Utdannings-
direktoratet

# Grunnkrav til behandling av personopplysningsloven

Grunnkrav er krav som enhver skole- og barnehageeier må oppfylle for å kunne behandle personopplysninger.

**ARTIKKEL** | SIST ENDRET: 23.04.2018

Skole- og barnehageeier skal oppfylle grunnkravet for å kunne behandle personopplysninger. Hvis de ikke blir oppfylt, vil det være i strid med personvernet til barn i barnehage og skole, foresatte eller ansatte. Da kan man risikerer bøter. Det er et relativt alvorlige bruddet å ikke oppfylle grunnkravene i personvernforordningen.

Personvernforordningen har sju grunnkrav for behandling av personopplysninger.

## 1. Lovlig, rettferdig og gjennomsiktig

**Behandlingen av personopplysninger skal være lovlig.** Det at behandlingen skal være lovlig betyr at skole- og barnehageeier skal ha et rettslig grunnlag for behandlingen av personopplysninger. Det er redegjort mer for dette grunnkravet under rettslig grunnlag for behandling av personopplysninger.

**Behandlingen av personopplysninger skal være rettferdig.** Dette kravet innebærer blant annet at barn i barnehage og skole, foresatte og ansatte sine rimelige forventninger til hva deres personopplysningene skal brukes til, skal respekteres. Rettferdig behandling innebærer også at barn i barnehage og skole, foresatte og ansatte sine rettigheter som registrerte skal ivaretas. Datatilsynet har utarbeidet en egen veileder om temaet.

**Behandlingen av personopplysninger skal være gjennomsiktig**. Dette vil si at skole- og

barnehageeier skal være åpne om hva opplysningene brukes til, og at barn i barnehage og skole, foresatte og ansatte skal vite hva som skjer med deres personopplysninger. Datatilsynet har i sin veileder understreket at gjennomsiktighet betyr at behandlingen skal være forståelig for de registrerte; den skal ikke foregå på fordekte eller manipulerende måter.

## 2. Formålsbegrensning

Personopplysningene skal ikke brukes til noe annet enn det de ble samlet inn for (formålsbegrensning).

Enhver behandling av personopplysninger skal ha et klart formål; personopplysningene skal samles inn og brukes til «noe» konkret. Dette «noe» er formålet med behandlingen.

Kravet om formålsbegrensning innebærer at personopplysningene ikke skal gjenbrukes til helt andre ting enn det de opprinnelig ble samlet inn for. Vi sier at de ikke kan brukes til noe som er uforenelig med det opprinnelige formålet. Det at en personopplysning ikke skal brukes til noe som er uforenelig med det opprinnelige formålet, betyr at behandlingsansvarlig har en viss mulighet til å bruke personopplysningene til noe som er innenfor det opprinnelige formålet.

> Utdanningsdirektoratet anbefaler at skole- og barnehageeier er svært forsiktig med å bruke personopplysninger til andre formål enn det de ble samlet inn til.
>
> Det er Utdanningsdirektoratets vurdering at det ikke skal mye til for å være utenfor det opprinnelige formålet på en måte som ikke er i tråd med personvernforordningen.
>
> Hvis skole- og barnehageeier mener at en ny behandling av personopplysninger er forenelig med det opprinnelige formålet, anbefaler Utdanningsdirektoratet at denne vurderingen dokumenteres og begrunnes skriftlig, og at kommunens personvernombud involveres i vurderingen. For offentlig barnehager og skoler er personvernombudet ansatt i kommunene, mens private barnehager og skoler kan ha et eget personvernombud.

Datatilsynet har i sin veileder fastsatt at sentrale momenter i vurderingen om en behandling er uforenelig med det opprinnelige formål. Det fremgår av GDPRs fortale at en behandling til arkivformål i allmennhetens interesse, forskning eller statistikk, bør være forenelig med det opprinnelige formålet. Formålsbegrensning vil ikke være til hinder for at en skole- eller

barnehageeier skal kunne anmelde straffbare forhold.

Pseudonymisering: enkelte direkte identifiserende personopplysninger erstattes med pseudonymer, som fremdeles vil være unike indikatorer. Dette vil være en indirekte personopplysning da det vil være mulig for noen å knytte indikatoren til en enkeltperson.

Kryptering: kan gjøre data (for eksempel tekst) uleselig for andre ved hjelp av en matematisk funksjon (krypteringsteknikk/algoritme) og en forhåndsbestemt nøkkel. Datatilsynet har en egen veiledning om anonymisering av personopplysninger.

## 3. Dataminimering

Det skal ikke samles inn flere personopplysninger enn det som er nødvendig for å oppfylle den oppgaven (formålet) som opplysningene er samlet inn for å løse.

Hvis en oppgave kan løses uten at man trenger å behandle personopplysninger, skal heller ikke personopplysninger behandles. Dette kalles «dataminimering».

Det er skole- og barnehageeier som skal sørge for det ikke behandles flere personopplysninger om barn i barnehage og skole, foresatte og ansatte, enn det som er nødvendig for å løse en bestemt oppgave. Skole- og barnehageeier skal i den forbindelse iverksette tiltak som ivaretar dataminimering:

1. Et eksempel på tiltak som kan sikre at det ikke samles inn flere personopplysninger enn det som er nødvendig, kan være å redusere bruken av fritekstfelter. Det er Utdanningsdirektoratets erfaring at fritekstfelter ofte gjør at den registrerte oppgir flere personopplysninger enn det skole- og barnehageeier trenger for å løse en bestemt oppgave. I stedet for fritekstfelter kan man bruke avkrysningsbokser hvor man ber den registrerte krysse av for den informasjonen man faktisk har bruk for.
2. Et annet eksempel på tiltak som kan sikre at det ikke samles inn flere personopplysninger enn det som er nødvendig, kan være å gjøre et representativt utvalg av personopplysninger.

Utdanningsdirektoratet og flere andre offentlige virksomheter ønsker ofte å bruke personopplysninger til forskning av forbedringshensyn.

I stedet for å samle inn personopplysninger fra for eksempel alle lærere som gjennomfører videreutdanning, vil det kunne være lurt å ta stilling til hvor mange av disse lærernes personopplysninger som trengs for at man skal få god nok representasjon i forskningen.

## 4. Riktighet

Personopplysningene som behandles skal være korrekte.

Det betyr at skole- og barnehageeier skal sørge for at personopplysninger som er feil rettes og oppdateres. Å korrigere personopplysninger om barn i barnehage og skole, foresatte og ansatte i barnehage og skole, er oppgaver som av praktiske hensyn må ligge hos den enkelte skole og barnehage, og ikke hos kommunen som skole- og barnehageeier.

Skole- og barnehageeier plikter å legge til rette for at retting og oppdatering kan skje, og å sette føringer for hvordan skoler og barnehager skal arbeide med personopplysninger.

> Eksempler på tiltak som skole- og barnehageeier kan etablere for å sikre at personopplysninger behandles med riktighet:
>
> a. Sørge for at den læringsplattformen som brukes på skolene i kommunen regelmessig varsler brukere (barn i skolen, foresatte og ansatte) om at de må kontrollere sine personopplysninger. Mange banker gjør dette ved innlogging til for eksempel nettbank.
>
> b. Tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, straks slettes eller korrigeres.
>
> c. Dersom back-up brukes for å gjenopprette data, må skole- og barnehageeier også ha rutiner for gjennomgang av disse systemene for å sørge for at nødvendig korrigering skjer også i back-up.

## 5. Lagringsbegrensning

Personopplysningene som behandles skal ikke lagres lengre enn nødvendig for å oppnå formålet med behandlingen.

Lagringsbegrensning betyr at skole- og barnehageeier skal sørge for at personopplysningene blir slettet (eller anonymiseres), når det ikke lenger er bruk for dem. Det vil som regel ikke lenger være nødvendig å lagre personopplysningene når formålet med behandlingen er oppfylt.

Datatilsynet har i sin veileder anbefalt at det bør innføres tidsfrister for sletting i de systemene som brukes, for eksempel i læringsplattformer. Videre anbefales det at skole- og barnehageeier ved jevne mellomrom har gjennomganger i læringsplattformen for å sikre at personopplysninger ikke oppbevares lengre enn nødvendig.

## 6. Integritet og konfidensialitet (fortrolighet)

Personopplysningene som behandles skal beskyttes slik at uvedkommende ikke får tilgang til personopplysningene og slik at personopplysningene ikke endres utilsiktet. I dette ligger det blant annet at personopplysninger skal sikres i forhold til risiko. Jo mer sensitive personopplysningene er, jo bedre skal de sikres.

**Konfidensialitet** betyr at skole- og barnehageeier skal sørge for at bare de som trenger tilgang til personopplysningene får tilgang til dem. Skole- og barnehageeier skal med andre ord ha et bevisst forhold til hvem som får og hvem som ikke får tilgang til systemer som inneholder personopplysninger. Dette kalles tilgangsstyring.

**Integritet** betyr at skole- og barnehageeier skal ha et bevisste forhold til hvem som skal ha adgang til å endre personopplysninger om barn i skole og barnehage, foresatte og ansatte som er lagret i ulike systemer. Det er ikke gitt at alle brukere som har tilgang til et system hvor personopplysninger lagres har behov for å endre personopplysningene. Ofte vil man kunne skille mellom lesetilgang og skrivetilgang. Det er skole- og barnehageeiers ansvar å sette

føringer for hvem som skal ha hvilke tilganger slik at personopplysninger ikke endres eller slettes uten at det er grunnlag for det.

For å oppnå integritet og konfidensialitet, anbefaler Utdanningsdirektoratet skole- og barnehageeiere stiller følgende spørsmål:

a. Har man et bevisst forhold til hvem som skal være bruker i et system? Skole- og barnehageeier kan enten selv kontrollere hvem som skal ha tilgang til systemer som læringsplattformer, eller sette føringer for hvordan skole- og barnehageledere skal ha tilgangsstyring.

> Utdanningsdirektoratet anbefaler at det bare er de som trenger tilgang til et system for å løse sine arbeidsoppgaver, som skal ha det.

b. Har man et bevisst forhold til hvem som skal ha de ulike brukertilgangene? Skole- og barnehageeier kan enten selv kontrollere hvem som skal ha administrasjonsrettigheter, lesetilgang eller skrivetilgang til systemer som læringsplattformer, eller sette føringer for hvem som bør ha hvilke tilganger. Generelt anbefaler Datatilsynet at personopplysninger ikke skal gjøres tilgjengelig for et ubegrenset antall mennesker.

c. Har man sørget for at systemer har logger hvor skole- og barnehageeier kan spore hvilke endringer som gjøres? Slik logging kan brukes for å håndtere sikkerhetsbrudd, for eksempel hvis personopplysninger blir publisert uten at man har et rettslig grunnlag som sier at personopplysningene kan publiseres. Logging kan også ha en preventiv effekt; når brukerne av et system er klar over at endringer blir loggført, vil kanskje også risikoen for at de endrer personopplysninger som ikke skal endres reduseres.

d. Sørg for at systemer er sikret mot sårbarheter som angrep og uhell.

## 7. Ansvarlighet

Skole- og barnehageeiere skal etterleve personvernforordningen. Dette kan virke selvsagt, men personvernforordningen slår fast at det er den behandlingsansvarlige som er ansvarlig for å etterleve personvernforordningen.

Ansvarlighet innebærer at skole- og barnehageeier skal dokumentere at personopplysninger behandles i samsvar med reglene i personvernforordningen. Det er ikke nok at man ha

ansvaret – man må vise at man faktisk tar ansvaret.

Ansvarlighet innebærer blant annet at skole- og barnehageeier skal etablere nødvendige organisatoriske og tekniske tiltak for å sikre at personvernforordningen etterleves. Hva som er et nødvendig tiltak vil avhenge av personvernrisiko, noe som betyr at skole- og barnehageeier må gjennomføre risikovurderinger.

Ansvarlighet kan for eksempel dokumenteres ved at personvern inntas i en kommunes styringssystem eller internkontrollsystem.

For offentlige barnehager og skoler vil barnehage- og skoleeier være kommunen, mens for private barnehager og skoler er ofte barnehage- eller skoleledelsen også barnehage- og skoleeier.