Retningslinje for Behandling av personopplysninger

Type dokument	Retningslinje
Forvaltes av	Direktør for Organisasjon og infrastruktur
Godkjent av	Direktør for Organisasjon og infrastruktur
Gjelder fra	12.06.2023
Neste revisjon innen	12.06.2025
Klassifisering	Åpen
Referanse ISO	ISO 27002:2022; 5.10, 5.34, 8.10, 8.11
Referanse NSMs grunnprinsipper for IKT-sikkerhet	
Referanse LOV/Regel	EUs personvernforordning artikkel 5 (grunnleggende prinsipper) og 24
Referanse interne dokumenter	Retningslinje for behandling av personopplysninger er underlagt NTNUs Politikk for informasjonssikkerhet og IKT-reglementet

1. Formål

Formålet med retningslinjen er å

a. sikre at personopplysninger om søkere, studenter, ansatte, forskningsdeltakere og andre som NTNU behandler personopplysninger om, blir behandlet i samsvar med gjeldende lovverk
b. beskytte den enkelte mot at personvernet blir krenket
c. sikre at den enkelte ved forespørsel får innsyn i de opplysninger som er registrert om vedkommende
d. legge forholdene til rette for forskning som omfatter innsamling og bearbeiding av personopplysninger samtidig som forskningsdeltakernes rettigheter og krav etter gjeldende lovverk blir ivaretatt på en god måte

2. Gjelder for

a. alle ansatte ved NTNU
b. alle studenter ved NTNU
c. alle som har tilgang til og/eller bearbeider og forvalter personopplysninger gjennom NTNUs IKT-infrastruktur

2.1. Anvendelsesområde

Retningslinjen gjelder for alle virksomhetsområder ved NTNU. Retningslinjen gjelder for personopplysninger som behandles elektronisk, helt eller delvis. Retningslinjen gjelder også ved manuell behandling av personopplysninger som inngår eller skal inngå i et register, dvs. som medfører at de er lett å finne igjen på enkeltpersoner.

Personopplysninger innebefatter også pseudonymiserte opplysninger, indirekte opplysninger og taushetsbelagte opplysninger. Anonyme opplysninger regnes ikke som personopplysninger.

3. Sentrale begreper og definisjoner

Personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson, enten direkte eller indirekte, f.eks. navn, identifikasjonsnummer, personbilde, on-line-identifikator, IP-adresse, ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet. Indirekte personidentifiserende opplysninger er bakgrunnsopplysninger som kan gjøre det mulig å spore opplysningene tilbake til en enkeltperson, for eksempel bostedskommune eller institusjonstilknytning kombinert med opplysninger om alder, kjønn, yrke, nasjonalitet, etc.

Helseopplysning: personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om mottatte helsetjenester, som gir informasjon om vedkommendes helsetilstand.

Særlige kategorier personopplysninger: opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Pseudonymisering: behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt person uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person. Opplysningene vil fortsatt regnes som personopplysninger etter loven.

Indirekte personopplysninger er bakgrunnsopplysninger som kan gjøre det mulig å spore opplysningene tilbake til en enkeltperson, for eksempel bostedskommune eller institusjonstilknytning kombinert med opplysninger om alder, kjønn, yrke, nasjonalitet, etc.

Taushetsbelagte opplysninger er opplysninger om noens personlige forhold (for eksempel familie, sykdom, helse, personlige økonomiske forhold). Særlige kategorier personopplysninger er en egen kategori i EUs personvernforordning som krever ekstra sikkerhetstiltak (for eksempel opplysninger om helse, seksuelle forhold, etnisk opprinnelse, politisk oppfatning). Både taushetsbelagte og særlige kategorier personopplysninger klassifiseres som fortrolige eller strengt fortrolige etter NTNUs Retningslinje for klassifisering av informasjon.

Anonyme opplysninger: opplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson. Først når man er sikker på at

opplysningene ikke kan knyttes til en gruppe på under 5 personer, anses opplysningene som anonymiserte. Anonymiserte opplysninger er ikke personopplysninger og reguleres ikke av personvernlovgivningen.

Behandling av personopplysning: enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Register: enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier, enten samlingen er plassert sentralt, er desentralisert eller spredt på et funksjonelt eller geografisk grunnlag.

Behandlingsansvarlig: en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. NTNU er behandlingsansvarlig i de aller fleste tilfellene der det behandles personopplysninger ved NTNU. Dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formål og midler som skal brukes skal de være felles behandlingsansvarlige.

Behandlingsgrunnlag: der rettslige grunnlaget for behandling av personopplysninger. Behandling av personopplysninger må ha et rettslig grunnlag for å være lovlig. Behandlingsgrunnlagene fremgår personvernforordningen art 6 og art. 9 for særlige kategorier personopplysninger.

Databehandler: en *ekstern* fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige. Blackboard, som er leverandør av læringsstøttesystem til NTNU, er et eksempel på en databehandler.

Samtykke: enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende. Må kunne dokumenteres.

4. Krav til behandling av personopplysninger

4.1. Generelle prinsipper for personvern

Personvern handler om retten til privatliv og retten til å bestemme over egne personopplysninger. Den enkelte skal i størst mulig grad kunne bestemme over egne personopplysninger. Reglene for behandling av personopplysninger bygger på noen grunnleggende prinsipper. Prinsippene fremgår av artikkel 5 i EUs personvernforordning (GDPR). Øvrige bestemmelser i EUs personvernforordning bygger på disse. All behandling av personopplysninger skal skje i samsvar med disse prinsippene som er:

a. **Lovlig, rettferdig og åpenhet om behandlingen -** Det må finnes en lov (behandlingsgrunnlag) som tillater behandlingen av personopplysninger. Minst ett av de grunnlagene som fremgår i EUs personvernforordning, må være oppfylt. Behandlingen av personopplysninger skal gjøres i respekt for de registrertes interesser og skape tillit. Behandlingen av personopplysninger skal være forståelig og forutsigbar for den registrerte slik at vedkommende kan innrette seg og gis mulighet til å gjøre sine

rettigheter gjeldende. Åpenhet om behandlingen er en forutsetning for at enkeltpersoner skal kunne ivareta sine rettigheter og interesser.

b. **Formålsbegrensning -** Personopplysninger skal bare behandles for spesifikke, uttrykkelige, angitte og legitime formål. Personopplysninger kan ikke gjenbrukes til formål som er uforenlig med det opprinnelige formålet. Viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål anses som forenlig med de opprinnelige formålene. Dette forutsetter at det er innført tekniske og organisatoriske tiltak for å sikre den registrertes rettigheter, særlig for å sikre at prinsippet om *dataminimering* overholdes. Aktuelle tiltak kan omfatte pseudonymisering. Dersom tiltakene kan oppfylles ved viderebehandling som ikke gjør det mulig å identifisere de registrerte, skal formålene oppfylles på denne måten (anonymisering av personopplysningene). Viderebehandling forutsetter at EUs personvernforordning og loven har vært fulgt ved den opprinnelige innsamlingen av personopplysningene.
c. **Dataminimering -** Mengden innsamlede personopplysninger skal begrenses til det som er nødvendig for formålet med innsamlingen.
d. **Riktighet -** Personopplysninger som behandles, skal være korrekte, og skal om nødvendig oppdateres.
e. **Lagringsbegrensning -** Personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for med mindre personopplysningene er arkivpliktige (dvs. inngår i dokumenter som er gjenstand for saksbehandling og har verdi som dokumentasjon). Offentlige virksomheter er underlagt arkivplikt hvilket medfører at NTNU i stor grad er pliktig til å arkivere opplysninger om ansatte og studenter.
f. **Integritet og konfidensialitet -** Dette betyr at den behandlingsansvarlige (NTNU eller den som handler på vegne av NTNU) må sørge for tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger. Dette skal gå foran tilgjengelighet.
g. **Ansvarlighet -** NTNU skal opptre i samsvar med disse prinsippene og sørge for at de registrertes rettigheter blir ivaretatt. NTNU skal kunne dokumentere at virksomheten har gjennomført nødvendige organisatoriske og tekniske tiltak for å etterleve EUs personvernforordning.

4.2. Oversikt over behandling av personopplysninger (protokoll)

a. Oversikten skal inneholde informasjon som fremgår i EUs personvernforordning artikkel 30[1].
b. Oversikten skal føres i NTNUs felles system for oversikt over behandling av personopplysninger.
c. Meldingsarkivet til Sikt personverntjenester for forskning, som utpekte ansatte ved NTNU har tilgang til, gir en oversikt over behandling av personopplysninger i student- og forskningsprosjekter som er meldt til Sikt.
d. Helseforskningsprosjekter der Fakultet for medisin og helse er forskningsansvarlig, skal føres i NTNUs oversikt over helseforskningsprosjekter (sharepointløsning).
e. Helseforskningsprosjekter der andre fakultet er forskningsansvarlig, skal meldes til Sikt og vil bli registrert i Sikts meldingsarkiv.

[1] https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_30#gdpr/ARTIKKEL_30

4.3. Behandlingsgrunnlag

4.3.1. Generelt

Behandling av personopplysninger krever et behandlingsgrunnlag (lovlig grunn), dvs. at det er en lov (f.eks. EUs personvernforordning, personopplysningsloven, universitets- og høyskoleloven) eller forskrift som tillater den aktuelle behandlingen.

For å behandle personopplysninger må ett av grunnlagene i EUs personvernforordning (GDPR) artikkel 6 nr.1 være oppfylt. Grunnlaget kan være samtykke eller ett av de andre alternativene. Minst ett av følgende vilkår må være oppfylt:

a. den registrerte har gitt *samtykke* (som må være dokumentert) til behandling av sine personopplysninger for ett eller flere spesifikke formål
b. behandlingen er *nødvendig* for å
    i. oppfylle en avtale med den registrerte
    ii. verne den registrertes eller en annen fysisk persons vitale interesser (liv og helse)
    iii. oppfylle en rettslig forpliktelse som den behandlingsansvarlige er pålagt
    iv. utføre en oppgave i allmennhetens interesse
    v. utøve offentlig myndighet som den behandlingsansvarlige er pålagt

For de tre siste alternativene kreves i tillegg et *supplerende grunnlag* i nasjonal lov. Bestemmelser i personopplysningsloven eller universitets- og høyskoleloven eller andre lover kan være et slikt supplerende lovgrunnlag.

Hvis det skal behandles særlige kategorier personopplysninger (helseopplysninger, opplysninger om etnisitet, politisk oppfatning mm.), kreves i tillegg at ett av punktene i EUs personvernforordning artikkel 9 nr. 2 er oppfylt.

EUs personvernforordning artikkel 6 nr. 1 bokstav f tillater behandling av personopplysninger hvis virksomheten som behandler personopplysningene, har en berettiget interesse i den aktuelle behandlingen og hensynet til den registrertes personvern ikke overstiger denne interessen. Bestemmelsen vil som regel ikke kunne brukes som grunnlag for behandling av personopplysninger om studenter da den ikke gjelder for behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver. Bestemmelsen kan være et grunnlag for behandling av personopplysninger om ansatte.

4.3.2. Personopplysninger om søkere, studenter og doktorgradsstudenter

Universitets- og høyskoleloven § 4-15 vil gi adgang til å behandle personopplysninger om søkere, studenter og doktorgradskandidater (heretter studenter) i studieadministrative systemer i følgende tilfeller:

a. Formålet må være å ivareta den registrertes rettigheter, eller å oppfylle institusjonens oppgaver og plikter etter UH-loven.
b. Navn, fødselsnummer, D-nummer (midlertidig identitetsnummer[2]) og karakterer fra videregående opplæring og universiteter og høyskoler *som er hentet fra* offentlige myndigheter, offentlige systemer for vitnemål, statlige, fylkeskommunale og private utdanningsinstitusjoner kan behandles når dette er nødvendig for å oppfylle formålet.

[2] https://www.skatteetaten.no/person/utenlandsk/norsk-identitetsnummer/d-nummer/

c. Opplysninger om helse, sosiale forhold og andre sensitive opplysninger som studenten selv har gitt institusjonen eller har samtykket til, når opplysningene er nødvendige for formålet nevnt i punket over.

Dersom personopplysninger skal behandles i andre sammenhenger, må studenten samtykke eller det må finnes et annet behandlingsgrunnlag.

4.3.3. Personopplysninger om ansatte

Det rettslige grunnlaget for behandling av grunnopplysninger om ansatte er EUs personvernforordning artikkel 6 nr. 1 b, dvs. at behandlingen er nødvendig for å oppfylle en avtale med den registrerte. For særlige kategorier personopplysninger må et av vilkårene i artikkel 9 nr. 2 i tillegg være oppfylt. Personopplysningsloven § 6 gir et supplerende grunnlag for behandling av særlige kategorier personopplysninger når dette er nødvendig for å gjennomføre arbeidsrettslige plikter eller rettigheter.

Bestemmelser om innsyn i arbeidstakers e-postkasse og kameraovervåking på arbeidsplassen er fastsatt av departementet som forskrifter til arbeidsmiljøloven, med hjemmel i aml. §§ 9-5 og 9-6.

4.3.4. Samtykke som behandlingsgrunnlag

Samtykke fra den registrerte kan være et behandlingsgrunnlag for behandling av personopplysninger. Dette forutsetter at følgene vilkår er oppfylt:

a. **Frivillig -** Det må ikke knytte seg noen fordeler eller negative sanksjoner til samtykket. Det må tas hensyn til ulikevekten mellom partene dersom universitetet vurderer å bygge behandlingen på samtykke fra studenter og ansatte. Dette kan medføre at samtykket i realiteten ikke anses som fritt.
b. **Spesifikt -** Det må fremgå hvilke(t) formål samtykket gjelder for.
c. **Informert -** Det må være klart hva som er omfattet av samtykket når den registrerte samtykker.
d. **Utvetydig -** Det må være klart at vedkommende har gitt samtykke, hvilken dato det ble gitt og navnet på den som ga samtykket. Behandlingsansvarlig må kunne påvise dette, dvs. at det må kunne dokumenteres, enten skriftlig eller elektronisk.

Den registrerte må, til enhver tid, kunne trekke tilbake samtykke og det må være like enkelt å trekke det tilbake som å gi det.

4.4. Risikovurdering

Risikovurderingen skal bidra til å forebygge uønskede hendelser eller mangler ved behandlingen av personopplysninger ved NTNU, som kan ha konsekvenser for studenter, ansatte, forskningsdeltakere og/eller samfunnet mer generelt. Sentrale forhold i risikovurderingen er prosjektets/behandlingens omfang, opplysningenes følsomhet, trusselbildet knyttet til miljøet opplysningene bearbeides og lagres i, og prosjektets/behandlingens varighet. Alle vurderinger og tiltak skal være dokumentert.

NTNUs *Retningslinje for risikostyring for informasjonssikkerhet* gir anvisning på hvordan man kan foreta en risikovurdering. I tillegg finnes det støttemateriell på innsida for risikovurdering av informasjonssikkerhet og risikovurdering av forskningsprosjekt som inneholder personopplysninger.

4.5. Vurdering av personvernkonsekvenser og forhåndsdrøfting med Datatilsynet

4.5.1. Generelt om personvernkonsekvensvurderinger (DPIA)

Hvis det er sannsynlig at en type behandling vil medføre høy risiko for enkeltpersoners rettigheter og friheter, skal den behandlingsansvarlige foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personvernet, jf. EUs personvernforordning artikkel 35.

Dette vil som eksempel være aktuelt ved bruk av ny teknologi, ved automatiserte behandlinger som vil ha rettslige virkninger for enkeltpersoner, behandling i stor skala av særlige kategorier personopplysninger, systematisk overvåkning i stor skala av et offentlig område. Datatilsynet har utarbeidet en veileder for vurdering av personvernkonsekvenser. Veilederen gir en oversikt over når det må gjennomføres en vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA). DPIA gjennomføres i samråd med personvernombud. NTNUs mal skal brukes og vurdering skal dokumenteres i NTNUs saks- og arkivsystem.

En vurdering som konkluderer med at det ikke er nødvendig å utføre en DPIA skal også dokumenteres, enten i NTNUs felles system for oversikt over behandling av personopplysninger eller i saks- og arkivsystemet.

Se Datatilsynets veileder og sjekkliste for vurdering av personvernkonsekvenser (DPIA) og NTNUs nettside Vurdere personkonsekvenser.

4.5.2. Rådføringsplikt med Datatilsynet ved fortsatt høy risiko

NTNU er pliktig til å rådføre seg med Datatilsynet dersom konklusjonen er at behandlingen fortsatt, etter at det er satt inn tekniske og/eller organisatoriske tiltak, vil medføre *høy risiko*, det ikke treffes tiltak for å redusere risikoen og det fortsatt er ønskelig å igangsette den planlagte behandlingen. Rektor avgjør om NTNU skal be om en forhåndsdrøfting med Datatilsynet. En eventuell henvendelse skal gå fra rektor.

4.6. Databehandleravtale

Hvis eksterne (en virksomhet eller fysisk person) skal behandle personopplysninger på vegne av NTNU skal det inngås databehandleravtale. Det kan bare inngås avtale med databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysningene oppfyller kravene etter EUs personvernforordning og vern av de registrertes rettigheter.

Avtalen skal oppfylle de kravene som fremgår av EUs personvernforordning artikkel 28. NTNU har i samarbeid med UH-sektoren utarbeidet en standard databehandleravtale som skal brukes. Hvis NTNUs mal for databehandleravtale ikke kan brukes, skal forelagt avtale vurderes av jurist ved NTNU før den blir inngått.

NTNUs rutine for inngåelse av databehandleravtale skal følges, se NTNUs nettside[3] og skal bli gjennomgått hvert annet år, samt revidert hvis det er behov for det.

Databehandleren skal ikke engasjere en annen databehandler (underleverandør) uten at det er skriftlig godkjent av NTNU som behandlingsansvarlig. NTNU er ansvarlig for databehandleres og eventuelle

[3] https://i.ntnu.no/wiki/-/wiki/Norsk/Databehandleravtale

underleverandørers behandling av personopplysningene og har ansvar for å vurdere og kontrollere om de er kompetent til å behandle de aktuelle personopplysningene i tråd med EUs personvernforordning.

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet. Databehandler skal dokumentere sikkerhetsrevisjonene. NTNU skal gis tilgang til revisjonsrapportene.

Når NTNU sammen med andre behandlingsansvarlige i fellesskap fastsetter formål med og midler for behandlingen av personopplysningene, foreligger et delt behandlingsansvar. I slike tilfeller må det inngås en avtale som angir partenes ansvar. NTNUs mal kan benyttes[4].

4.7. Overføring av personopplysninger til utlandet

Personopplysninger skal bare overføres til land eller internasjonale organisasjoner utenfor EU/EØS dersom kravene etter EUs personvernforordning kap. V (artikkel 44 flg.) er oppfylt. Merk at *overføring* også omfatter det å gi tilgang til personopplysninger.

Det må gjøres en risikovurdering av overføringen, for å sikre at informasjonssikkerheten er tilfredsstillende. Risikovurderingen må kunne dokumenteres.

a. Overføring til land utenfor EU/EØS kan skje dersom EU-kommisjonen har godkjent at landet har en forsvarlig behandling av personopplysninger[5]
b. Overføring utover dette krever at EUs standardkontrakt for overføring til behandlingsansvarlig eller databehandler i tredjeland brukes, eller at overføringen er tillatt etter øvrige punkter i EUs personvernforordning kap. V. EUs standardkontrakter er tilgjengelig på Datatilsynets nettsider.
c. Overføring med hjemmel i EUs personvernforordning artikkel 49 gir unntak for *særlige tilfeller*. Dette gjelder f.eks. dersom den registrerte uttrykkelig har samtykket til aktuell overføring eller overføringen er nødvendig for å oppfylle en avtale inngått i den registrertes interesse mellom den behandlingsansvarlige og en annen fysisk eller juridisk person. Eksempel på dette er medlemmer hjemmehørende utenfor EU/EØS i sakkyndige komiteer

Avtale om overføring av personopplysninger til utlandet skal forelegges IT-avdelingen og vurderes av jurist før avtalen blir inngått.

4.8. De registrertes rettigheter

Med registrert menes enkeltpersoner, søkere, studenter, ansatte, forskningsdeltakere og andre som NTNU behandler personopplysninger om. Den det er registrert personopplysninger om, har en rekke rettigheter knyttet til å få informasjon når det samles inn opplysninger om vedkommende, innsyn i egne personopplysninger som blir behandlet i virksomheten, krav på retting, sletting, begrensning av behandling, innsigelse og rett til dataportabilitet (EUs personvernforordning artikkel 12 – 23).

Det er flere unntak fra retten, både i EUs personvernforordning og personopplysningsloven §§ 16 og 17. Som eksempel kan nevnes opplysninger som er taushetsbelagt (der innsyn vil røpe opplysninger om andre personer eller sikkerhetstiltak). Det er også enkelte unntak knyttet til arkiv-, forsknings- eller statistiske

[4] Overføring av personopplysninger – avtalemaler
[5] Rules for the protection of personal data inside and outside the EU

formål. NTNU er som offentlig institusjon underlagt arkivloven hvilket innebærer at personopplysninger om ansatte og studenter i stor grad er arkivpliktig og ikke kan kreves slettet.

Registrerte som ønsker innsyn mm., skal henvende seg i samsvar med NTNUs fremgangsmåte og identifisere seg før innsyn mm. kan gis. Behandling av innsynskrav skal skje i samsvar med NTNUs rutine. Avdeling for dokumentasjonsforvaltning skal være mottaker av innsynskrav i henhold til NTNUs rutine.

4.9. Bilde, video-, og lydopptak

Den som skal publisere et bilde offentlig (f.eks. på internett, intranettet, i læringsstøttesystem, i trykt versjon) av en enkeltperson eller en mindre gruppe av personer, må innhente samtykke fra den som er avbildet. Samtykket må være skriftlig eller kunne dokumenteres på annen måte, f.eks. elektronisk.

Det følger av åndsverkloven av 15. juni 2018 § 104 at fotografi som avbilder en person, ikke kan gjengis eller vises offentlig uten samtykke fra den avbildede. Unntak gjelder hvis

a. avbildningen har aktuell og allmenn interesse
b. avbildningen av personen er mindre viktig enn hovedinnholdet i bildet
c. bildet gjengir forsamlinger, folketog i friluft eller forhold eller hendelser som har allmenn interesse.

Video-, og/eller lydopptak av personer som kan gjenkjennes, krever samtykke fra den enkelte. Det samme gjelder publisering f.eks. på internett, intranettet og i læringsstøttesystem.

Samtykkeskjema og veiledning/rutine skal være tilgjengelig på NTNUs nettsider[6].

4.10. Kameraovervåkning

Det skal, ved skilting, gjøres tydelig at stedet blir overvåket, om det inkluderer lydopptak og hvem som er behandlingsansvarlig (NTNU ved Eiendomsavdeling). Behov for kameraovervåking blir vurdert jevnlig.

Opptak skal slettes *én* uke etter at opptakene er gjort. Hvis det er sannsynlig at opptaket vil bli utlevert til politiet i forbindelse med etterforskning av straffbare handlinger eller ulykker, kan opptakene oppbevares i inntil 30 dager.

Utlevering av opptak kan kun skje i følgende tilfeller:

a. den som er avbildet, samtykker
b. utleveringen skjer til politiet ved etterforskning av straffbare handlinger eller ulykker, og lovbestemt taushetsplikt ikke er til hinder for utleveringen
c. det ellers følger av lov at utleveringen kan skje

4.11. Adgangskontroll

Personopplysninger fra NTNU overføres daglig fra felles database til NTNU Vakt og service. Persondata som overføres, er den enkeltes navn, fødselsnummer/studentnummer, e-postadresse, arbeidssted og dato for oppstart. Opplysningene skal kun benyttes til produksjon av adgangskort. Det er kun dedikerte medarbeidere i Vakt og service som skal ha tilgang til opplysningene.

[6] https://i.ntnu.no/wiki/-/wiki/Norsk/Samtykke+ved+foto+-+video+-+lyd

4.12. Generell behandling av personopplysninger

NTNUs saks- og arkivsystem støtter digital saksflyt og signering samt digital utsendelse (sikker digital post).

Taushetsbelagte eller særlige kategorier personopplysninger skal behandles i NTNUs saks- og arkivsystem eller i annet godkjent fagsystem. Dette er opplysninger som betegnes som fortrolige eller strengt fortrolige i NTNUs klassifiseringssystem.

Papirdokumenter som inneholder taushetsbelagte, sensitive eller andre personopplysninger som etter sitt innhold er unntatt offentlighet, skal oppbevares i låsbare skap på kontorer/arealer som er låst utenom ordinær arbeidstid.

Dokumenter som inneholder taushetsbelagte eller særlige kategorier personopplysninger som sendes elektronisk til medlemmer i styrer og utvalg, skal være atskilt fra øvrige saker slik at medlemmene kan slette disse opplysningene når saken er behandlet. Det er kun adgang til å benytte elektronisk forsendelse dersom den digitale løsningen er klassifisert for overføring av taushetsbelagte eller særlige kategorier personopplysninger.

NTNU har utarbeidet en oversikt over lagring av filer og dokumenter og hvilke systemer/verktøy som kan brukes til hva. Denne skal være tilgjengelig på NTNUs nettsider.

4.13. Taushetsplikt

Alle som rutinemessig arbeider med taushetsbelagte personopplysninger, skal ha kjennskap til personvernregelverket og underskrive taushetserklæring.

Ansatte samt konsulenter og leverandører som gjennom vedlikehold og drift av NTNUs IKT-struktur og systemer får tilgang til taushetsbelagte personopplysninger, skal kjenne til regelverket om behandling av personopplysninger og underskrive taushetserklæring. Krav til, og opplysninger om taushetsplikten for medlemmer i utvalg, styrer og råd skal innarbeides i oppnevningsbrevet til medlemmene.

4.14. 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. Dette følger av prinsippet om lagringsbegrensning og dataminimering.

Hver enkelt medarbeider er ansvarlig for å slette personopplysninger som er lagret på vedkommendes personlige brukerområde.

a. Personopplysninger som ikke skal oppbevares med hjemmel i arkivloven eller annen lovgivning, skal slettes.
b. Personopplysninger skal slettes eller ryddes opp i fortløpende – og senest innen seks måneder – etter at en ansatt slutter eller en student er uteksaminert/sluttet.
c. Personopplysninger, som det midlertidig er nødvendig å lagre på personlig område i forbindelse med utføring av en arbeidsoppgave, skal slettes når formålet ikke lenger er tilstede.
d. Medlemmer i nemnder og utvalg som får tilsendt saksdokumenter elektronisk som inneholder taushetsbelagte eller særlige kategorier personopplysninger, skal slette tilsendt materiale når saken er behandlet.

e. Arkivpliktige dokumenter, dvs. dokumenter som er gjenstand for saksbehandling og har verdi som dokumentasjon, skal arkiveres i institusjonens arkivsystem.

4.15. Bruk av fødselsnummer

a. Fødselsnummer og andre entydige identifikasjonsmidler kan bare behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering, jf. personopplysningsloven § 12.
b. Fødselsnummer kan sendes i sikker digital post. Fødselsnummer skal ikke være tilgjengelig for andre enn mottakeren. Dersom fødselsnummer sendes pr. post skal det ikke være synlig i konvoluttvindu eller være skrevet på utsiden av konvolutten.
c. Hvis fødselsnummer skal sendes pr. e-post, skal e-posten krypteres[7].

4.16. Bruk av e-post

I samsvar med Datatilsynets føringer skal følgende ikke sendes på e-post:

a. taushetsbelagte eller særlige kategorier personopplysninger
b. fødselsnummer og andre entydige identifikasjonsnummer
c. personopplysninger om mange, f.eks. regneark, lister

Disse punktene gjelder både e-post som sendes internt ved NTNU og eksternt.

Dersom e-post og/eller vedlagte filer krypteres, kan e-post unntaksvis brukes[8]. Risikoen må vurderes, passord må sendes separat (SMS eller muntlig) og må være i samsvar med NTNUs krav til passord, jf. «Retningslinje for Kryptografiske kontrollere».

4.17. Utlevere informasjon om studenter og ansatte til eksterne

Informasjon som er innsamlet og lagret for generell personalforvaltning og om studenter for administrative formål, skal normalt ikke utleveres til utenforstående med mindre de som ber om opplysningene har rett til innsyn etter offentleglova. Utlevering av personopplysninger fra NTNUs systemer til andre formål enn det de er samlet inn for, skal godkjennes av systemeier. Systemeier er ansvarlig for at utleveringen blir dokumentert slik at informasjonsplikten ved krav om innsyn fra den registrerte kan ivaretas.

Hvis det gjelder opplysninger, som det ikke er innsynsrett i etter offentleglova, må den instansen (f.eks. NAV, Vernepliktsverket) som ber om opplysningene, vise til en lovhjemmel som gir rett til å få opplysningene utlevert. Denne type henvendelser skal behandles av systemeier. **Systemeier** har ansvar for å undersøke om det foreligger nødvendig lovhjemmel for utleveringen og om nødvendig etterlyse dette.

Taushetsbelagte opplysninger kan utleveres dersom vilkårene etter forvaltningsloven § 13 b er oppfylt, f.eks. til en advokat som representerer en student eller ansatt i en sak ved NTNU.

[7] https://i.ntnu.no/wiki/-/wiki/Norsk/Sikker+e-post
[8] https://i.ntnu.no/wiki/-/wiki/Norsk/Sikker+e-post

Hvis innsyn gis, skal det opplyses om at den som får innsyn må ha et eget behandlingsgrunnlag for eventuell elektronisk viderebehandling av opplysningene.

4.18. Forholdet til innsyn etter andre lover

Spørsmål om innsyn i det offentliges dokumenter reguleres av lov av 19. mai 2006 om rett til innsyn i offentleg verksemd (offentleglova). Partsinnsyn reguleres av lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven)[9].

Etter EUs personvernforordning artikkel 86 kan den enkelte stat fastsette regler om innsyn i offentlige dokumenter. Bestemmelsene om innsyn for enhver etter offentleglova og partsinnsyn etter forvaltningsloven går derfor foran bestemmelsene i EUs personvernforordning og personopplysningsloven. Dette innebærer at det ved spørsmål om innsyn i dokumenter ved NTNU kan gis innsyn i dokumenter som inneholder personopplysninger dersom offentleglova hjemler dette. Det vil da være dokumentbegrepet i offentleglova som blir avgjørende for hvilke dokumenter det kan gis innsyn i. Tilsvarende gjelder for partsinnsyn etter forvaltningsloven. Saksbehandler, eventuelt i samråd med sin leder, avgjør spørsmål om innsyn.

4.19. Innebygd personvern (Privacy by Design)

Innebygd personvern og personvern som standard innstilling betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Dette er en forpliktelse som virksomheten har etter EUs personvernforordning artikkel 25[10].

Formålet med innebygd personvern er at den behandlingsansvarlige før og under anskaffelse / utvikling av systemer og tjenester vurderer personvernspørsmål. Kravet til innebygd personvern og personvern som standardinnstilling gjelder uavhengig av risiko.

5. Kontroll og etterlevelse

Institutter skal årlig, ved hjelp av en mal for egenkontroll, rapportere til fakultetet angående behandling av personopplysninger. Det samme gjelder seksjoner ved avdelinger i fellesadministrasjonen. Fakultet / avdeling skal sammenfatte den innsamlede informasjonen ved hjelp av malen. Instituttene skal også rapportere om kontroll av forskningsprosjekter. En sammenfatning av dette skal også inngå i fakultetets rapport.

Dekan/avdelingsleder skal sørge for at det blir utarbeidet en rapport som skal sendes til Avdeling for virksomhetsstyring. Rapporten oversendes Direktør for organisasjon og infrastruktur for rektors gjennomgang. Rapportene skal blant annet danne grunnlag for rektors årlige orientering til NTNUs styre om arbeidet med informasjonssikkerhet, herunder behandling av personopplysninger.

6. Særlig om behandling av personopplysninger i forskning

Ifølge fortalen punkt 159 (forarbeidene) til EUs personvernforordning bør behandling av personopplysninger i forbindelse med formål knyttet til vitenskapelig forskning *tolkes vidt* og f.eks.

[9] https://i.ntnu.no/wiki/-/wiki/Norsk/Innsyn+i+offentlige+dokument
[10] Retningslinje for Operativ sikkerhet

omfatte teknologisk utvikling og demonstrasjon, grunnleggende forskning, anvendt forskning og privatfinansiert forskning.

6.1. Melding til Sikt personverntjenester

Forsknings-, student-, og kvalitetssikringsprosjekter som behandler personopplysninger samt helseforskning hvor andre fakultet enn MH er forskningsansvarlig, skal meldes til Sikt personverntjenester[11]. Det samme gjelder prosjekter der personopplysninger behandles på papir hvis disse inngår eller skal inngå i et personregister.

Sikt har en rådgivende rolle. Sikt skal vurdere om prosjektet tilfredsstiller kravene i EUs personvernforordning. Behandlingen av personopplysninger kan ikke settes i gang før Sikt har gitt tilbakemelding til prosjektleder om at den planlagte behandlingen vurderes å være i samsvar med EUs personvernforordning, samt at nødvendige forutsetninger og anbefalte tiltak og vurderinger gjennomføres. Ved spørsmål til Sikts vurdering vil det bli en dialog mellom Sikt og NTNU for å avstemme nødvendige tiltak. Dersom Sikt og NTNU gjør ulike vurderinger om hva som er tilstrekkelig, tas endelig avgjørelse av Forskningsansvarlig i samråd med jurist i Virksomhetsstyring.

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

Prosjektet skal meldes senest 30 dager før datainnsamlingen skal starte. Sikt tilbyr også arkivering av prosjektdata ved prosjektslutt.

Etter EUs personvernforordning er det et krav at virksomheten skal føre oversikt (protokoll) over alle behandlinger av personopplysninger. Sikt skal på vegne av NTNU føre oversikt over alle forsknings-, student og kvalitetssikringsprosjekter som blir meldt til Sikt. Oversikten vil danne grunnlag for tilsyn og kontroll med forskningsprosjekter, jf. retningslinjens punkt Kontroll og etterlevelse - forskningsprosjekter.

6.2. Helseforskning – forhåndsgodkjenning av REK

Medisinsk og helsefaglig forskning (helseforskning) er forskning på mennesker, humant biologisk materiale eller helseopplysninger der formålet er å skaffe til veie ny kunnskap om helse og sykdom. Det samme gjelder forskning som omfatter pilotstudier og utprøvende behandling.

Helseforskning skal være forhåndsgodkjent av Regional komite for medisinsk og helsefaglig forskningsetikk (REK) før prosjektet kan starte, jf. helseforskningsloven §33. REK skal gjøre en forskningsetisk vurdering av prosjektet. REKs forhåndsgodkjenning vil ikke være et tilstrekkelig lovlig grunnlag for behandling av personopplysninger i helseforskning. Behandlingen av personopplysninger må også ha et lovlig grunnlag i EUs personvernforordning. Forskningsansvarlig vil være ansvarlig for å vurdere om behandlingen av personopplysninger i helseforskningsprosjekter vil være i samsvar med EUs personvernforordning.

Denne retningslinjen gir de overordnede retningslinjene også for helseforskning. NTNUs portal for medisinsk og helsefaglig forskning gir mer detaljerte forskningsadministrative rutiner og retningslinjer.

[11] https://Sikt.no/omrade/personverntjenester

Der andre fakultet enn Fakultet for medisin og helse (MH) er forskningsansvarlig i helseforskningsprosjekter, skal forskningsprosjektet i tillegg til søknad til REK også meldes til Sikt personverntjenester. Sikt skal vurdere om den planlagte behandlingen av personopplysninger i prosjektet er i samsvar med kravene etter EUs personvernforordning. Behandling av personopplysninger kan ikke starte før Sikt har gitt tilbakemelding om sin vurdering.

Generelt anbefales at prosjektopplysninger sendes inn/meldes inn til Sikt og REK så fort som mulig, dvs. parallelt. Sikt vil vurdere fra sak til sak om de vurderer ferdig prosjektet, eller om de vil avvente REK sin vurdering av prosjektet.

6.3. Vurdering av personvernkonsekvenser (DPIA)

Hvis det er sannsynlig at en type behandling vil medføre høy risiko for enkeltpersoners rettigheter og friheter, skal den behandlingsansvarlige foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personvernet, jf. EUs personvernforordning artikkel 35[12]. Dette gjelder også for forskning.

Sikt tar initiativ til - og bistår - i vurdering av personvernkonsekvenser personvernkonsekvenser (Data Protection Impact Assessment - DPIA) for de prosjektene som blir meldt til Sikt. Sikt skal utføre vurderingen av DPIA i samråd med personvernombudet.

Fakultet for medisin og helsevitenskap har utarbeidet en egen mal for vurdering av personvernkonsekvenser i helseforskningsprosjekter. Prosjektleder er ansvarlig for at det blir foretatt en vurdering av personvernkonsekvenser. Personvernombudet skal på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av denne.

6.4. Behandlingsgrunnlag

6.4.1. Generelt

Dersom personopplysninger skal behandles i forbindelse med forskning, kreves et behandlingsgrunnlag (samtykke fra deltakere eller en lov som tillater det). Etter forskningsetiske prinsipper er samtykke hovedregelen ved forskning på opplysninger som kan knyttes til enkeltindivider. Etter fortalen punkt 33 (forarbeidene) til EUs personvernforordning bør forskningsdeltakere kunne gi samtykke til visse områder innen vitenskapelig forskning når dette er i samsvar med anerkjente etiske standarder for vitenskapelig forskning. Forskningsdeltakerne bør ha mulighet til å gi sitt samtykke bare til visse forskningsområder eller deler av forskningsprosjektet i det omfang det tilsiktede formålet tillater det. Se nærmere om informasjon til forskningsdeltakere og samtykke hos Sikt[13].

Ved behandling av alminnelige personopplysninger vil behandlingsgrunnlag være:

a. Samtykke etter EUs personvernforordning artikkel 6 nr. 1 bokstav a, eller
b. Hvis ikke samtykke: at behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse og er nødvendig for formål knyttet til vitenskapelig forskning, jf. artikkel 6 nr. 1 bokstav e) og personopplysningsloven § 8 som supplerende grunnlag.

[12] https://i.ntnu.no/wiki/-/wiki/Norsk/Vurdere+personvernkonsekvenser
[13] https://sikt.no/samtykke-og-andre-behandlingsgrunnlag

c. Behandlingen må omfatte nødvendige tiltak for å sikre at den er i tråd med EUs personvernforordning og at forskningsdeltakeres personvern ivaretas.

Ved behandling av særlige kategorier personopplysninger vil behandlingsgrunnlag være:

d. Samtykke etter artikkel 9 nr. 2 bokstav a, eller
e. Hvis ikke samtykke: at behandlingen er nødvendig for vitenskapelig forskning forutsatt at samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene for den enkelte, jf. artikkel 9 bokstav j og personopplysningsloven § 9 som supplerende grunnlag.
f. Behandlingen må være omfattet av nødvendige garantier, f.eks. at personopplysningene pseudonymiseres slik at opplysningene ikke lenger blir direkte knyttet til den enkelte uten tilleggsopplysninger, at det er tilgangsstyring og logging.

Ved behandling av personopplysninger om straffedommer og lovovertredelser vil behandlingsgrunnlag være:

g. Samtykke etter artikkel 6 nr. 1 bokstav a, eller
h. Hvis ikke samtykke: da gjelder tilsvarende som for særlige kategorier personopplysninger, dvs. at samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene for den enkelte. I interesseavveiningen skal det legges vekt på at behandlingen skjer uten den registrertes samtykke. Vurderingen må dokumenteres. Behandlingsgrunnlag: artikkel 6 nr. 1 bokstav e og artikkel 10 med supplerende grunnlag i personopplysningsloven § 11.
i. Behandlingen må være omfattet av nødvendige garantier for å ivareta forskningsdeltakernes personvern, jf. punktet ovenfor om særlige kategorier personopplysninger.

6.4.2. Helseforskning

Vedtak om dispensasjon fra taushetsplikt vil utgjøre et supplerende lovgrunnlag. REKs forskningsetiske vurdering (forhåndsgodkjenning etter helseforskningsloven §§ 9 og 33) vil utgjøre et egnet og særlig tiltak for å verne den registrertes rettigheter og interesser. REK skal, som ledd i den forskningsetiske vurderingen, også vurdere behandlingen av personopplysninger.

6.4.3. Viderebehandling til forskningsformål

Viderebehandling av personopplysninger til forskningsformål av allerede innsamlede personopplysninger anses som forenlig med det opprinnelige formålet. Dette forutsetter at det er innført tekniske og organisatoriske tiltak for å sikre den registrertes rettigheter, særlig for å sikre at prinsippet om *dataminimering* overholdes. Aktuelle tiltak kan f.eks. være pseudonymisering.

Dersom forskningsformålet kan oppfylles ved anonymiserte opplysninger, skal viderebehandlingen skje på denne måten. Viderebehandling til forskningsformål forutsetter at de allerede innsamlede opplysningene er behandlet i samsvar med regelverket.

Dersom viderebehandlingen innebærer utlevering til en annen behandlingsansvarlig (dvs. andre enn NTNU), må den som mottar opplysningene, ha et eget behandlingsgrunnlag for behandlingen.

6.5. Datahåndteringsplan (DMP)

Alle forskningsprosjekter skal ha en datahåndteringsplan[14]. Datahåndteringsplanen skal beskrive hvordan forskningsdata skal samles inn, lagres og deles slik at dataene blir håndtert sikkert og forsvarlig.

Planen skal være et aktivt dokument som oppdateres underveis i prosjektet og som dokumenterer hvordan forskningsdata blir behandlet og organisert gjennom hele prosjektet. En datahåndteringsplan skal også inkludere vurderinger knyttet til etikk og personvern. Planen skal tilfredsstille krav fra finansieringskildene og være i tråd med NTNUs retningslinje for behandling av personopplysninger.

6.6. Lagring av aktive 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 f.eks. i forbindelse med finansiering av forskning.

6.7. Prosjektmedarbeideres tilgang til forskningsdata

Forskningsdataene skal bare være tilgjengelig for godkjente prosjektmedarbeidere fram til prosjektavslutning. Prosjektleder bestemmer hvilke prosjektmedarbeidere som skal ha tilgang til pseudonymiserte personopplysninger og koblingsnøkkel. Prosjektleder skal ha dokumenterbar oversikt over hvem som har tilgang til data. Oversikten skal være tilgjengelig for forskningsansvarlig.

Prosjektmedarbeidere skal normalt ikke ha tilgang til koblingsnøkkel. I de tilfeller de har tilgang til koblingsnøkkelen, er ikke lenger dataene å anse som pseudonymiserte, men som direkte personidentifiserbare, noe som skjerper kravene til forsvarlig behandling og oppbevaring.

6.8. Avslutning av forskningsprosjekter

Personopplysningene skal anonymiseres eller slettes hvis det ikke er krav om lagring etter godkjenninger som er gitt, eller i forbindelse med finansiering av forskningsprosjektet. Nødvendige bekreftelser skal sendes til REK og Sikt.

6.9. Kontroll og etterlevelse - forskningsprosjekter

Forskningsansvarlig skal gjennomføre systematiske tiltak for å påse at prosjektet gjennomføres i tråd med retningslinjene og at behandling av personopplysninger er i samsvar med lover, forskrifter og NTNUs egne retningslinjer.

Et utvalg på 10 % av forskningsprosjektene samlet sett skal kontrolleres årlig. Utvalget skal hentes fra forskjellige faser i gjennomføringen: oppstart, gjennomføring og avslutning.

6.9.1. Kontroll med oppstart

Forskningsprosjekter som er tildelt forskningsmidler og andre kjente prosjekter skal kontrolleres i forhold til meldingsoversikten hos Sikt. Dette for å kontrollere om rådføringsplikten er overholdt.

6.9.2. Kontroll med gjennomføring

Forskningsansvarlig kontrollerer om forskningsprosjektet har innhentet eventuelle nødvendige godkjenninger / tillatelser og om rådgivningsplikten med Sikt og personvernombud er overholdt.

[14] https://i.ntnu.no/wiki/-/wiki/Norsk/Datah%C3%A5ndteringsplan

Kontrollen skal avdekke om prosjektet gjennomføres i samsvar med de opplysninger som er gitt til REK / Sikt og de godkjenninger / råd som er gitt.

6.9.3. Kontroll med avslutning

Forskningsansvarlig skal kontrollere om rutinene knyttet til avslutning er fulgt og at forskningsdata som er oppbevart elektronisk eller i andre arkiv er slettet eller anonymisert.

I styringsdialogen med sin leder skal forskningsansvarlig rapportere om i hvilken grad lover, retningslinjer og rutiner etterleves og hvilke tiltak som er gjort.

7. Særlig om behandling av personopplysninger i forbindelse med undervisning

7.1. Video-, og lydopptak

Det er ikke nødvendig å innhente samtykke fra faglærer for å strømme/gjøre opptak av undervisning som er nødvendig for å oppfylle NTNUs plikt til å gi studenter undervisning og som krever NTNU-pålogging for å kunne følges. EUs personvernforordning artikkel 6 nr. 1 bokstav f gir behandlingsgrunnlag. NTNU kan ha en berettiget interesse i at undervisningen strømmes, f.eks. for at den skal være tilgjengelig for studenter på flere campus. Personvernulempen anses som lav når det kreves NTNU-pålogging for å kunne følge undervisningen.

Dersom opptaket skal legges ut åpent på internett, kreves alltid samtykke fra faglærer. NTNUs avtaleskjema om tilgjengeliggjøring på nett skal brukes.

Hvis det er studenter til stede, skal det være tydelig merket ved inngangen og i rommet at undervisningen blir tatt opp på video. .

Video- og / eller lydopptak av studenter slik at de kan gjenkjennes, krever samtykke fra studenten. Dette gjelder for eksempel hvis studenter skal presentere et prosjekt eller liknende. Samtykket skal tilfredsstille kravene til gyldig samtykke, se punktet «Samtykke som behandlingsgrunnlag», og skal kunne dokumenteres.

Studenter som ønsker å ta opptak (video-, og/eller lyd) av undervisning må ha samtykke fra faglærer hvis det ikke foreligger vedtak om tilrettelegging. Studenten kan kun bruke opptaket i forbindelse med egne studier. Studenten kan ikke bruke opptaket på annen måte eller publisere opptaket uten faglærers skriftlige samtykke (f.eks. på internett eller i andre sammenhenger).

Dersom videoopptak av studenter er en obligatorisk del av undervisningen for at læringsmålene skal nås, skal det fremgå av *studieplanen*. I slike tilfeller er det rettslige grunnlaget for opptak og bruk av opptaket EUs personvernforordning artikkel 6 nr. 1 bokstav e med supplerende grunnlag i universitets- og høyskoleloven § 4-15.

7.2. Bilde, video- og lydopptak – studenter i praksis

Hvis studenter i praksis skal ta bilde eller video-, og / eller lydopptak av personer, krever dette samtykke fra personen, jf punktet «Samtykke som behandlingsgrunnlag». Bilde, video-, eller lydopptak av mindreårige krever samtykke fra foreldre eller foresatte. Bilder fra praksis skal ikke legges ut på internett/sosiale medier.

7.3. Læringsplattformer

Det er NTNUs valgte læringsplattformer som har godkjent databehandleravtale som skal brukes til å koordinere og administrere emneinnhold og til kommunikasjon i undervisningen mm.

7.4. Studentprosjekt

Ved behandling av personopplysninger i forbindelse med bachelor-, master-/ hovedoppgave og doktorgrad skal reglene for behandling av personopplysninger i forskning følges, se kap. 5.

8. Erstatning og oppreisning ved personvernbrudd

Brudd på personvernreglene kan føre til overtredelsesgebyr fra Datatilsynet og at den berørte får krav på erstatning/oppreisning. Dersom NTNU ilegges gebyr, er den enheten hvor bruddet skjedde, ansvarlig for å dekke dette. Tilsvarende gjelder eventuelle erstatnings-/oppreisningsbeløp til berørte.

9. Roller og ansvar

Rektor har delegert til organisasjonsdirektøren å godkjenne, koordinere og iverksette nødvendige tiltak, herunder pålegge fakultetene og avdelingene i fellesadministrasjonen plikter for å sikre at behandlingen av personopplysninger skjer i henhold til NTNUs mål og overordnede retningslinjer og lovbestemte krav samt at informasjonssikkerheten fungerer tilfredsstillende.

Linjeleder, systemeier og prosesseier har sentrale roller i forbindelse med behandling av personopplysninger.

9.1. Styret

a. Har et overordnet ansvar for behandling av personopplysninger ved NTNU

9.2. Rektor

a. er NTNUs øverste behandlingsansvarlig for behandling av personopplysninger ved NTNU
b. skal årlig orientere styret om behandling av personopplysninger i virksomheten

9.3. Direktør for organisasjon og infrastruktur

a. er delegert oppgaven å godkjenne, koordinere og iverksette nødvendige tiltak for å sikre at behandlingen av personopplysninger skjer i samsvar med lovbestemte krav og NTNUs retningslinjer.
b. er ansvarlig for innsamling og rapportering til ledelsens årlige gjennomgang
c. skal påse at relevante parter blir varslet ved alvorlige brudd på personvernet
d. er ansvarlig for å iverksette nødvendige tiltak for å sikre en forsvarlig avviksbehandling

9.4. Avdelingsdirektører og seksjonssjefer i Fellesadministrasjonen

a. er ansvarlig for etterlevelsen av krav til behandling av personopplysninger ved enheten
b. er ansvarlig for å følge opp at lovverk og rutiner og godkjenninger følges, og at avvik lukkes
c. er ansvarlig for å holde en løpende og oppdatert oversikt over IKT-systemer som anvendes
d. er ansvarlig for at ansatte i enheten har tilstrekkelig opplæring i behandling av personopplysninger og kan ivareta sin plikt til å vurdere risiko ved nye prosjekt og behandlinger, samt melde avvik ved brudd på informasjonssikkerheten

e. er ansvarlig for at alle ansatte innen enheten har tilgang til tjenester og materiell slik at brukerne kan ivareta den registrertes personvern
f. er ansvarlig for en systematisk gjennomgang av databehandleravtaler og andre avtaler av betydning og gjennomgang av avvik ved enheten på minimum årlig basis
g. er ansvarlig for at internkontrollen fungerer ved enheten

9.5. Dekan/museumsdirektør

a. er ansvarlig for etterlevelsen av kravene til behandlingen av personopplysninger ved fakultetet / vitenskapsmuseet
b. er ansvarlig for at alle instituttledere er kjent med gjeldende rutiner og retningslinjer for behandling av personopplysninger
c. er ansvarlig for å fastsette nødvendige lokale rutiner ved behov
d. er ansvarlig for å følge opp at lovverk og rutiner og godkjenninger følges, og at avvik lukkes
e. er ansvarlig for å holde en løpende og oppdatert oversikt over IKT-systemer som anvendes
f. er forskningsansvarlig / behandlingsansvarlig ved eget fakultet og skal ha oversikt over forskningsporteføljen ved fakultetet
g. er ansvarlig for at ansatte i enheten har tilstrekkelig opplæring i behandling av personopplysninger og kan ivareta sin plikt til å vurdere risiko ved nye prosjekt og behandlinger, samt melde avvik ved personvernbrudd
h. er ansvarlig for at studentene ved NTNU har nødvendig opplæring i behandling av personopplysninger
i. er ansvarlig for at alle ansatte innen enheten har tilgang til tjenester og materiell slik at brukerne kan ivareta de registrertes personvern
j. er ansvarlig for å gjennomføre dialog med respektive underliggende enheter, herunder om oppfølgingen av rutiner og avvik, på minimum årlig basis
k. er ansvarlig for at internkontrollen ved behandling av personopplysninger fungerer ved fakultetet/Vitenskapsmuseet

9.6. Instituttleder

a. er ansvarlig for etterlevelsen av kravene til behandling av personopplysninger ved instituttet
b. er ansvarlig for at ansatte er kjent med relevante lover og regler, samt rutiner for behandling av personopplysninger og forskningsetiske retningslinjer
c. er ansvarlig for at ansatte istandsettes til å ivareta sine plikter til å vurdere risiko ved nye prosjekt og behandlinger, samt melder avvik ved personvernbrudd
d. er ansvarlig for at internkontrollen for behandling av personopplysninger fungerer ved instituttet

9.7. Leder av IT-avdelingen

a. er ansvarlig for å holde en løpende og oppdatert oversikt over NTNUs IKT-infrastruktur, og at informasjonssikkerheten i og mellom systemene ivaretas
b. er ansvarlig for at alle ansatte og studenter ved NTNU har tilgang til tjenester og materiell slik at brukerne kan ivareta de registrertes personvern

9.8. Leder av Seksjon for digital sikkerhet

a. er ansvarlig for gjennomføring av sikkerhetskrav til NTNUs IKT-infrastruktur og mottak av avviksmeldinger

9.9. Systemeier

Leder som er ansvarlig for å utvikle, forvalte og/eller drifte et informasjonssystem på vegne av NTNU. En som oppbevarer data kan også anses som systemeier.

a. er ansvarlig for at IT-systemets utvikling, forvaltning og/eller drift møter kravene til informasjonssikkerhet, herunder behandling av personopplysninger
b. har ansvar for å føre oversikt over behandling av personopplysninger (protokoll) for system som vedkommende er systemeier for og har også ansvar for at oversikten blir oppdatert og vedlikeholdt
c. er pliktig til å sørge for at det gjennomføres en risikovurdering før behandlingen av personopplysninger kan starte
d. skal sørge for at det blir utført en DPIA der det er krav om dette, i samråd med personvernombud
e. har ansvar for å inngå skriftlig databehandleravtale hvis eksterne (en virksomhet eller fysisk person) skal behandle personopplysninger på vegne av NTNU
f. er ansvarlig for at databehandleravtale blir gjennomgått hvert andre år og revidert hvis det er behov for det, samt innhente dokumentasjon fra databehandlers sikkerhetsrevisjon
g. er ansvarlig for at personopplysninger som skal overføres til land eller internasjonale organisasjoner utenfor EU/EØS, bare overføres dersom kravene etter EUs personvernforordning kap. V (artikkel 44 flg.) er oppfylt
h. skal sørge for at den det samles inn opplysninger om, blir informert og at henvendelser fra den registrerte blir fulgt opp i samsvar med kravene etter EUs personvernforordning
i. skal oppnevne en systemkontakt som kan bistå med innsynskrav når den registrerte krever kopi av personopplysninger fra et gitt system
j. har ansvar for å utarbeide rutiner for å minimalisere sikkerhetsrisikoen ved behandling av personopplysninger i systemer den er systemeier for, dette innebærer også rutiner for sletting
k. skal sørge for fortløpende sletting / opprydding av unødvendige personopplysninger – innen 6 måneder – etter at en ansatt slutter eller en student er uteksaminert eller har sluttet
l. skal godkjenne utlevering av personopplysninger fra NTNUs systemer til andre formål enn det de er samlet inn for
m. er ansvarlig for at utleveringen blir dokumentert slik at informasjonsplikten ved krav om innsyn fra den registrerte kan ivaretas
n. har ansvar for å undersøke om det foreligger nødvendig lovhjemmel for utleveringen av personopplysninger for sitt system og om nødvendig etterlyse dette
o. er ansvarlig for at behandlingen i forbindelse med video- og lydopptak i undervisning (bruk, lagring og sletting mm.) skjer i samsvar med personvernregelverket og i tråd med NTNUs prosesser, rutiner og valgte løsninger
p. skal sørge for at innebygd personvern blir implementert i samsvar med EUs personvernforordning artikkel 25 ved utvikling og anskaffelse. Personvernombudet skal involveres[15]

9.10. Linjeleder

Leder med personalansvar (prorektorer, direktører, avdelingsledere, dekan, museumsdirektør, instituttledere, seksjonsledere).

[15] Retningslinje for operativ sikkerhet

a. skal sørge for at det blir ført oversikt (protokoll) over behandling av personopplysninger som utføres i sin enhet og har også ansvar for at oversikten blir oppdatert og vedlikeholdt
b. er pliktig til å sørge for at det gjennomføres en risikovurdering før behandlingen av personopplysninger kan starte
c. skal sørge for at det blir utført en DPIA der det er krav om dette, i samråd med personvernombud
d. har ansvar for å inngå skriftlig databehandleravtale hvis eksterne (en virksomhet eller fysisk person) skal behandle personopplysninger på vegne av NTNU
e. er ansvarlig for at databehandleravtale blir gjennomgått hvert andre år og revidert hvis det er behov for det, samt innhente dokumentasjon fra databehandlers sikkerhetsrevisjon
f. er ansvarlig for at personopplysninger som skal overføres til land eller internasjonale organisasjoner utenfor EU/EØS, bare overføres dersom kravene etter EUs personvernforordning kap. V (artikkel 44 flg.) er oppfylt
g. skal sørge for at den det samles inn opplysninger om, blir informert og at henvendelser fra den registrerte blir fulgt opp i samsvar med kravene etter EUs personvernforordning
h. er ansvarlig for at behandlingen (bruk, lagring, sletting, utlevering mm.) av bilde, video-, og lydppopptak, skjer i samsvar med personvernregelverket og i tråd med NTNUs prosesser, rutiner og valgte verktøy/systemer.
i. har ansvar for å sørge for at de fysiske rammebetingelsene ligger til rette for sikker behandling av personopplysninger i enheten
j. har ansvar for å utarbeide rutiner for å minimalisere sikkerhetsrisikoen ved behandling av personopplysninger i enheten, dette innebærer også rutiner for sletting
k. er ansvarlig for at personopplysninger blir slettet på fellesområder i sin enhet
l. skal sørge for fortløpende sletting / opprydding av unødvendige personopplysninger – innen 6 måneder – etter at en ansatt slutter eller en student er uteksaminert eller har sluttet
m. er ansvarlig for at ansatte får nødvendig opplæring i de bestemmelser som gjelder for behandling av personopplysninger

9.11. Prosesseier (vil være direktører)

En prosesseier er en leder i fellesadministrasjonen, som er ansvarlig for gjennomgående administrative prosesser ved NTNU. Prosesseier har ansvar for felles prosedyrer og retningslinjer samt til enhver tid, styre, forbedre og følge opp de gjennomgående prosessene innen sitt ansvarsområde.

a. er ansvarlig for gjennomgående administrative prosesser ved NTNU
b. skal føre oversikt over behandling av personopplysninger (protokoll) for gjennomgående administrative prosesser og har også ansvar for at oversikten blir oppdatert og vedlikeholdt
c. har ansvar for felles prosedyrer og retningslinjer og skal til enhver tid styre, forbedre og følge opp de gjennomgående prosessene slik at de ivaretar kravene til behandling av personopplysninger
d. skal foreta en overordnet risikovurdering av prosesser som behandler personopplysninger
e. har ansvar for å inngå skriftlig databehandleravtale hvis eksterne (en virksomhet eller fysisk person) skal behandle personopplysninger på vegne av NTNU
f. er ansvarlig for at databehandleravtale blir gjennomgått hvert andre år og revidert hvis det er behov for det, samt innhente dokumentasjon fra databehandlers sikkerhetsrevisjon

g. er ansvarlig for at personopplysninger som skal overføres til land eller internasjonale organisasjoner utenfor EU/EØS, bare overføres dersom kravene etter EUs personvernforordning kap. V (artikkel 44 flg.) er oppfylt
h. har ansvar for å utarbeide rutiner for å minimalisere sikkerhetsrisikoen ved behandling av personopplysninger i gjennomgående administrative prosessorer, dette innebærer også rutiner for sletting
i. skal sørge for fortløpende sletting / opprydding av unødvendige personopplysninger – innen 6 måneder – etter at en ansatt slutter eller en student er uteksaminert eller har sluttet

9.12. Forskningsansvarlig

Forskningsansvarlig er den som utøver behandlingsansvaret på vegne av rektor i forskningsprosjekter. Forskningsansvarlig er dekan som har det overordnete ansvaret for alle forskningsprosjekt som foregår ved fakultetet. Dekan kan delegere oppgavene til instituttleder.

a. skal tilrettelegge for at forskning blir utført slik at etiske, medisinske, helsefaglige, vitenskapelige, personvern- og informasjonssikkerhetsmessige forhold blir ivaretatt fra planlegging til avslutning og for etterforvaltning av forskningsdata og humant biologisk materiale.
b. skal sørge for rutiner, infrastruktur og internkontrollsystemer for forskningsvirksomheten i henhold til gjeldende lovverk og retningslinjer og for at disse er implementert og følges i praksis
c. er ansvarlig for at prosjektet blir meldt til Sikt/REK og skal informeres om utfallet av behandlingen
d. skal i forkant eller i etterkant vurdere om prosjektet faller innenfor enhetens strategi og om de nødvendige ressurser foreligger
e. skal etter at et prosjekt er forhåndsgodkjent av REK eller vurdert av Sikt godkjenne prosjektet før det kan settes i gang
f. skal ha oversikt over sin forskningsportefølje
g. skal stanse forskning som er etisk eller juridisk uforsvarlig eller som er i strid med forutsetningene for prosjektet
h. skal gjennomføre systematiske tiltak som fremmer god forskning og som sikrer at forskningen planlegges, organiseres, gjennomføres og avsluttes i samsvar med gjeldende regelverk
i. skal følge opp henvendelser om innsyn mm. fra forskningsdeltakere og er ansvarlig for at informasjonsplikten overfor disse blir fulgt opp

9.13. Prosjektleder og veileder for studentprosjekt

a. Skal foreta risikovurdering[16] og vurdere personvernkonsekvenser i forsknings- student- og kvalitetssikringsprosjekt
b. skal sørge for at det iverksettes tiltak angående forskningsdataene som står i forhold til faktisk risiko basert på en risikovurdering
c. skal i forbindelse med studentprosjekt sørge for at studenter er kjent med reglene for behandling av personopplysninger
d. er ansvarlig for de data som prosjektet samler inn og bruker og skal ha tilgang til alle forskningsdata som prosjektet omfatter

[16] https://i.ntnu.no/wiki/-/wiki/Norsk/Risikovurdering+av+forskningsprosjekter+med+personopplysninger

e. tildeler tilgangsrettigheter og holder oversikt over hvem som har tilgang til dataene
f. Skal følge opp henvendelser om innsyn mm. fra forskningsdeltakere og er ansvarlig for at informasjonsplikten overfor disse blir fulgt opp
g. har det operative ansvaret og skal sørge for internkontroll ved gjennomføringen av forskningsprosjektet, fra planlegging til avslutning, herunder at krav i relevant lovverk og forskningsetiske og interne retningslinjer for informasjonssikkerhet og personvern etterleves
h. skal sørge for nødvendig søknad til REK eller melding til Sikt og at skjema fylles ut i samsvar med hvordan prosjektet gjennomføres i praksis
i. skal involvere forskningsansvarlig i forkant av søknad til REK eller melding til Sikt og legge frem søknad og meldeskjema dersom forskningsansvarlig ber om det
j. skal utarbeide en datahåndteringsplan, jf. punktet Datahåndteringsplan (DMP)[17]
k. skal sørge for at avtaler som er påkrevet for ivaretakelse av informasjonssikkerhet og personvern blir inngått (for inngåelse av databehandleravtaler se punktet Databehandleravtale)
l. er ansvarlig for at relevante og nødvendige dokumentasjonskrav ivaretas i prosjektet
m. skal vurdere om personopplysningene kan pseudonymiseres
n. skal melde fra til forskningsansvarlig og Helsetilsynet om alvorlige, uønskede og uventede medisinske hendelser. Forskningsdeltakerne skal også omgående informeres dersom de har blitt påført skade eller det har oppstått komplikasjoner som følge av forskningsprosjektet.
o. Skal sørge for at personopplysningene blir anonymisert eller slettet ved avslutning av forskningsprosjekt hvis det ikke er krav om lagring etter godkjenninger som er gitt eller i forbindelse med finansiering av forskningsprosjektet, samt sørge for at det blir sendt nødvendige bekreftelser til REK og Sikt

Doktorgradskandidater kan være prosjektledere. Studenter på lavere nivå kan ikke være prosjektledere. Hvis det er kun én forsker er vedkommende prosjektleder.

9.14. Forskningsdatahjelpen/Research Data @NTNU

a. gir rådgivning og veiledning knyttet til behandling av personopplysninger i forskningsprosjekt
b. skal samarbeide med og være kontaktpunkt for Sikt for oppfølging av konkrete prosjekt

9.15. Personvernombudet ved NTNU

a. skal gi NTNUs ledelse og ansatte informasjon og råd om forpliktelser NTNU har i henhold til EUs personvernforordning og annen relevant lovgivning om personvern
b. skal på anmodning gi råd om vurdering av mulige personvernkonsekvenser (DPIA) og kontrollere gjennomføringen av den
c. skal kontrollere overholdelsen av EUs personvernforordning og annen relevant lovgivning om vern av personopplysninger og interne retningslinjer
d. skal holde seg informert om og følge opp avvik ved brudd på personvernet
e. skal samarbeide med og være kontaktpunkt for Datatilsynet og de registrerte

9.16. Personvernrådgiver for Sikt personverntjenester

a. skal gi råd om hvordan NTNU som behandlingsansvarlig best mulig kan ivareta personverninteressene i forskningsprosjekter

[17] https://i.ntnu.no/wiki/-/wiki/Norsk/Datah%C3%A5ndteringsplan

b. skal motta meldinger om behandlinger av personopplysninger i forskningsprosjekter og føre protokoll/oversikt over slike behandlinger i et eget meldingsarkiv

9.17. Eiendomsdirektør

a. har ansvar for lagring av personopplysninger ved adgangskortproduksjon.
b. avgjør om overvåkningskamera skal monteres og er ansvarlig for at rutiner for lagring, sletting og eventuell utlevering blir fulgt. Dette gjelder for hele NTNUs arealer og bygningsmasse

9.18. Alle brukere

a. som skal behandle personopplysninger, er ansvarlige for å sette seg inn i relevant lovgivning for behandling av personopplysninger
b. er ansvarlige for å gjøre seg kjent med retningslinjer og rutiner for behandling av personopplysninger ved bruk av NTNUs IKT-infrastruktur og i forskningsprosjekter og andre prosjekter
c. er pliktige til å melde avvik (uønsket hendelse) ved brudd på personvern i henhold til NTNUs *Retningslinje for avviksmelding og avvikshåndtering innen informasjonssikkerhet og personvern*
d. Hver enkelt medarbeider er ansvarlig for å slette personopplysninger som er lagret på vedkommendes personlige brukerområde.

10. Henvisninger

10.1. Særlig sentrale lover og forskrifter

a. EUs personvernforordning (General Data Protection Regulation (GDPR)) – gir regler for elektronisk behandling som kan knyttes til enkeltpersoner, plikter for NTNU som behandlingsansvarlig og rettigheter for den registrerte.
b. Personopplysningsloven - gjør EUs personvernforordning til norsk lov og gir enkelte bestemmelser i tillegg til forordningen.
c. Universitets- og høyskoleloven – gir regler (supplerende rettsgrunnlag) om behandling av personopplysninger om søkere, studenter og doktorgradskandidater, nasjonal vitnemåls- og karakterportal og rapportering til databaser for høyere utdanning og vitenskapelig publisering.
d. Grunnloven§ 102 – setter krav til vern om den personlige integritet
e. Arbeidsmiljøloven, forskrift til kap. 9
    i. Forskrift om kameraovervåking i virksomheten
    ii. Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale
f. Forvaltningsloven – gir regler om saksbehandling og blant annet taushetsplikt og partsinnsyn.
g. Offentleglova – gir regler om plikt til å gi innsyn i dokumenter samt unntak fra innsynsrett.
h. Arkivloven – gir regler om hvilke dokumenter som er arkivpliktige og krav til arkiveringen.
i. Helseregisterloven – gir regler om innsamling og behandling av helseopplysninger.
j. Helsepersonelloven – gir regler om taushetsplikt og dispensasjon fra denne til forskning.
k. Helseforskningsloven – gir regler om organisering, roller, ansvar og forhåndsgodkjenning av helseforskning.
l. Forskningsetikkloven – gir regler om at forskning skal skje i henhold til anerkjente forskningsetiske normer.
m. Åndsverkloven – gir regler om bruk av bilder (§ 104).

Listen er ikke uttømmende; andre lover og forskrifter kan også være aktuelle.