTSRET *(på forespørgsel)*

Den registrerede har ret til at få bekræftelse på, om personoplysninger vedr. den pågældende behandles og i givet fald få adgang til sine personoplysninger. Der er ingen formkrav til et krav om indsigt i egne personoplysninger. Retten gælder 'alle behandlinger af oplysninger om mig'. Dog skal skolen sikre sig, at indsigten gives til rette vedkommende. Det vil sige personen selv, eller, når der er tale om børn, indehavere af forældremyndigheden over barnet. Personoplysninger om andre end den registrerede må i udgangspunktet ikke udleveres.

Den registrerede har ret til at få indsigt i følgende elementer af behandlingen:

- Formålene med behandlingen.

- De berørte kategorier af personoplysninger.

- De modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til.

- Opbevaringsperiode og hvis ej muligt kriterierne derfor.

- Retten til at anmode om berigtigelse eller sletning, begrænsning og retten til at gøre indsigelse.

- Retten til at klage til Datatilsynet.

- Tilgængelig information om kilderne til oplysningerne.

- Oplysninger om overførsler til tredjelande.

- Ret til at få kopi af oplysningerne. Kun ved gentagen eller åbenbart grundløs indsigtsanmodning er skolen berettiget til at tage et mindre gebyr for at imødekomme indsigtsbegæringen, og gebyret skal modsvare de reelle omkostninger ved kopieringen.

Undtagelser fra indsigtsretten

Det er kun registrerede, der kan anmode om indsigt i egne oplysninger (bortset fra forældremyndighedsindehaveres anmodning på børns vegne). Men oplysninger om den registrerede kan godt omfatte oplysninger om andre, f.eks. om forfatter til oplysningen, klagers identitet i klagesager, etc.

Kun i særlige tilfælde kan det være nødvendigt at undtage personoplysninger om andre fra indsigtsretten. Det kan komme på tale, f.eks. i en klagesag, hvis der er afgørende hensyn til private interesser, som fordrer beskyttelse af tredjeparts identitet.

Forældres ret til indsigt er også behandlet i afsnit 4.2.2.

2.7.4 RET TIL BERIGTIGELSE

Den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af skolen uden unødig forsinkelse, dvs. hurtigst muligt og indenfor 1 måned.

Under hensyntagen til formålene med behandlingen, har den registrerede ret til at få ufuldstændige personoplysninger gjort fuldstændige, bl.a. ved at fremlægge en supplerende erklæring.

2.7.5 RETTEN TIL SLETNING *(Retten til at blive glemt)*

Den registrerede har ret til at få personoplysninger om sig selv slettet af skolen uden unødig forsinkelse. Skolen har pligt til at slette personoplysninger uden unødig forsinkelse, hvis et af følgende forhold gør sig gældende:

- Den registrerede trækker sit samtykke tilbage, og der ikke er et andet retsgrundlag for behandlingen.
- Dataene ikke længere er nødvendige til det oprindelige formål.
- Den registrerede gør indsigelse mod behandlingen, og der ikke foreligger legitime grunde til behandlingen, som går forud for indsigelsen.
- Behandlingen har været ulovlig.
- Sletteplig følger af lov.

Skolen bør som dataansvarlig udarbejde en slettepolitik, hvoraf det fremgår, hvor længe de forskellige oplysninger opbevares og til hvilke formål. Slettepolitikken bør opbevares sammen med skolens øvrige databeskyttelsespolitikker.

Skoleforeningerne har udarbejdet en oversigt over sletteplig ift. forskellige oplysninger, som kan findes på foreningernes hjemmesider.

Hvornår kan der undtages fra retten til sletning?

- For at udøve retten til ytrings- og informationsfrihed.
- For at overholde en retlig forpligtigelse.
- For at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse.
- For at retskrav kan fastlægges, gøres gældende eller forsvares, f.eks. i afskedigelsessager.

2.7.6 RET TIL BEGRÆNSNING AF BEHANDLINGEN

Den registrerede har ret til fra skolen at opnå begrænsning af behandlingen, hvis et af følgende forhold gør sig gældende:

- Rigtigheden af personoplysningerne bestrides af den registrerede. Da skal behandlingen begrænses i perioden indtil, at skolen har muligheden for at fastslå, om personoplysningerne er korrekte.
- Behandlingen er ulovlig, og den registrerede modsætter sig sletning og i stedet anmoder om begrænset anvendelse af sine personoplysninger (red.: Disse tilfælde er svære at forestille sig i praksis).
- Skolen ikke længere har brug for personoplysningerne til behandlingen, men de er nødvendige, for at et retskrav kan fastlægges, gøres gældende eller forsvares.
- Den registrerede har gjort indsigelse mod behandlingen. I disse tilfælde har personen ret til begrænset behandling i perioden, indtil det klarlægges, om den dataansvarliges legitime interesser går forud for den registreredes legitime interesser, f.eks. i afskedigelses- og bortvisningssager.

2.7.7 RETTEN TIL INDSIGELSE

Den registrerede har til enhver tid ret til at gøre indsigelse mod behandling af sine personoplysninger, hvis der er grunde, der vedrører den pågældendes særlige situation.

Skolen må dermed ikke længere behandle personoplysningerne, medmindre skolen påviser vægtige legitime grunde til behandlingen, der går forud for den registreredes interesser og rettigheder, eller behandlingen er nødvendig for, at et retskrav kan gøres gældende.

2.7.8 RET TIL OVERFØRSEL AF OPLYSNINGER TIL ANDRE DATAANSVARLIGE *(Dataportabilitet)*

Når en person har givet personoplysninger, som f.eks. navn, adresse, telefonnummer, til en dataansvarlig, kan vedkommende kræve at få dem udleveret igen. Formålet med ret til dataportabilitet er, at en person kan få udleveret en kopi af afgivne personlige oplysninger og videregive dem til andre databehandlere. Personen kan dermed slippe for at indtaste samme oplysninger flere steder. I praksis vil det oftest dreje sig om kundeoplysninger og er dermed næppe relevant for skoler.

Skulle det være nødvendigt, skal oplysningerne udleveres i en almindelig elektronisk form og skal være strukturerede, så de er overskuelige og letlæselige.

Retten omfatter udelukkende oplysninger, som en person aktivt har afgivet. Det er altså ikke de oplysninger, skolen selv har noteret f.eks. i en personalemappe eller elevmappe. Ved skift mellem to efterskoler kan man f.eks. forestille sig, at elevens indkomstoplysninger kan sendes videre til den nye skole.

2.8 Databehandleraftale

Når man lægger behandlingen af data ud til en databehandler, kræver det, at der indgås en skriftlig aftale mellem den dataansvarlige og databehandleren. Det kaldes en databehandleraftale. Det er skolens ansvar som dataansvarlig, at aftalen er indgået.

Det skal fremgå af aftalen, at databehandleren alene handler efter instruks fra den dataansvarlige, og at databehandleren skal opfylde en række tekniske og organisatoriske sikkerhedskrav. Disse sikkerhedsforanstaltninger skal sikre mod, at oplysningerne forsvinder, misbruges eller på anden måde behandles i strid med lovgivningen.

Det er et område med stor vægt i persondatareglerne og derfor noget, databehandlerne selv bør bidrage aktivt til at opfylde.

Datatilsynet har udarbejdet en standardskabelon til databehandleraftaler, som indeholder de væsentligste bestemmelser, aftalen bør regulere.

Der findes en række godkendte certificeringsordninger, f.eks. for it-sikkerhed (ISO27001). En certificering er ikke i sig selv en garanti for, at databehandleren til enhver tid overholder forordningens krav og fritager ikke den dataansvarlige for ansvaret, men kan være en hjælp til at vurdere kvaliteten hos databehandleren.

Find skabelonen her:
www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner

2.9 Data Protection Officer (DPO) eller Data-sikkerhedsrådgiver

En Data Protection Officer (DPO) er en medarbejder i den dataansvarlige organisation, som udnævnes til at varetage opgaven med at sikre, at man lever op til persondatareglerne.

Ifølge Justitsministeriets udmeldinger gælder kravet om at udnævne en person for offentlige myndigheder, som er omfattet af forvaltningslovens § 1. De frie skoler og gymnasier skal derfor IKKE udpege en DPO. Fritagelsen fra at udnævne en person betyder imidlertid ikke, at organisationen kan frasige sig ansvaret for at overholde forordningen.

Skolen kan naturligvis frit bestemme, hvordan organiseringen af opgaven med it- og datasikkerhed tilrettelægges, herunder kan man udpege/ansætte en person til varetagelse/koordinering af opgaven. I alle tilfælde er det skolens ledelse, der har det overordnede ansvar for overholdelse af persondatareglerne.

2.10 Konsekvensanalyse – Data Protection Impact Assessment (DPIA)

Persondatareglerne stiller krav om, at dataansvarlige organisationer i visse tilfælde udarbejder en konsekvensanalyse af brud på datasikkerheden. Det gælder primært myndigheder, som træffer afgørelser på baggrund af elektronisk registrering (profilering), eller hvis der behandles følsomme oplysninger i stort omfang (f.eks. en stor lægepraksis eller et hospital), eller data kommer fra overvågning af offentlige områder.

Skoleforeningerne vurderer på den baggrund, at frie skoler ikke er omfattet af kravet om obligatoriske konsekvensanalyser.

Alligevel er det en god idé at forholde sig til, om (nogle af) de data, skolen behandler om eleven, er af særlig privat karakter, så det vil være forbundet med væsentlige omkostninger for eleven, hvis data kommer til uvedkommendes kendskab. I de tilfælde, hvor sådanne data behandles, er det særlig relevant at overveje sikkerheden ved opbevaring af data og ved overførsel af data til tredjepart. Det kan f.eks. dreje sig om PPR-vurderinger, oplysninger fra sundhedsplejerske eller læge, notater til brug for underretninger til kommunen, notater om konflikter i familien, mv.

Hvis skolen tager nye teknologier i anvendelse, vil det også være relevant at overveje, om de data, der behandles, er behæftet med særlig høj risiko for de registrerede i tilfælde af et brud.

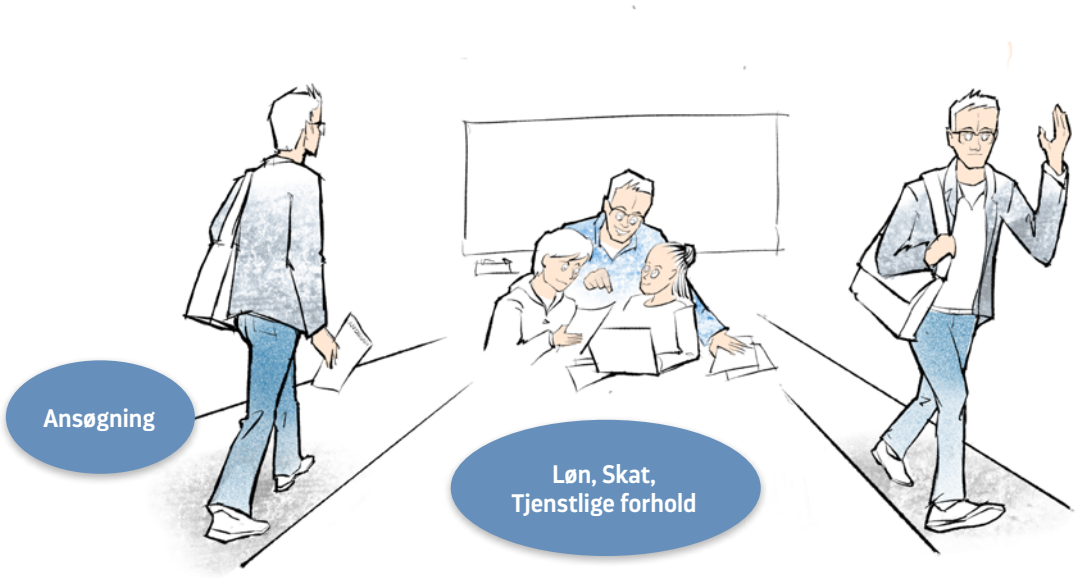
3

Behandling af data i praksis

Medarbejdere

Dette afsnit omhandler skolens behandling af medarbejdernes persondata. Afsnittet er bygget kronologisk op: Fra før ansættelse, over medarbejderens ansættelse på skolen frem til ansættelsens ophør. Afsnittet kan både læses i sin helhed og bruges som opslagsværk, hvis man er i tvivl i en konkret situation.

! Kravene til databehandling gælder alle typer ansatte, dvs. også praktikanter.



› I løbet af en ansættelse behandler skolen en række personoplysninger om medarbejderen

3.1 Før ansættelsens start

Allerede ved modtagelsen af ansøgningerne, behandler skolen personoplysninger og skal derfor iagttage persondatareglerne, herunder oplysningspligten.

Modtagelse og behandling af ansøgninger og oplysninger
Oplysningerne, som normalt modtages, er i kategorien almindelige personoplysninger, og behandlingen af disse oplysninger kræver derfor enten et samtykke til den konkrete behandling, eller at behandlingen er nødvendig for opfyldelsen af kontrakten/formålet med ansøgningen.

I tilfældet med ansøgninger er behandlingen nødvendig for at udfylde ansøgningens formål, nemlig at besætte et job. Derfor skal man ikke indhente samtykke til at behandle oplysningerne. Skolen skal dog stadig leve op til reglerne om oplysningspligt, opbevaring af oplysningerne osv. Skolen skal i den forbindelse overveje, hvordan ansøgningerne opbevares, og hvilke personer på skolen der har et sagligt behov for at læse dem (typisk ansættelsesudvalget og sekretæren).

Vær særligt opmærksom på, at det kræver særskilt samtykke at indhente referencer. Selv hvis ansøger har angivet referencer i ansøgningen, bør man ikke tage kontakt uden forudgående advisering af ansøger.

Sletteplig
En ansøgning skal slettes efter 6 måneder, medmindre ansøgeren giver udtrykkeligt samtykke til en længere opbevaring.

– EKSEMPEL 1 –

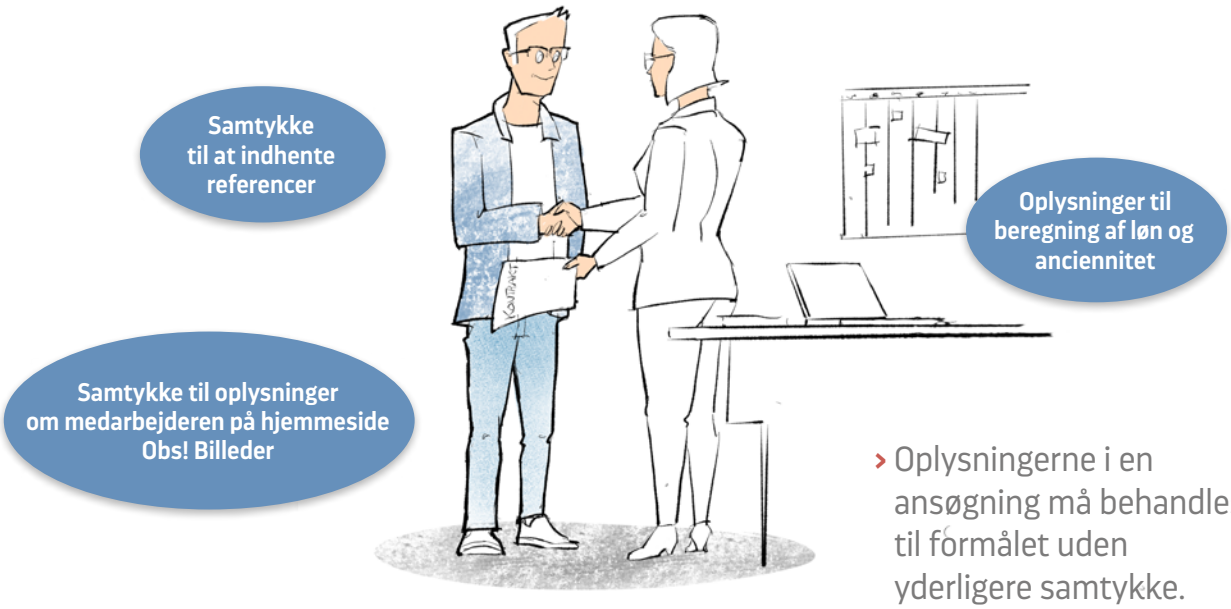
Kontaktoplysninger

- **Kontaktoplysninger** som navn, telefonnummer, e-mail o.lign. er nødvendige at behandle for at opfylde formålet med ansøgningen. Det kræver derfor ikke særskilt samtykke at behandle oplysningerne.
- **Kontaktoplysningerne** må kun bruges til kontakt som led i indkaldelse til samtale, afslag og lignende som har forbindelse til processen.

– SÆRLIGT OM –

CPR-numre

- **CPR-nummer er en særlig oplysningskategori**, som må anvendes, når det følger af lov, såsom indberetning til Skat, eller den ansatte har givet samtykke hertil. Oplysningen må kun videregives, hvis det f.eks. kræves af en offentlig myndighed, såsom kommunen i en sygdagpengesag eller til brug for statistiske formål (indberetning til Danmarks Statistik).
- **CPR-nummer må aldrig offentliggøres uden samtykke** fra den registrerede, men det er i praksis meget vanskeligt at forestille sig en situation, som nødvendiggør offentliggørelse.



› Oplysningerne i en ansøgning må behandles til formålet uden yderligere samtykke.

Skal slettes senest 6 måneder efter behandling af sagen.

3.2 Ved ansættelsens start

Ved ansættelsens start har skolen behov for at indhente en række supplerende oplysninger fra medarbejderen. En arbejdsgiver skal i ansættelsesbeviset oplyse medarbejderen om, at man behandler vedkommendes personoplysninger. Der kan være tale om såvel almindelige som følsomme personoplysninger.

Eksempler på almindelige personoplysninger som indhentes ved ansættelsens start:

- Navn, adresse, køn og alder.
- Kontakt- og stamoplysninger.
- Billede.
  NB! Der skal særskilt samtykke til brug af billede på hjemmeside
- Stilling, arbejdsopgaver, arbejdstider.
- Oplysninger om uddannelse, udtalelser og tidligere beskæftigelse.
  NB! Indhentelse af referencer skal man have særskilt samtykke til
- Lønoplysninger, skatteoplysninger, pensionsforhold og kontonummer.
- Personlighedstest og lignende.

Behandlingen af almindelige oplysninger i ansættelsesmæssige sammenhænge kan enten ske, hvis man har et samtykke til et eller flere specifikke formål, eller det er nødvendigt for at opfylde ansættelseskontrakten. Da behandling af oplysningerne er nødvendige for opfyldelse af ansættelseskontrakten, har skolen altså hjemmel til at behandle oplysningerne og behøver derfor ikke et generelt samtykke til behandling af almindelige oplysninger. Det er kun brug af billeder og behandling af følsomme oplysninger (fagforening og helbredsforhold), som kræver samtykke.

Brug af fotos
Det kræver i udgangspunktet samtykke at bruge billeder af medarbejderne på internettet. Det gælder både portrætbilleder og situationsbilleder (se afsnit 4.1.1 om billeder for en nærmere beskrivelse af denne skelnen). Der er dog undtagelser, hvis skolen f.eks. kan argumentere for, at det er nødvendigt af pædagogiske hensyn, som f.eks. at eleverne kan finde læreren via billede på intranettet.

Følsomme personoplysninger
Følsomme oplysninger er racemæssig eller etnisk baggrund, religion, politisk overbevisning, fagforeningsmæssige tilhørsforhold (ikke a-kasse), helbredsmæssige og seksuelle forhold, genetiske (nationalitet er som hovedregel ikke følsom oplysning) og biometriske data (f.eks. fingeraftryk).

Behandling af følsomme oplysninger i ansættelsesmæssige sammenhænge er som udgangspunkt forbudt, medmindre arbejdsgiver har fået udtrykkeligt samtykke til et eller flere specifikke formål, ELLER der påhviler den dataansvarlige en retlig forpligtigelse.

Alle virksomheder, der behandler særlige oplysningskategorier, har fra 1. januar 2019 pligt til at bruge en form for 'sikker mail', når de sender følsomme eller fortrolige oplysninger via e-mail.

Skoleforeningerne har udarbejdet en skabelon til brug for opfyldelse oplysningspligten og indhentning af samtykke hos medarbejdere til behandling af følsomme oplysninger og brug af fotos.

3.2.1 ANSATTE MED FLEKSJOB

Ved fleksjob behandles en række følsomme oplysninger om medarbejderens sygehistorik. Behandlingen er nødvendig for at afdække hvilke skånebehov, der er nødvendige for ansættelsesforholdet, og der er desuden krav om videregivelse af oplysninger i forbindelse med refusionsansøgninger.

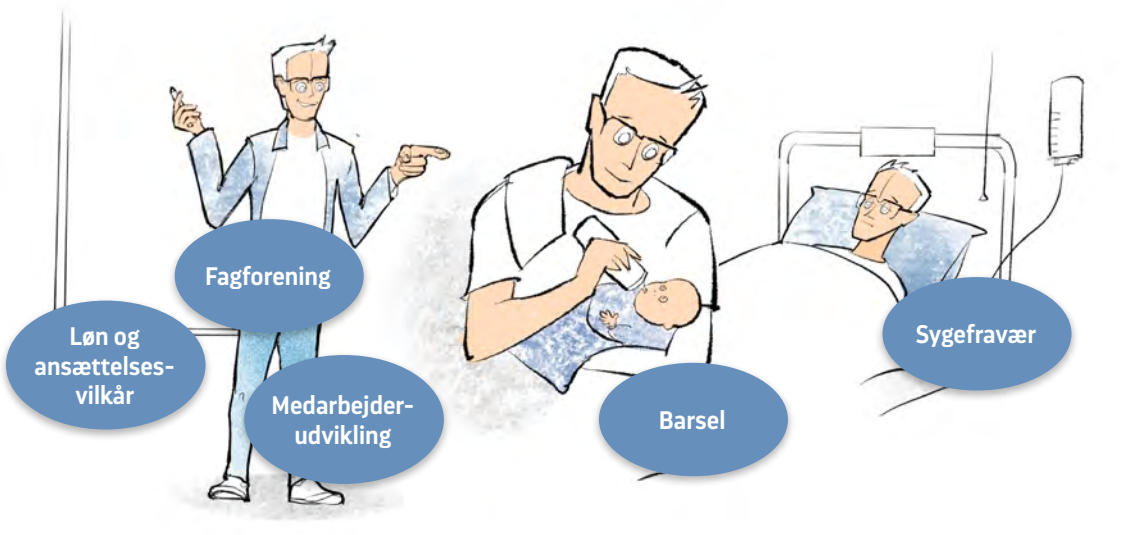
Det er følsomme oplysninger, som skolen ikke skal indhente særskilt samtykke til at behandle, da formål og hjemmel er givet i Lov om en aktiv beskæftigelsesindsats og bekendtgørelse om fleksjob. Grundlaget for skolens behandling ift. persondata er dermed Databeskyttelseslovens § 12 om varetagelse af den/de registreredes arbejdsretlige og sociale rettigheder i ansættelsesforhold.

– EKSEMPEL 2 –

Andre oplysninger

- **Kontaktoplysninger** – er nødvendige at behandle, da skolen har behov for oplysningerne til brug for kontakt til de ansatte.
- **Billede** - kræver samtykke, hvis billeder bruges på hjemmeside eller sociale medier. (Se afsnit 3.3)
- **Stilling, arbejdsopgaver og arbejdstider** – er nødvendige at behandle af hensyn til arbejdets planlægning og udførelse og kræver derfor ikke særligt samtykke.
- **Børneattest** – er nødvendig for at ansætte medarbejdere og frivillige, som har eller vil få mulighed for at opnå direkte kontakt med børn og unge under 15 år. Indhentning af børneattest kræver iflg. bkg. om behandling af personoplysninger i det centrale kriminalregister samtykke fra den pågældende, før Kriminalregisteret vil udskrive attesten. En børneattest bør straks destrueres efter modtagelsen, men skolen bør gemme kvitteringen for modtagelse som dokumentation på, at indhentning er foretaget.
- **Oplysninger om uddannelse, udtalelse og tidligere beskæftigelse** – kan være nødvendige at behandle for at lave en korrekt lønindplacering af medarbejderen og for at bekræfte, at vedkommende har de oplyste uddannelser. I tilfælde hvor det er nødvendigt at behandle oplysningerne, kræves der ikke særskilt samtykke.
- **Lønoplysninger, skatteoplysninger, pensionsforhold og kontonummer** – er nødvendige at behandle for, at der kan udbetales løn, pension og for overholdelse af overenskomster, hvor bestemte pensionsforhold er påkrævet. Oplysningerne skal desuden indhentes og behandles for, at skolen kan leve op til lovgivningen på skatteområdet, og der kræves derfor ikke særskilt samtykke.

Personoplysninger i løbet af ansættelsen



› Registrering af sygefravær og andet fravær er almindelige oplysninger. Oplysninger om ***årsager til fraværet***, er helbredsoplysninger og dermed ***følsomme oplysninger***, som kun må behandles efter udtrykkeligt samtykke og med henblik på opfyldelse af særlige formål.

3.3 Under ansættelsen

I løbet af ansættelsesforholdet vil der også være en naturlig behandling af medarbejderens personoplysninger. Igen kan der være tale om både almindelige og følsomme personoplysninger.

Som beskrevet under afsnittet 3.2 'Ved ansættelsens start' kræver behandling af de almindelige oplysninger enten et samtykke til et eller flere specifikke formål, ELLER at det er nødvendigt for at opfylde ansættelseskontrakten.

Ud over de oplysninger, som også er nævnt under afsnit 3.2, kan der komme oplysninger om sygefravær og sygdomsperioder, andet fravær fra arbejdet (se mere nedenfor) og væsentlige sociale problemer eller andre private forhold. Herunder personlighedstest, der bruges i forbindelse med evaluering og udviklingssamtaler, mv.

Endelig er data, som indsamles elektronisk i forbindelse med medarbejderens udførelse af jobbet, såsom billeder fra tv-overvågning, nøglechips, og automatisk tidsregistrering, også personoplysninger, der er omfattet af kravene i persondatareglerne. Dvs., at skolen skal oplyse medarbejderen om, at oplysningerne indsamles og til hvilket formål.

– EKSEMPEL 3 –

Sygdom og fravær

Sygefravær og sygdomsperioder samt andet fravær fra arbejdet – er nødvendige at behandle i forbindelse med planlægning af f.eks. vikardækning, sygedagpenge-refusion, udarbejdelse af planer for tilbage-venden til arbejdet og lignende.

NB!
Hvis man har viden om sygdommen eller dennes årsag, er det en helbredsoplysning i kategorien følsom personoplysning. Det kræver derfor et specifikt formål og et udtrykkeligt samtykke fra personen, som oplysningerne omhandler. Ofte er det medarbejderen selv, som oplyser om sygdom eller årsagen ved sygemeldingen, f.eks. i mulighedserklæring. Det anbefales under alle omstændigheder, at skolen sikrer sig udtrykkeligt samtykke til behandling af oplysningerne. Oplysningerne kan også være nødvendige for at imødekomme særlige tilpasningsbehov, som skal hjælpe en medarbejder tilbage til tjenesten.

I denne sammenhæng skal skolen være opmærksom på tavshedspligten og må aldrig dele oplysninger om årsagen til sygefravær, heller ikke mundtligt i medarbejdergruppen, uden udtrykkeligt samtykke.

– EKSEMPEL 4 –

Arbejdsskader

Skolen er retligt forpligtet til at anmelde arbejdsskader og må derfor behandle oplysningerne.

Offentliggørelse af oplysninger om medarbejderen
Skolen må i udgangspunktet offentliggøre almindelige oplysninger om medarbejderen, som er nødvendige for skolens drift. Dvs. oplysninger om navn, stilling og funktioner, som f.eks. hvilke fag man underviser i og evt. klassetrin og andre relevante oplysninger. Detaljerede oplysninger om opholdssted og tid eller oplysninger, der kan bruges til identitetstyveri, må ikke offentliggøres.

Privatadresse og telefonnummer samt andre ikke strengt relevante oplysninger må ikke offentliggøres uden samtykke.

Skolen kan, ud fra pædagogiske hensyn, argumentere for, at offentliggørelse af portrætbillede på skolens intranet er obligatorisk, men øvrige portrætbilleder på nettet eller i trykt materiale kræver samtykke. Se mere om fotos i afsnit 3.2 og afsnit 4.1.1.

Personoplysninger ved ansættelsens ophør

3.4 Ved fratræden

Ved fratræden er udgangspunktet, at alle personfølsomme oplysninger skal slettes. Det kan dog følge af lov, at oplysninger skal gemmes. Dette kan f.eks. forekomme, når der er behov for oplysningerne i forbindelse med dagpengerefusion, skatteoplysninger eller regnskaber. Skolen kan desuden gemme oplysningerne, hvis der er en verserende sag, en arbejdsretlig tvist eller lignende.

En del af persondatabeskyttelsen er også at iagttage tavshedspligten i forbindelse med fratrædelser. Dette kan særligt være relevant i afskedigelsessager, hvor de øvrige medarbejdere føler sig utrygge og vil have indsigt i begrundelsen for afskedigelsen. Ledelsen må ikke dele oplysninger af privat eller fortrolig karakter om medarbejderen med andre, som ikke har et sagligt begrundet behov for indsigt i disse. Dvs., at man bør begrænse sig til at oplyse nøgternt om fratrædelsen og fokusere på de fremadrettede konsekvenser for de tilbageværende medarbejdere (ny opgavefordeling, etc.).

– SÆRLIGT OM –

Orienteringspligt ved opsigelser

Der kan fremgå af overenskomster, at skolen har pligt til at orientere en specifik faglig organisation ved opsigelse eller påtænkt opsigelse af en medarbejder. Orienteringen må dog ikke indeholde oplysninger om vedkommendes sygefravær eller andre følsomme oplysninger om baggrunden for afskedigelsen.

Det er tilstrækkeligt at orientere organisationen om at opsigelsen er effektueret med angivelse dato. Herefter påhviler det den faglige organisation at indhente samtykke fra den opsagte medarbejder til videregivelse af yderligere oplysninger fra skolen, herunder kopi af opsigelsen.

– EKSEMPEL 5 –

Opsigelse

› **Medarbejderen opsiger selv sin stilling**
Der er behov for opbevaring af oplysninger, som følger af lov, f.eks. skatteoplysninger og oplysninger til regnskaber.

› **Skolen opsiger medarbejderen**
I tilfælde, hvor skolen opsiger en medarbejder, kan der opstå uenighed om saglighedenaf opsigelsen. Hvis der verserer en sag, eller der er en risiko for, at der opstår en sag om opsigelsen, har skolen et sagligt behov for behandling af oplysningerne om medarbejderen. Skolen skal derfor ikke slette oplysningerne, før sagen er endeligt afsluttet. Heller ikke hvis medarbejderen påberåber sig retten til at blive glemt.

Som tommelfingerregel kan skolen opbevare oplysninger om fratrådte medarbejdere i op til 5 år.

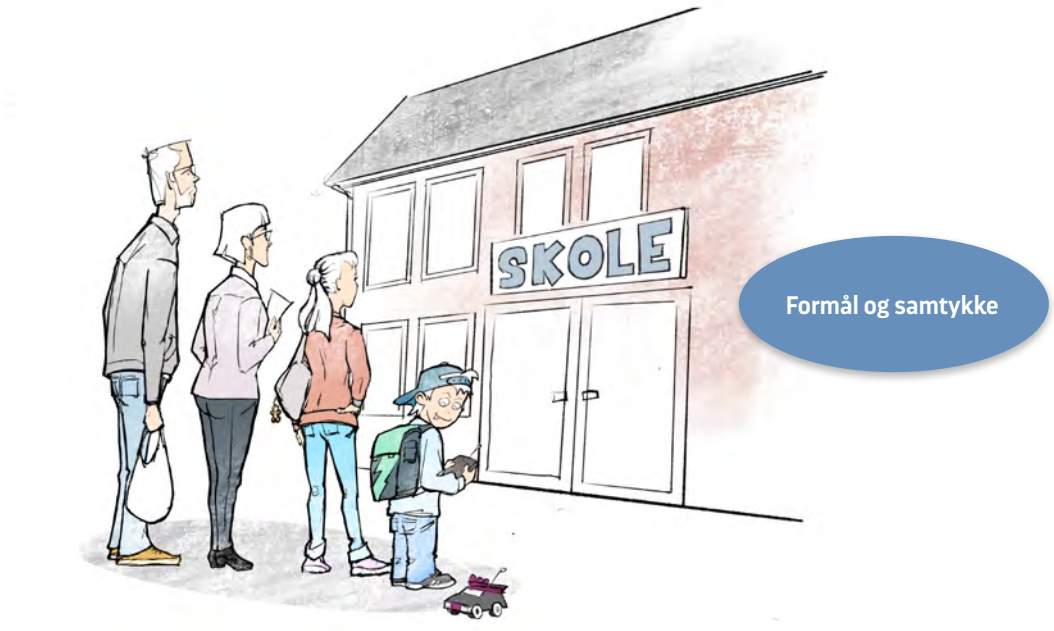
Iflg. regnskabsbekendtgørelsen SKAL bogføringsmateriale gemmes i fem år efter regnskabsårets afslutning.

4

Behandling af data i praksis

Elever og forældre

Dette afsnit omhandler skolens behandling af elevers og forældres persondata. Afsnittet er bygget kronologisk op: Fra familien tager kontakt til skolen første gang, og barnet optages som elev; mens eleven går på skolen, og til eleven forlader skolen igen. Afsnittet kan både læses i sin helhed og bruges som opslagsværk, hvis man er i tvivl i en konkret situation.



› Oplysninger i ansøgningsskemaet er nødvendige for at behandle ansøgningen. Skolen skal aktivt gøre opmærksom på den registreredes rettigheder.

4.1 Venteliste og indmeldelse

Pligten til at oplyse om, hvilke oplysninger der behandles, og hvilke formål behandlingen tjener, gælder i alle forhold. Når skolen indsamler oplysninger hos forældre og elever, skal skolen oplyse om, hvad de indsamlede oplysninger skal bruges til eller påtænkes brugt til; om oplysningerne videregives til andre, og i hvilket tidsrum personoplysningerne vil blive opbevaret.

I forbindelse med indskrivning på venteliste registrerer skolen en lang række data om de kommende elever og deres forældre.

Ved endelig indmeldelse bør skolen sikre sig, at begge forældremyndighedsindehavere skriver under på indmeldelsespapirerne. Dermed får skolen umiddelbart personoplysninger på begge forældremyndighedsindehavere, som bliver registreret sammen med oplysninger om eleven.

FOR ELEVEN kan der være tale om almindelige og følsomme oplysninger som:

Almindelige oplysninger
- Navn
- Adresse
- Evt. søskende på skolen
- Forældremyndighedsindehavere

Særlige kategorier
- CPR-nr.
- Oplysninger fra tidligere skoler

Følsomme oplysninger
- Oplysninger af privat karakter, f.eks. fra Pædagogisk Psykologisk Rådgivning (PPR)
- Generelle helbredsoplysninger som medicinforbrug, allergier, mv.

Følsomme oplysninger kræver altid samtykke.

Når skolen indsamler CPR-nummer alene til optagelse på en venteliste, kræver det ligeledes samtykke. Først når eleven optages som elev, er der lovhjemmel til behandlingen af CPR, da det kræves for at kunne indhente tilskud.

Indhentning af oplysninger fra tidligere skole kræver også samtykke, som den nye skole er ansvarlig for at indhente og dokumentere overfor den tidligere skole.

FOR FORÆLDREMYNDIGHEDSINDEHAVERNE kan der være tale om oplysninger som:

- Navn
- Adresse
- E-mail og telefonnr.
- Stilling
- Økonomi ifm. friplads (for efterskoler til beregning af statslig elevstøtte)

Dette er almindelige personoplysninger. Skolen skal sikre, at der indhentes samtykke til at registrere disse oplysninger, eller beskrive i indmeldelsesblanketten, at disse oplysninger er nødvendige, for at skolen kan indskrive barnet, samt hvordan og hvor længe oplysningerne vil blive opbevaret.

4.1.1 BRUG AF FOTOS: HVORNÅR KRÆVES DER SAMTYKKE?

Ved indmeldelse bør skolen sørge for at få forældremyndighedsindehavernes samtykke til brug af fotos, hvor eleven kan genkendes, på skolens hjemmeside, trykt materiale og sociale medier. Listen over hvilke steder og på hvilke medier, fotos kan blive brugt, bør så vidt muligt være udtømmende.

Samtykke til brug af billeder på forskellige medier skal gives frivilligt og må derfor ikke være en betingelse for optagelse på skolen.

Datatilsynet skelner mellem ***portrætbilleder***, som altid kræver samtykke og ***situationsbilleder***, der principielt kan anvendes uden samtykke.
Et portrætbillede er kendetegnet ved, at det er fremstilling af personen på billedet, som er det primære formål. På situationsbilleder er det derimod situationen, der er det primære formål med

billedet. I praksis kan grænsen mellem portræt- og situationsbilleder imidlertid være vanskelig at definere entydigt. Grænsen mellem, hvornår en skole alene dokumenterer det daglige liv, og hvornår der er tale om elevrekruttering, er oftest usynlig.

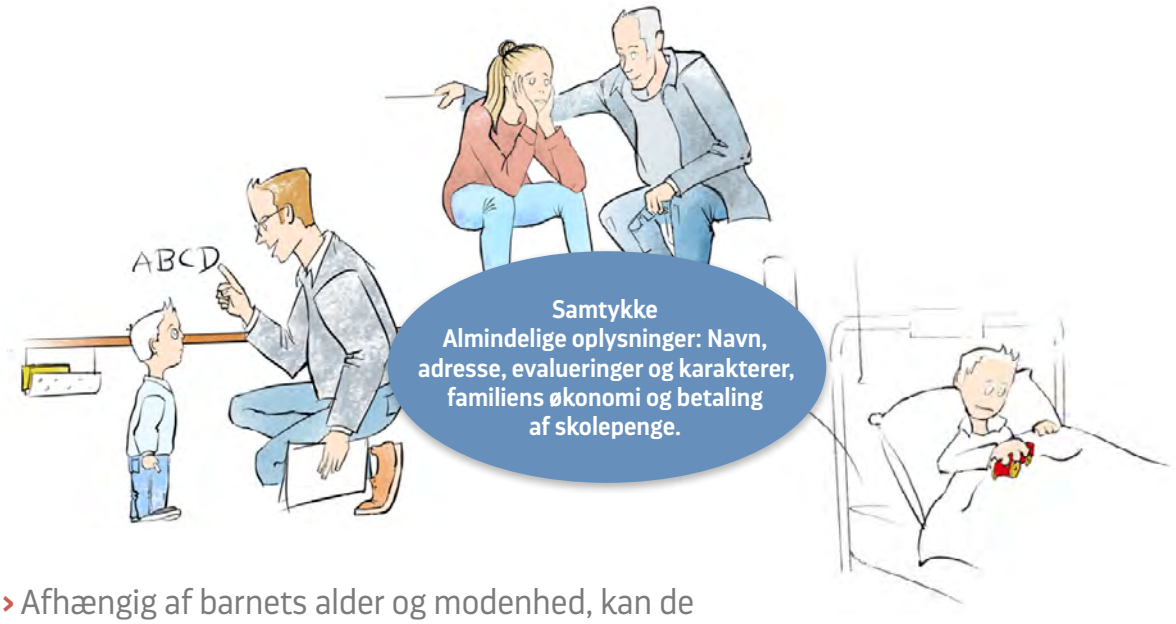
Skoleforeningerne anbefaler, at skolen beder om samtykke til at anvende billeder (under ét), hvor eleven kan genkendes på skolens hjemmeside, i trykte materialer og på sociale medier. Det sikrer, at man ikke fra billede til billede skal tage stilling til, om der er tale om hhv. portræt- eller situationsbillede, og at skolen ikke kommer i klemme, hvis eleven er uenig i vurderingen heraf.

Billeder fra offentlige begivenheder på skolen, f.eks. åbent hus, bedsteforældredage, teater- eller gymnastikopvisninger, debatarrangementer eller ekskursioner til offentlige områder, vil altid regnes som situationsbilleder, og kan anvendes uden samtykke.

Datatilsynet råder til, at man altid efterkommer en anmodning, hvis en person ønsker et situationsbillede fjernet, hvor vedkommende kan genkendes.

Skoleforeningerne har udarbejdet en skabelon til formulering af samtykke til brug af billeder, som findes på foreningernes hjemmesider.

Elevens skolegang



› Afhængig af barnets alder og modenhed, kan de selv give samtykke til behandling af personoplysninger.

Frem til barnet fylder 15 år, er behandlingen kun lovlig i det omfang, forældremyndighedsindehaver har givet samtykke hertil.

4.2 Behandling af personoplysninger under elevens skoletid

Imens en elev går på skolen, har skolen umiddelbart en saglig (lovlig) grund til at behandle personoplysninger om eleven samt dennes forældre, hvis oplysningerne bruges i skoleøjemed, som f.eks. videregivelse af oplysninger om barnets generelle trivsel til klasselæreren eller brug af kontaktoplysninger til at indkalde forældrene til forældremøde.

4.2.1 SAMTYKKE FOR ELEVER UNDER 18 ÅR

Skolen kan som tidligere beskrevet have behov for at indhente samtykke til behandling af oplysninger om en elev. Spørgsmålet bliver herefter, om eleven selv kan give samtykke til behandling af sine personoplysninger eller ej.

– EKSEMPEL 6 –

Videregivelse af elev- og forældreoplysninger til tredjepart

En videregivelse af elevens eller forældrenes kontaktoplysninger til et privat firma til brug for firmaets markedsføring vil ikke være sagligt. Derimod vil det være sagligt at videregive kontaktoplysninger om en forælder, der er blevet valgt til bestyrelsen, til Undervisningsministeriet.

Det fremgår af gældende ret, at børn bør behandles i overensstemmelse med deres psykiske og fysiske modenhed, og at de fra og med en vis alder er i stand til at tage stilling til spørgsmål, som vedrører dem. Hvorvidt en elev er i stand til at give samtykke selv, beror derfor på en konkret vurdering af elevens modenhed i hver enkelt situation.

Som tommelfingerregel kan unge over 15 år selv give samtykke til behandling af deres personoplysninger, hvilket også betyder, at de selv kan anmode om indsigt, mv. i overensstemmelse med deres rettigheder.

På mange skoler er det forældrene, der underskriver optagelsespapirer og giver samtykke til behandling af oplysninger på deres barns vegne. Skolen er således ikke forpligtet til at indhente fornyet samtykke hos eleven, når denne fylder 15 år. Den unge vil stadig kunne bruge sine rettigheder som registreret til f.eks. at søge om indsigt. I praksis vil det være meget sjældent, at forældre giver samtykke til behandling af oplysninger mod barnets vilje.

Elever over 18 år betragtes som voksne og skal afgive samtykke på egne vegne.

4.2.2 INDSIGTSRET FOR FORÆLDREMYNDIGHEDSINDEHAVERE

I udgangspunktet kan forældremyndighedsindehavere kræve indsigt på barnets vegne indtil det fyldte 18. år. Der gælder imidlertid samme krav til en konkret modenhedsvurdering og barnets egne interesser i indsigtsbegæringen, som ved samtykke. Som tommelfingerregel medfører det, at elever over 15 år selv kan søge om indsigt i egne oplysninger.

En forælder, der har forældremyndighed, kan på vegne af sit barn bede om indsigt i alle de oplysninger, skolen har registreret om barnet og vedrører

Forældrenes personoplysninger og samtykke

Forældre skal afgive samtykke til behandling af personoplysninger på børnenes vegne frem til det fyldte 13. år. De skal også give samtykke til behandling af egne oplysninger. Deling af oplysninger skal altid være sagligt begrundet og tjene et formål.

barnets skolegang; fagligt og socialt. Dvs. karakterblade, PPR-rapporter mv. Endvidere har forældremyndighedsindehaveren ret til at få information om formålet med behandlingen, hvem personoplysningerne er eller vil blive videregivet til, og – om muligt – det tidsrum, hvor personoplysningerne vil blive opbevaret.

Skolen må ikke udlevere akter, der vedrører private forhold om andre end den forælder, der anmoder og/eller barnet selv. Skolen skal også sikre sig, at det rent faktisk er den korrekte forælder, der anmoder om indsigt.

På ***efterskoler og skoler med kostafdeling***, hvor eleverne bor på skolen, behandles også data om elevernes samlede og individuelle færden. Det sker f.eks. i logbøger, hvor nattevagten overleverer døgnets begivenheder til dagvagten. I de tilfælde, hvor elever kan identificeres, er der tale om personoplysninger, som dermed er reguleret af persondatareglerne. Generelt bør skolen ikke opbevare denne type oplysninger længere, end formålet med behandlingen tilsiger.

Det kan også ske, at ***eleven giver skolen oplysninger om sig selv eller andre, som han/hun ikke vil have, deles med forældrene***. Forældremyndighedsindehavere har i udgangspunktet ret til indsigt i alle oplysninger om barnet, som skolen behandler. Undtagelse til indsigtsretten kan kun ske, hvis skolen ud fra en konkret vurdering finder, at forældrenes interesse i indsigt i oplysningerne findes at burde vige for afgørende hensyn til offentlige eller private interesser, herunder eleven selv. Undtagelser til indsigtsretten er behandlet i databeskyttelsesloven § 22. Dvs., at skolen, ved krav om indsigt i oplysningerne fra forældrene, skal foretage en individuel, konkret vurdering i forhold til barnets tarv.

Undtagelser fra indsigtsretten er også beskrevet i afsnit 2.7.3.

4.3 Skærpet underretningspligt og persondata

Den skærpede underretningspligt, der gælder for alle medarbejdere, der har med børn at gøre, påvirkes ikke af persondatareglerne. Den skærpede underretningspligt er hjemlet i lov om social service. Således er der et udtrykkeligt formål med udveksling af data, som har fortrinsret fremfor den/de registreredes rettigheder.

I sager med underretning skal man fortsat orientere forældrene i de relevante tilfælde, i overensstemmelse med lovgivningen.

4.4 Forældreansvarsloven og persondata

Forældre med delt forældremyndighed har samme ret til indsigt i barnets forhold. Forældre uden del i forældremyndigheden har ikke samme rettigheder. De har ret til orientering om barnets forhold. Disse rettigheder er beskrevet i Socialministeriets vejledning fra januar 2014 (Skolers pligt til at give orientering om barnets forhold til en forælder, der ikke har del i forældremyndigheden).

Samlevere, bonus- og papforældre har ret til indsigt efter udtrykkeligt samtykke fra forældremyndighedsindehaveren og barnet/eleven selv afhængig af alder og modenhed.

› Når eleven forlader skolen er der en række oplysninger, som iflg. love og regler skal gemmes. Det gælder fx afgangsprøvebevis.

De øvrige oplysninger om eleven skal slettes.

4.5 Eleven går ud af skolen

Når eleven forlader skolen f.eks. ved skoleskift eller afsluttet skolegang, er der en række oplysninger om eleven og forældrene, som enten skal slettes eller gemmes.

Der skal være et specifikt sagligt formål med opbevaring af oplysninger, og oplysningerne må ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum, end det er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. De oplysninger, som skolen har lovmæssig pligt til at opbevare, er omfattet af et sådant formål. Opbevaring af andre oplysninger efter endt skolegang kræver samtykke.

Styrelsen for Undervisning og Kvalitet (STUK) har slået fast, at PPR-vurderinger af elevers behov for specialundervisning skal gemmes i fem år efter regnskabsårets afslutning til brug for revision.

Der kan ikke angives faste regler for, hvor længe elevoplysninger skal opbevares, efter eleven har forladt skolen. Det skal afgøres i den enkelte situation ud fra hvilke konkrete behov, der er for at gemme dem.

Hvis skolen ønsker at opbevare adresse- og kontaktoplysninger på familien med henblik på indkaldelse til jubilæer, mv. skal der foreligge et samtykke hertil.

› Se eksempel 7.

– EKSEMPEL 7 –

Saglig grund til at bevare elevoplysninger

Det vil være sagligt at gemme elevoplysninger på en elev, der er stoppet på skolen, hvis der verserer en klagesag eller en forsikringssag, der ikke er afsluttet på tidspunktet for udmeldelse. Modsat er der ikke en saglig grund til at opbevare elevoplysninger ved en sædvanlig afsluttet elevsag, længere end regnskabsbekendtgørelsen tilsiger, bortset fra afgangsbeviser.

4.5.1 AFGANGSBEVISER OG PRØVE-BESVARELSER

Afgangsbeviser og – udtalelser, herunder relevante oplysninger, der er nødvendige for at udstede beviser og udtalelser, skal opbevares til 'tid og evighed' iht. lovgivning om offentlige arkivalier. Det vil sige, at beviserne aldrig må kasseres.

Elevbesvarelser skal opbevares et år efter bedømmelsen. Censors og eksaminators notater skal også opbevares et år. Censor har ansvaret for opbevaring af egne notater.

4.5.2 VIDEREGIVELSE AF OPLYSNINGER TIL NY SKOLE

Som det fremgår ovenfor, beror det på en konkret vurdering, hvorvidt en elev modenhedsmæssigt selv er i stand til at give et samtykke eller ej.

Det antages, at hvis en mindreårig på egen hånd kan indgive en ansøgning til myndighed, må den pågældende også kunne give samtykke til de efterfølgende skridt som f.eks. indsamling og videregivelse af personoplysninger.

› Se eksempel 8.

– EKSEMPEL 8 –

Optagelse på en ungdoms- eller videregående uddannelse

Ansøgning om optagelse på en ungdomsuddannelse eller videregående uddannelse gennem Optagelse.dk kræver mindst en af forældremyndighedsindehavernes samtykke, når eleven er under 18 år.

4.5.3 OPLYSNINGER OM FORÆLDRE

Når en elev meldes ud, skal skolen som overvejende hovedregel slette oplysninger om forældrene, da der ikke længere er en saglig grund til at opbevare oplysningerne. En eventuel opbevaring af disse oplysninger skal være konkret og sagligt begrundet. F.eks. kan det være sagligt at opbevare oplysninger om en forælder, der stadig sidder i bestyrelsen, funktionsperioden ud.

4.5.4 PERSONDATA VED UDSKRIVNINGER OG BORTVISNINGER

I sager, hvor afbrydelse af skolesamarbejdet sker på skolens initiativ, dvs. at man enten udskriver eller bortviser en elev, sker det, at forældrene kræver alle data om forløbet udleveret, eller kræver, at skolen udfærdiger en skriftlig redegørelse for årsagerne til udskrivningen/bortvisningen.

Skolen kan ikke nægte forældrene indsigt i registrerede oplysninger om deres barn, men har ikke pligt til at udarbejde skriftlige materialer, der ikke allerede foreligger. Skolen skal være opmærksom på, at udleveret materiale ikke må omfatte oplysninger om andre end den pågældende.

5

Dokumentation/ databehandlingsrapport

Skolen skal udarbejde en skriftlig dokumentation for, at skolen lever op til persondatareglerne om behandling af personoplysninger.

DOKUMENTATIONEN bør være samlet tilgængelig på skolen og skal som minimum indeholde følgende:

- Formalia om skolen (kontaktoplysninger, mv.)
- Fortegnelse med en oversigt over datastrømme, herunder angivelse af de kategorier og typer af personoplysninger, skolen behandler, og hvordan registrering, behandling og opbevaring af data finder sted.
- Beskrivelse af skolens procedurer og kopier af formuleringer til iagttagelse af oplysningspligten ift. elever, forældre, jobansøgere og medarbejdere, m.fl.
- Kopi af skolens samtykkeerklæringer til elever/forældre og medarbejdere.
- Oversigt over skolens sikkerhedsforanstaltninger, herunder politikker og procedurebeskrivelser for både fysisk og digital sikkerhed. Typisk udarbejdes en ekstern databeskyttelsespolitik, som kan lægges på hjemmesiden. Herudover bør skolen udarbejde en intern databeskyttelseshåndbog eller medarbejderinstruks med retningslinjer for databeskyttelse.
- Beskrivelse af skolens beredskab ved sikkerhedsbrud.
- Oversigt over alle skolens databehandleraftaler.
- Dokumentation for bestyrelsens stillingtagen til overholdelse, som opdateres årligt (compliance).

– VÆRKTØJ –

Hjælp til dokumentationsarbejdet

Skoleforeningerne har udarbejdet et værktøj med navnet 'Persondatamappe' som indeholder en oversigt over de nødvendige elementer i dokumentationsarbejdet samt en række skabeloner til udarbejdelse af f.eks. instruks til medarbejdere, mv.

› Værktøjet findes på foreningernes hjemmesider.

6

Brud på persondata-sikkerheden

Skolen skal have de nødvendige procedurer på plads til at opdage, undersøge og rapportere brud på persondatasikkerheden.

BRUD PÅ PERSONDATASIKKERHEDEN er enhver hændelse, hvorved persondata forringes, fortabes, kommer til uvedkommendes kendskab eller direkte misbruges. Oftest kommer risikoen indefra, ved at personer med tilknytning til skolen får adgang til oplysninger, de ikke burde have haft adgang til. Det kan dog også være eksternt, f.eks. ved hackerangreb, tyveri, brand, mv.

Beredskab indebærer, at man skal have taget stilling til, hvem, der gør hvad hvis situationen opstår. Herunder er det især vigtigt, at der er en klar fordeling af ansvaret ift. at anmelde bruddet til Datatilsynet, kommunikere med de registrerede og evt. eksterne interessenter (presse, sociale medier, mv.).

Persondatareglerne foreskriver, at alle brud på persondatasikkerheden dokumenteres. Hvis bruddet kan medføre risiko for fysiske personers rettigheder eller frihedsrettigheder, skal bruddet desuden anmeldes til Datatilsynet indenfor 72 timer. Desuden skal skolen informere de berørte personer om bruddet, hvis der er høj risiko for, at de pågældende f.eks. kan blive udsat for diskrimination, identitetstyveri eller bedrageri på baggrund af sikkerhedsbruddet.

Hvis brud på persondatasikkerheden sker hos en af skolens databehandlere, er det ligeledes skolens ansvar at vurdere risikoen for de registrerede, og afhængig af vurderingen hurtigst muligt at sørge for kommunikation om bruddet til de berørte personer.

I udgangspunktet skal alle brud på persondatasikkerheden anmeldes til Datatilsynet, med mindre det er usandsynligt, at bruddet har medført nogen risiko for den/de registrerede. Det påhviler den dataansvarlige at løfte bevisbyrden for, at der ikke har været nogen risiko i forbindelse med bruddet.

I vurderingen af risikoen for den/de registrerede, skal man bl.a. inddrage en vurdering af oplysningens karakter, omfanget af bruddet ift. antal personer, tidsmæssig udstrækning af bruddet (har uvedkommende f.eks. haft adgang i en time eller en uge).

Anmeldelsen til Datatilsynet bør omfatte kontaktoplysninger til skolen vedr. bruddet, angivelse af antallet af berørte personer, oplysningernes karakter, omfanget af bruddet og angivelse af de sandsynlige konsekvenser ved bruddet samt evt. skolens foranstaltninger for at minimere skadevirkningerne.

Anmeldelser af brud på datasikkerheden, som indgives til Datatilsynet, bliver omfattet af reglerne om offentlig aktindsigt. Dvs., at der i anmeldelsen ikke må indgå personhenførbare oplysninger om registrerede af nogen art.

Yderligere vejledning kan findes hos Datatilsynet:
www.datatilsynet.dk/media/6558/haandtering-af-brud-paa-persondatasikkerheden.pdf

Udarbejdet af de frie skoleforeninger i Danmark
2019

Danmarks Private Skoler grundskoler & gymnasier
efterskolerne
FRISKOLERNE
Højskolerne
Foreningen af Kristne Friskoler