Retningslinje for behandling av personopplysninger ved DMMH

Vedtatt av styret: 09.04.2019 Sist revidert: 20.11.2020

Innhold

1 Definisjoner

1.1 Personopplysninger

Personopplysninger er all informasjon som kan knyttes til en bestemt enkeltperson. Informasjonen kan foreligge som tekst, bilder, video, lydopptak eller elektroniske spor, for eksempel IP-adresser eller aktivitetslogger i IT-systemer. For at informasjonen skal regnes som personopplysninger, må det være mulig å identifisere den eller de personer som opplysningene knytter seg til.

Pseudonyme opplysninger om enkeltpersoner regnes som personopplysninger. Dette er opplysninger hvor identiteten er skjult (identifiserende informasjon, for eksempel navn eller fødselsnummer, er fjernet), men det er likevel mulig å finne ut hvem opplysningene handler om (re-identifisering). I forbindelse med eksamenssensur, kan re-identifisering av personopplysninger – studentenes karakterer – skje ved at kandidatnummer erstattes med studentnavn etter at sensuren har falt.

Dersom det ikke på noen måte er mulig å identifisere hvem opplysningene knytter seg til, er opplysningene anonyme. Anonyme opplysninger regnes ikke som personopplysninger og omfattes derfor ikke av reglene i GDPR.

1.2 Sensitive personopplysninger

Sensitive personopplysninger refererer til et begrenset antall opplysningstyper som gjelder særlige personlige forhold. Informasjon (om enkeltpersoner) som tilhører følgende opplysningstyper regnes som sensitive:

- rase eller etnisk opprinnelse,
- politisk oppfatning,
- religiøs overbevisning eller livssyn,
- genetiske opplysninger,
- biometriske opplysninger (som har til hensikt å entydig identifisere en fysisk person),
- helseopplysninger,
- opplysninger om seksuelle forhold eller seksuelle orientering,
- fagforeningsmedlemskap

1.3 Taushetsbelagte personopplysninger

Personopplysninger som gjennom lov er definert som taushetsbelagte, altså unntatt offentlighet.

1.4 Behandling av personopplysninger

Behandling er all bruk av personopplysninger i undervisning, administrasjon, forskning og formidling. Dette kan omfatte en rekke bruksformer, for eksempel innsamling, strukturering, analyse, lagring, endring, gjenfinning, utlevering, sammenstilling, publisering eller sletting.

1.5 Behandleransvarlig

Behandlingsansvarlig er vedkommende virksomhet (DMMH) som bestemmer hva som skal skje med personopplysningene (hva opplysningene skal brukes til og hvilke tekniske hjelpemidler som skal anvendes i behandlingen av dem). Den behandlingsansvarlige skal sørge for at bruken av personopplysninger skjer på en måte som er i samsvar med reglene i GDPR og ikke krenker de registrertes personvern.

1.6 Den registrerte

Den registrerte er vedkommende person eller personer som opplysningene handler om. Dette kan for eksempel være studenter, ansatte, gjester eller respondenter i spørreundersøkelser.

1.7 Databehandler

Databehandler er en virksomhet (eller enkeltperson) som utfører databehandlingsoppdrag på vegne av den behandlingsansvarlige (DMMH). Databehandlere kan for eksempel være kommersielle virksomheter som leverer nettbaserte tjenester eller universiteter/høyskoler som drifter IT-tjenester (hvor personopplysninger behandles) for andre institusjoner i sektoren. Leverandører av skytjenester, for eksempel systemer som plagiatkontroll eller læringsplattformer, er konkrete eksempler på databehandlere.

1.8 Samtykke

Samtykke er en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar den planlagte/foreslåtte behandlingen av personopplysninger. Behandlingsansvarlig må kunne dokumentere at samtykke er gitt.

1.9 Lovlig grunn (behandlingsgrunnlag)

Lovlig grunn (behandlingsgrunnlag) er ulike mekanismer definert i GDPR som gjør det lovlig for behandlingsansvarlig å behandle personopplysninger om de registrerte. Det må derfor finnes én eller flere lovlige grunner for all behandling av personopplysninger i administrasjon, undervisning, forskning og formidling.

1.10 Personvernansvarlig

En personvernansvarlig er en ressursperson som skal hjelpe behandlingsansvarlig eller databehandler (tjenesteleverandøren) i spørsmål som omhandler personvern og behandling av personopplysninger.

2 Formål og omfang

2.1 Formål

Formålet med retningslinjen er å sikre at personopplysninger om søkere, studenter, ansatte og andre som DMMH behandler personopplysninger om, blir behandlet i samsvar med gjeldene lovverk. Retningslinjen skal også sikre at den enkelte ved forespørsel får innsyn i de opplysningene som er registrert om vedkommende, og anledning til å be om sletting der dette er mulig. Retningslinjen skal også sikre at innsamling og bearbeiding av personopplysninger i forbindelse med forskning, skjer i tråd med gjeldene lovverk

2.2 Hvem retningslinjene gjelder for

Retningslinjen gjelder for ansatte, studenter og andre som har tilgang til og/eller bearbeider og forvalter personopplysninger gjennom DMMHs IKT-infrastruktur

2.3 Når retningslinjene gjelder

Retningslinjen gjelder for alle virksomhetsområder ved DMMH. Retningslinjen gjelder for alle tilfeller der personopplysninger (vanlige eller sensitive) helt eller delvis behandles elektronisk. Retningslinjen gjelder også ved manuell behandling av personopplysninger som inngår i, eller skal inngå i et register.

3 Krav til behandling av personopplysninger ved DMMH

Personopplysninger skal behandles i tråd med Lov om behandling av personopplysninger (personopplysningsloven), som bygger på EUs personvernforordning. Behandling skal skje etter følgende prinsipper, hentet fra artikkel 5 av forordningen:

3.1 Lovlig, rettferdig og gjennomsiktig

At behandlingen av personopplysninger må være lovlig innebærer først og fremst at det må finnes et rettslig grunnlag for en planlagt behandling av personopplysninger. Personvernforordningens artikkel 6 er en liste over rettslige grunnlag og minst ett av disse må være oppfylt for at behandlingen skal være lovlig. Prinsippet om lovlighet kan også sies å inkludere alle de øvrige prinsippene og reglene for behandling av personopplysninger som en behandlingsansvarlig må oppfylle.

At behandlingen av personopplysninger må skje rettferdig betyr at den skal gjøres i respekt for de registrertes interesser og rimelige forventninger. Behandlingen skal være forståelig for de registrerte og ikke foregå på skjulte eller manipulerende måter. Gjennomsiktig betyr i denne sammenheng at bruken av personopplysninger skal være oversiktlig og forutsigbar for den opplysningene gjelder. Gjennomsiktighet bidrar til å skape tillit og det setter enkeltpersonen i stand til å bruke sine rettigheter og ivareta sine interesser.

3.2 Formålsbegrensning

Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist. Alle formål skal være forklart på en måte som gjør at alle berørte har samme forståelse av hva personopplysningene skal brukes til. At formålet skal være legitimt innebærer at det i tillegg til å ha et rettslig grunnlag også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer. Personopplysninger kan ikke gjenbrukes til formål som er uforenelig med det opprinnelige formålet.

3.3 Dataminimering

Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen. Dersom personopplysninger ikke er nødvendige for å oppnå formålet, skal man heller ikke samle dem inn.

3.4 Riktighet

Personopplysninger som behandles skal være korrekte og skal om nødvendig oppdateres. Dette betyr at den behandlingsansvarlige må sørge for straks å slette eller rette personopplysninger som er uriktige ut i fra de formålene de er samlet inn for.

3.5 Lagringsbegrensning

Prinsippet om lagringsbegrensning innebærer at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for. Unntak skal kun gjøres der opplysningene er arkivpliktige.

3.6 Integritet, konfidensialitet og tilgjengelighet

Personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet og tilgjengelighet beskyttes. Dette betyr at den behandlingsansvarlige må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger.

3.7 Ansvarlighet

Prinsippet om ansvarlighet understreker ansvaret for å opptre i samsvar med reglene for behandling av personopplysninger. Dette ansvaret ligger på alle virksomheter som behandler personopplysninger. Det er ikke nok bare å ha ansvar – man må vise at man tar ansvar. Det betyr at organisasjonen må kunne dokumentere at gjennomføring av tiltak for å etterleve personvernforordningen. Organisasjonen må opptre proaktivt og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

4 Om behandling av personopplysninger ved DMMH

4.1 Risikovurdering ved nye systemer

Dersom det skal tas i bruk nye systemer som behandler personopplysninger skal det i forkant gjennomføres en risikovurdering. Den som skal være systemeier skal sammen med personvernansvarlig gjennomføre en risikovurdering av systemet og dokumentere denne. Dette skal gjøres i forkant av anskaffelse og inngå i vurderingen av anskaffelse.

4.2 Databehandleravtale

Systemeier har ansvar for at det inngås skriftlig databehandleravtale i de tilfeller hvor databehandler skal behandle personopplysninger på vegne av DMMH.

4.3 Rutinebeskrivelser

For alle administrative eller studieadministrative prosesser som innebærer repetitiv behandling av personopplysninger skal det utarbeides rutinebeskrivelser. Med repetitiv menes at behandlingsformen gjentar seg jevnlig, eksempelvis søknader, klagebehandling og lignende. Rutinebeskrivelsen skal beskrive hvordan personopplysningene behandles, i hvilke system(er) og hvordan man forhindrer sikkerhetsavvik.

4.4 Lagring, sletting og arkivering

Personopplysninger skal ikke lagres lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen hvis ikke annet er bestemt i lov eller f.eks. i forbindelse med finansiering av forskning. Den enkelte ansatt er ansvarlig for å slette personopplysninger som er lagret på vedkommende sitt personlige brukerområde. Systemeier er ansvarlig for å følge opp at sletting skjer i de systemer som vedkommende er systemeier for.

4.5 Samtykke

Der hvor behandling av personopplysninger ikke følger av lovgivning, skal det alltid hentes inn samtykke. For at samtykke skal være gyldig må det være:

- Frivillig – gitt uten press eller tvang
- Spesifikt – beskriver nøyaktig hva man samtykker til
- Informert – hvem behandlingsansvarlig er, formål, hvilke opplysninger, rett til å trekke tilbake samtykke
- Utvetydig – Gitt ved aktiv handling (signering, hake av boks, klikke på knapp eller lignende)
- Dokumenterbart – Samtykke skal kunne dokumenteres i ettertid
- Mulig å trekke – Samtykke skal kunne trekkes tilbake når som helst

4.6 Bruk av e-post

I tråd med Datatilsynets føringer skal følgende ikke sendes på e-post uten kryptering eller passordbeskyttelse:

- sensitive personopplysninger
- taushetsbelagte personopplysninger
- store mengder med personopplysninger samlet (f.eks. i excel-ark, lister i word eller lignende)
- personnummer (11 siffer, fødselsdato alene kan sendes)

Føringen gjelder både e-post til eksterne og interne mottakere. Dersom opplysninger sendes med passordbeskyttelse, må passordet meddeles mottakeren på annen måte (sms, telefon, muntlig)

4.7 Bilde, video og lydopptak

Fotografering må skje i tråd med åndsverksloven § 104. Det vil si at bilde ikke kan gjengis eller vises offentlig uten samtykke av den avbildede unntatt når:

- avbildningen har aktuell og allmenn interesse
- avbildningen av personen er mindre viktig enn hovedinnholdet i bildet
- bildet gjengir forsamlinger, folketog i friluft eller forhold eller hendelser som har allmenn interesse
- eksemplar av avbildningen på vanlig måte vises som reklame for fotografens virksomhet og den avbildede ikke nedlegger forbud
- bildet brukes som kriminalitetsbekjempelse, eller
- offentliggjort personbilde i form av fotografisk verk kan mot vederlag gjengis i tekst av biografisk innhold.

Video- og/eller lydopptak av personer som kan gjenkjennes skal kun skje etter samtykke fra den enkelte. Dersom innholdet skal publiseres, må også publiseringen skje etter samtykke fra den enkelte. Samtykke må gis i tråd med punkt 4.5. I vurderingen skal det tas ekstra hensyn dersom barn gjengis i bilde, video eller lydopptak.

Ved opptak i forbindelse med undervisning vises det til retningslinjer for behandling av personopplysninger ved digital undervisning ved DMMH og disse retningslinjene kapittel 7.

4.8 Behandling av taushetsbelagte og/eller sensitive personopplysninger

All behandling av taushetsbelagte og/eller sensitive personopplysninger skal skje i Public360 eller annet godkjent fagsystem. Slike opplysninger skal ikke lagres ned på den enkeltes privatområde eller direkte på fysiske enheter som bærbar, minnepenn eller lignende.

4.9 Papirutgave av taushetsbelagte og/eller sensitive personopplysninger

Dersom det er nødvendig å oppbevare papirutgave av dokumenter med taushetsbelagte og/eller sensitive personopplysninger, skal dette skje i låsbart skap. Skapet skal stå i kontor eller i annet areale som er låst utenom ordinær arbeidstid.

4.10 Særlig om behandling av personopplysninger i forbindelse med skikkethetssaker eller fusk/mistanke om fusk.

Dokumenter eller opplysninger som angår en students skikkethet, mistanke om fusk eller fusk, skal ikke sendes med e-post. Det skal benyttes Digipost eller vanlig postgang. Behandling av dokumenter skal skje i tråd med punkt 4.8. Adgangen til saksdokumentene i Public 360 skal begrenses til saksbehandler(e), studenten selv, de som har behov for innsyn i saken og systemeier.

4.11 Utlevering av personopplysninger til eksterne

Informasjon som er innsamlet og lagret for generell personalforvaltning og om studenter for administrative formål, skal normalt ikke utleveres til utenforstående. Unntak skal gjøres der de som ber om opplysningene har rett til innsyn etter offentlighetslova, eller har lovhjemmel for sitt innsyn.

5 Særlig om behandling av personopplysninger i forskning

5.1 Henvisning til personopplysningsloven

Det vises her til personopplysningslovens paragrafer, som definerer tilfeller som er unntatt kravene i personvernforordningen (GDPR). Det vises spesielt til kapittel 3.

5.2 Melding til NSD

Forsknings- og studentprosjekter, som behandler personopplysninger elektronisk helt eller delvis, skal meldes til Norsk senter for forskningsdata (NSD). Det samme gjelder prosjekter der personopplysninger behandles manuelt hvis disse inngår eller skal inngå i et personregister.

NSD er ikke lenger personvernombud for forskning, og har kun en rådgiverrolle. Prorektor for FoU og oppdrag, vil være personvernansvarlig for forskning.

Forsknings- og studentprosjekter som behandler personopplysninger, skal fortsatt meldes til NSD. NSD skal vurdere om prosjektet tilfredsstiller kravene i EUs personvernforordning.

Behandlingen av personopplysninger kan ikke settes i gang før NSD har gitt tilbakemelding til prosjektleder og/eller forskningsansvarlig om at den planlagte behandlingen vurderes å være i samsvar med EUs personvernforordning.

Dersom student eller forsker skal samle inn data i utlandet, gjelder meldeplikten til NSD ved behandling av personopplysninger på lik linje som ved datainnsamling i Norge samt lovgivningen i vertslandet.

Prosjektleder, eller veileder ved studentprosjekt, er ansvarlig for at prosjektet blir meldt til NSD.

5.3 Forhåndsgodkjenning fra REK

Helseforskning skal være forhåndsgodkjent av Regional komite for medisinsk og helsefaglig forskningsetikk (REK) før prosjektet kan starte, jf. helseforskningsloven §33. REK gjør en forskningsetisk vurdering av prosjektet.

Etter at EUs personvernforordning har tredd i kraft vil ikke REKs forhåndsgodkjenning lenger være et tilstrekkelig lovlig grunnlag for behandling av personopplysninger i helseforskning. Behandlingen av personopplysninger må også ha et lovlig grunnlag i EUs personvernforordning.

En forskningsetisk vurdering omfatter også en vurdering av behandlingen av personopplysninger i prosjektet, men denne vil ikke være bindende for Datatilsynet ved et eventuelt tilsyn.

Prosjektleder vil ha ansvar for behandlingen av personopplysninger men skal rådføre seg med personvernansvarlig for forskning før søknad sendes.

5.4 Personvernansvarlig for forskning

Prorektor for FoU og oppdrag er personvernansvarlig for forskning dersom rektor ikke har bestemt annet.

Ved forskningsprosjekter skal personvernansvarlig for forskning:

- sørge for rutiner, infrastruktur og internkontrollsystemer for forskningsvirksomheten i henhold til gjeldende lovverk og retningslinjer, samt at disse implementeres i praksis.
- være involvert når søknad sendes til REK / melding sendes til NSD, og skal informeres om resultatet.
- ha oversikt over DMMHs pågående forskningsprosjekter
- stanse forskning som er etisk/juridisk uforsvarlig eller i strid med prosjektets forutsetninger
- sikre at forskning ved DMMH planlegges, organiseres, gjennomføres og avsluttes i samsvar med gjeldende personvernlovgivning

5.5 Prosjektleders ansvar

Dersom det kun er én forsker, er vedkommende å regne som prosjektleder.

Ved forskningsprosjekter skal prosjektleder:

- ha det operative ansvaret og sørge for internkontroll ved gjennomføringen av forskningsprosjektet, fra planlegging til avslutning, herunder at krav i relevant lovverk og forskningsetiske retningslinjer etterleves.
- sørge for nødvending søknad til REK eller melding til NSD
- legge frem søknad og meldeskjema dersom personvernansvarlig for forskning ber om det
- dersom det er trolig at behandlingen av personopplysninger har høy risiko for personers rettigheter eller friheter, foreta en risikovurdering og rådføre seg med NSD om mulige konsekvenser. Undersøkelsen skal være i tråd med GDPR artikkel 35.
- lage en datahåndteringsplan som beskriver hvordan forskningsdata skal samles inn, lagres, deles og slettes, slik at dataene blir håndtert sikkert og forsvarlig. Planen skal oppdateres underveis i prosjektet og dokumentere hvordan forskningsdata blir behandlet. Planen skal også inkludere vurderinger knyttet til etikk og personvern.

- sørge for tilgangsstyring dersom det er behov for konfidensialitet ved behandling av personopplysninger i prosjektet
- sørge for at relevante og nødvendige dokumentasjonskrav ivaretas
- sette seg inn i relevant lovgivning for behandling av personopplysninger
- følge opp eventuelle henvendelser fra forskningsdeltakere angående innsyn m.m.
- umiddelbart melde eventuelle avvik ved brudd på informasjonssikkerhet og personvern i henhold til gjeldende rutine (se punkt 7.1)

5.6 Veileder for studentprosjekt

Veileder skal

- alltid opptre som prosjektleder for studentprosjekter på bachelor- og mastergradsnivå
- sikre at studenten er kjent med denne retningslinjen, samt lovgivning rundt behandling av personopplysninger
- sikre at studentene melder sine prosjekter

5.7 Lagring av forskningsdata

Personopplysninger skal ikke lagres lenger enn det som er nødvendig for formålet de ble innhentet for, hvis ikke annet er bestemt i lov eller i forbindelse med finansiering av forskningen.

Der hvor det er mulig, skal personopplysningene pseudonymiseres eller anonymiseres.

Pseudonymiserte opplysninger regnes fortsatt som personopplysninger og må behandles etter gjeldende lovverk. Pseudonymisering brukes kun for å øke sikkerhetsgraden.

For at personopplysninger skal regnes som anonymisert skal det være umulig å knytte opplysningene til enkeltpersoner. Opplysningene regnes som anonymisert når de ikke kan knyttes til en gruppe på mindre enn 5 personer. Anonymiserte opplysninger er ikke lenger personopplysninger og reguleres derav ikke av personvernlovgivning.

5.8 Avslutning av forskningsprosjekter

Ved prosjektets slutt skal prosjektleder:

- sørge for at prosjektmedarbeidere ikke lenger har tilgang til personopplysningene
- anonymisere eller slette personopplysningene, dersom ikke lov eller krav i godkjenning av finansiering av prosjektet tilsier noe annet.
- sende nødvendig bekreftelser til REK og NSD

Prosjektleder (veileder) er ansvarlig for at dette blir gjort også i avslutningen av studentprosjekter

5.9 Kontroll og etterlevelse i forskningsprosjekter

Personvernansvarlig for forskning skal

- sørge for at et uttrekk av forskningsprosjekter og studentprosjekter blir kontrollert for å sikre at retningslinjen blir fulgt opp.
- kontrollere at alle prosjekter gjør nødvendige søknader/meldinger til REK/NSD
- kontrollere at alle prosjekter avsluttes i tråd med punkt 5.7

- sende rapport til personvernansvarlig på slutten av kalenderåret, som kort beskriver hvilke prosjekter (ikke studentprosjekter) som er avsluttet, og bekrefte at alle disse er gjennomført og avsluttet i tråd med retningslinjen.

6 Særlig om behandling av personopplysninger i forbindelse med arbeidskrav

6.1 Bilde, video- og lydopptak ved arbeidskrav eller i praksis

Bilde, video- og/eller lydopptak skal kun skje når dette er en planlagt del av et arbeidskrav eller inngår som en del av praksis.

Dersom studenter skal ta bilde eller video,- og/eller lydopptak av personer kreves det samtykke fra personen i tråd med punkt 4.5. Dersom personen er mindreårig kreves samtykke fra foreldre eller foresatte.

Ved arbeidskrav eller i praksis, er faglærer ansvarlig for å sikre at nødvendig samtykke innhentes.

Signert samtykkeskjema skal leveres som vedlegg til det som skal leveres til vurdering.

Når det skal bes om samtykke fra foreldre/foresatte i praksis, skal dette skje gjennom barnehagen ved praksislærer. Studenten skal ikke kontakte foreldre/foresatte direkte, men kan besvare eventuell henvendelse fra foreldre/foresatte.

Samtykke skal innhentes på DMMHs samtykkeskjema, eller skjema som oppfyller kravene til punkt 4.5 og er godkjent av personvernansvarlig.

6.2 Godkjent utstyr for bilde, video- og lydopptak

Utstyr som studentene bruker for å ta bilde, video- og/eller lydopptak skal som utgangspunktet lånes hos DMMHs AV-ansvarlig. Utstyret skal ikke være koblet direkte mot internett. Det vil si at man f.eks. ikke kan bruke en mobiltelefon for å ta lydopptak. Unntak fra dette kan kun gjøres etter avtale med personvernansvarlig

Dersom studenten skal bruke privat utstyr, skal dette forhåndsgodkjennes av personvernansvarlig.

6.3 Oppbevaring og publisering

Bilde, video- eller lydopptak skal som utgangspunkt oppbevares på den enheten hvor det ble tatt opp, og slettes når det ikke lenger er bruk for bildet, video- eller lydopptaket.

Dersom bilde, video- eller lydopptak skal leveres til vurdering eller inngå i noe som skal levers til vurdering, skal dette fremgå av samtykkeskjema. Bilde, video- eller lydopptak skal behandles i tråd med retningslinjen. Opplasting skal da skje enten i læringsplattform (p.t. itslearning) eller system for digital eksamen (p.t. WiseFlow). Bilde, video- eller lydopptaket skal aldri sendes på e-post.

Bilde, video- eller lydopptak skal slettes når det ikke lenger er behov for å oppbevare det, med mindre annet er avtalt i samtykkeskjema.

7 Særlig om rettslig grunnlag og formålsopplysning ved digital undervisning

7.1 Formål

DMMH skal tilby undervisning på et høyt faglig nivå. Det overordnede formålet med å behandle personopplysninger gjennom digital undervisning er å øke studentenes kunnskap.

Formålet med undervisningen skal være tydeliggjort for den eller de personene som er med i opptaket eller direktestrømmen[1]. Dersom et emne har flere undervisnings- eller vurderingsaktiviteter av samme karakter, for eksempel en forelesningsrekke, kan formålet beskrives felles for undervisningsaktiviteter som er like.

7.2 Rettslig grunnlag

For at behandling av personopplysninger skal være lovlig, må behandlingen ha et gyldig behandlingsgrunnlag (lovhjemmel) i personvernforordningen artikkel 6. Det rettslige grunnlaget skal oppgis sammen med formålet for undervisningen, se også retningslinjer for personvern ved digital undervisning, kapittel 5, om informasjon ved opptak.

Minst ett av de følgende rettslige grunnlagene må foreligge for at behandlingen av personopplysninger skal være lovlig:

7.2.1 Grunnlag i avtale

Arbeidsavtalen og arbeidsgivers styringsrett gir DMMH anledning til å bestemme at ansatte skal gjennomføre undervisningen digitalt. Dette gjelder tilsvarende for avtaler med ekstern faglærer.

7.2.2 Nødvendig for å gjennomføre en oppgave i allmenhetens interesse

Allmennhetens interesse vil som hovedregel være det rettslige grunnlaget når det er nødvendig å behandle studenters personopplysninger ved digital undervisning, jf. personvernforordningen artikkel 6 nr. 1.[2]

Det må begrunnes om aktiv studentdeltakelse er *påkrevd* – det vil si obligatorisk – for å oppnå formålet med undervisningen, eller om formålet kan oppnås ved frivillighet, eventuelt ved opptak av kun faglæreren. Er det obligatorisk må dette komme tydelig frem i studie- og emneplanen.

Å oppfordre og legge til rette for aktiv deltakelse krever ingen særskilt begrunnelse, bare informasjon om at studentene selv bestemmer om de vil delta med lyd/bilde i undervisningen.

7.2.3 Samtykke som rettslig grunnlag

Samtykke vil som hovedregel ikke være et egnet rettslig grunnlag grunnet manglende reell frivillighet og utfordringer med å håndtere følgene av tilbaketrekking av et samtykke.

Et gyldig samtykke etter personvernforordningen forutsetter en informert, frivillig, utvetydig, spesifikk erklæring, som fritt kan trekkes tilbake uten konsekvenser for den enkelte.

[1] Jf. Retningslinjer for personvern ved digital undervisning, kapittel 5.
[2] Jf. også universitet- og høyskoleloven §§ 1-3, 3-8, 4-2 og 4-3.

Når det ikke er annet egnet rettslig grunnlag (se punkt 7.2.1 og 7.2.2, og det ikke er lagt til rette for å reservere seg fra å delta med lyd og bilde, må det innhentes samtykke, jf. punkt 1.8 og 4.5 i disse retningslinjene.

DMMH har utarbeidet et eget samtykkeskjema for studenter som ligger på våre nettsider.

8 Håndtering av avvik

8.1 Rapportering av avvik

Dersom det oppstår et avvik, skal dette umiddelbart og uten unødig opphold rapporteres til personvernansvarlig både skriftlig (til personvern@dmmh.no) og muntlig. Alle ansatte, studenter og andre som er knyttet til DMMH er ansvarlig for å rapportere eventuelle avvik de oppdager.

8.2 Rapportering fra personvernansvarlig

Personvernansvarlig skal

- rapportere avviket til rektor og eventuelt andre aktuelle ledere.
- varsle Datatilsynet i tråd med «Varslingsrutiner ved sikkerhetshendelse – Datatilsynet»
- varsle de som avviket rammer i tråd med «Varslingsrutiner ved sikkerhetshendelse – De registrerte»
- varsle systemeier dersom varsel kom fra andre enn systemeier

8.3 Systemeiers kontakt med databehandler

Dersom avviket skyldes feil i datasystem, skal systemeier ta dette videre med databehandler. Det skal kreves rapport fra databehandler som sendes til personvernansvarlig for eventuell videresending til Datatilsynet og de registrerte.

8.4 Oppfølging ved menneskelig svikt

Dersom avviket skyldes menneskelig svikt, skal personvernansvarlig sikre at vedkommende får nødvendig opplæring i lover og retningslinjer for behandling av personopplysninger.

9 Roller og ansvar

9.1 Styret

- har det overordnede ansvaret for behandling av personopplysninger ved DMMH

9.2 Rektor

- er øverste behandlingsansvarlig for behandling av personopplysninger ved DMMH.
- skal orientere styret om behandling av personopplysninger i virksomheten i årsrapporten.

9.3 Prorektorer

- er ansvarlig for etterlevelsen av krav til behandling av personopplysninger i sin avdeling
- skal ha en løpende oversikt over hvilke IKT-systemer som anvendes av avdelingens ansatte
- skal sikre at deres ansatte har tilstrekkelig opplæring i håndtering personopplysninger og kan ivareta sin plikt til å løpende vurdere risiko ved nye prosjekt og behandlinger, samt melde avvik ved brudd på informasjonssikkerheten

9.4 Studiesjef og administrasjonssjef

- er ansvarlig for etterlevelsen av krav til behandling av personopplysninger i sin avdeling
- skal sikre at alle det finnes rutinebeskrivelse for alle gjentakende saksbehandling. Rutinebeskrivelsen skal inneholde informasjon om hvordan personopplysninger behandles og hvordan sikkerheten rundt denne behandlingen ivaretas.
- skal ha en løpende oversikt over hvilke IKT-systemer som anvendes av avdelingens ansatte
- skal sikre at deres ansatte har tilstrekkelig opplæring i håndtering personopplysninger og kan ivareta sin plikt til å løpende vurdere risiko ved nye prosjekt og behandlinger, samt melde avvik ved brudd på informasjonssikkerheten

9.5 IT-leder

- skal ha en løpende oversikt over DMMHs IKT-infrastruktur og at informasjonssikkerheten i og mellom systemene ivaretas
- er ansvarlig for at alle ansatte og studenter ved DMMH har tilgang til tjenester og materiell slik at brukerne kan ivareta de registrertes personvern
- Er ansvarlig for gjennomføring av sikkerhetskrav til DMMHs IKT-infrastruktur

9.6 Personvernansvarlig

- skal gi DMMHs ledelse og ansatte informasjon og råd om forpliktelser DMMH har i henhold til relevant personvernlovgivning
- skal sikre at det er foretatt risikovurderinger før nye systemer tas i bruk, samt risikovurdering av eksisterende systemer, og at slike vurderinger er dokumentert.
- skal kontrollere overholdelsen av EUs personvernforordning og annen relevant lovgivning om vern av personopplysninger og interne retningslinjer og rutiner
- skal betjene personvern@dmmh.no
- skal være kontaktpunkt for Datatilsynet og de registrerte
- skal holde seg informert om og følge opp avvik ved brudd på personvernet

9.7 Personvernansvarlig for forskning

- skal gi råd om hvordan DMMH som behandlingsansvarlig best mulig kan ivareta personverninteressene i forskningsprosjekter
- skal motta meldinger om behandlinger av personopplysninger i forskningsprosjekter

Se for øvrig punkt 5.4

9.8 Prosjektansvarlig og veiledere

Se henholdsvis punkt 5.5 og 5.6

9.9 Systemeiere

- er ansvarlig for at IT-systemets utvikling, forvaltning og/eller drift møter kravene til informasjonssikkerhet, herunder behandling av personopplysninger
- skal gjennomføre risikovurdering av nye systemer før de tas i bruk
- er ansvarlig for at det inngås databehandleravtaler med de aktuelle leverandørene

9.10 Alle brukere

- som skal behandle personopplysninger, er ansvarlig for å sette seg inn i relevant lovgivning for behandling av personopplysninger

- er ansvarlig for å gjøre seg kjent med denne retningslinjen
- er pliktige til å melde avvik (uønskede hendelser) ved brudd på personvern etter punkt 7.1