UNIVERSITETET I AGDER

Retningslinje for personvern

Utarbeidet: Anne Lågstad	**Retningslinje for personvern**	Gyldig fra: 06.07.2018
Eier: Solveig Svendsberget		Sist revidert: 06.07.2018
Godkjent av: Solveig Svendsberget		Versjonsnummer: 00

Innhold

1. Formål

Formålet med UiAs retningslinje for personvern er å gi en overordnet beskrivelse av UiAs håndtering av personopplysninger.

Når UiA behandler personopplysninger, for eksempel ved innsamling, registrering, lagring og utlevering av personopplysninger, gjelder visse krav ifølge personopplysningsloven. UiA plikter å ha en internkontroll for å sikre at personopplysningslovens krav oppfylles i virksomheten. Denne dokumentasjonen er implementert for å oppfylle kravet om internkontroll.

Dette dokumentet gjelder elektronisk og manuell behandling av personopplysninger i administrative systemer ved UiA. Det følger av lov av 14.04.200 nr. 31 om behandling av personopplysninger (personopplysningsloven/pol) § 2 nr. 1) at en personopplysning er «[…] opplysninger og vurderinger som kan knyttes til en enkeltperson»

Dokumentet gir en overordnet beskrivelse av UiAs behandling av personopplysninger, roller og ansvar og hva slags behandling UiA foretar.

2. Gyldig for

Denne retningslinjen er virksomhetsovergripende. Det betyr at den gjelder for alle virksomhetsområder og organisatoriske enheter og er gjeldende for alle medarbeidere og ledere ved fakulteter og administrasjonen ved UiA.

3. Definisjoner

Personopplysning er en opplysning eller vurdering som kan knyttes til deg som enkeltperson.

Opplysninger om atferdsmønstre er også regnet som personopplysninger. Opplysninger om hva du handler, hvilke butikker du går i, hvilke tv-serier du ser på, hvor du beveger deg i løpet av en dag og hva du søker etter på nettet er alt sammen personopplysninger.

Sensitive personopplysninger kan være opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger

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

Behandlingsansvarlig er vedkommende virksomhet som bestemmer hva som skal skje med personopplysningene. Den behandlingsansvarlige skal sørge for at bruken av personopplysninger skjer på en måte som er i samsvar med reglene i loven og GDPR og ikke krenker de registrertes personvern.

Internkontroll. Internkontroll er en prosess, gjennomført av foretakets styre, ledelse og ansatte som er utformet for å gi rimelig sikkerhet vedrørende måloppnåelse innenfor følgende områder;

- Målrettet og effektiv drift
- Pålitelig rapportering
- Overholdelse av lover og regler

Risiko. Risiko kan forstås som summen av hvor sannsynlig en hendelse er, og de konsekvensene hendelsen kan føre til. En risikovurdering forutsetter at det fastsettes mål for virksomheten og aktivitetene. Risiko for ikke å oppnå fastsatte mål kartlegges og analyseres, og danner grunnlag for hva virksomheten velger å gjøre for å kontrollere risikoene.

4. Overordnede føringer og prinsipper

4.1 Grunnlag for behandling

4.1.1 Personopplysninger – Ansatte

Hensikten med behandlingen av personopplysningene om ansatte er personaladministrasjon. Dette omfatter blant annet å oppfylle arbeidsavtalen med den enkelte ansatte, utøve oppdrag pålagt av offentlig myndighet og oppfylle rettslige forpliktelser knyttet til arbeidsforholdet.

4.1.2 Personopplysninger – Studenter

Hensikten med behandlingen er å administrere forholdet og gjennomføre kontraktsforpliktelsene.

4.1.3 Personopplysninger - Eksterne

UiA behandler enkelte personopplysninger om kontaktpersoner hos leverandør og andre samarbeidsforbindelser.

Grunnlag for behandling av personopplysningene er nødvendig for å oppfylle leverandøravtalen/avtalen med annen samarbeidsforbindelse, og er hjemlet i personopplysningsloven § 8 a. Dette er i tråd med formålet med behandlingen.

4.2 De registrertes rettigheter

4.2.1 Informasjon ved innsamling av personopplysninger

Når det samles inn personopplysninger direkte fra den registrerte, skal den UiA av eget tiltak først informere den registrerte om følgende:

- identiteten og kontaktinformasjon til behandlingsansvarlig

- kontaktinformasjon til personvernombudet dersom det er relevant
- formålet ved behandlingen av personopplysningene, samt rettsgrunnlaget for behandlingen
- opplysningene som blir utlevert, og eventuelt hvem som er mottaker
- hvor lenge opplysningene skal lagres
- retten til innsyn, sletting og korrigering
- det er frivillig å gi fra seg opplysningene

4.2.2 Behandling av personopplysninger

Behandling av personopplysninger kan bare skje når det er tillatt etter personopplysningsloven §§ 8 og 9. Alternative behandlingsgrunnlag er:

- Samtykke
- Oppfyllelse av avtale
- Oppfyllelse av rettslig forpliktelse
- Berettiget interesse

Personopplysningene kan bare nyttes til uttrykkelig angitt formål som er saklig begrunnet i UiA sin virksomhet. Opplysningene kan ikke brukes til andre formål enn det opprinnelige formålet med innsamlingen. Når personopplysninger behandles, må de være korrekte og oppdaterte og de skal ikke lagres lenger enn nødvendig ut fra formålet med behandlingen.

4.2.3 Innsyn

Når det er samlet inn og behandles personopplysninger, har den registrerte rett til innsyn i personopplysninger tilknyttet seg selv. Ved innsyn skal det informeres om følgende:

- Formålet med behandlingen
- Hvilken kategori av opplysninger
- Eventuelle mottaker av opplysningene
- Hvor lenge opplysningene skal lagres
- Retten til å be om korrigering, sletting
- Retten til å klage

- Hvor opplysningene stammer fra

Den registrerte kan kreve at UiA utdyper informasjonen i første ledd bokstav a – f i den grad dette er nødvendig for at den registrerte skal kunne ivareta egne interesser.

4.2.4 Retting av personopplysninger

Dersom det viser seg at registrerte personopplysninger er uriktige, ufullstendige skal UiA av eget tiltak, eller på begjæring av den registrerte, rette de mangelfulle opplysningene uten ugrunnet opphold.

Retting av uriktige eller ufullstendige personopplysninger som kan ha betydning for dokumentasjon, skal skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger.

4.2.5 Sletting av personopplysninger

Den registrerte har rett til å kreve personopplysninger slettet på følgende grunnlag:

- Personopplysningene er ikke lenger nødvendige for formålet
- Den registrerte trekker tilbake samtykket
- Den registrerte gjør innsigelser mot behandlingen
- Personopplysningene er blitt behandlet ulovlig.
- Personopplysningene må slettes for å oppfylle en rettslig forpliktelse
- Personopplysningene er samlet inn i forbindelse med tilbud om informasjonssamfunnstjenester

Reglene om sletting inntreffer blant annet ikke dersom behandling av personopplysningene er nødvendig for arkivformål. UiA skal sørge for å underrette enhver mottaker som opplysningene er videreformidlet til om at sletting er utført.

4.2.6 Begrensing av behandling

Den registrerte har rett til å kreve at behandlingen av personopplysninger begrenses dersom følgende alternative forhold gjør seg gjeldene:

- Opplysningenes riktighet er omtvistet

- Behandlingen er ulovlig og den registrerte motsetter seg sletting av personopplysninger og isteden anmoder om begrensning
- Behandlingen ikke lenger er nødvendig, men opplysningene trengs for å fastsette, gjøre gjeldene eller forsvare et rettskrav
- Den registrerte har protestert mot videre behandling i påvente av en avgjørelse av om videre behandling kan finne sted

4.2.7 Underrettelse om retting, sletting og begrensning

Den behandlingsansvarlige plikter å sørge for å underrette enhver mottager som opplysningene er videreformidlet til om at retting, sletting eller begrensning er utført. Videre plikter UiA, dersom den registrerte anmoder om det og å opplyse den registrerte om hvem disse mottagerne er.

4.2.8 Manuell behandling av personopplysninger

Dokumenter som inneholder personopplysninger skal oppbevares forsvarlig. Leder for den enkelte avdeling/enhet må sørge for tilfredsstillende rutiner for oppbevaring av slike dokumenter.

4.3 Innebygd personvern

Alle nye systemer og tiltak skal utarbeides på en mest mulig personvennlig måte, jf. kravet om innebygd personvern i forordningens artikkel 25. Innebygd personvern skal sørge for at informasjonssystemene UiA bruker oppfyller personvernprinsippene, og at de ivaretar de registrertes rettigheter.

Dersom et tiltak utgjør en stor risiko for personvernet, skal systemeier utrede hvilke personvernskonsekvenser det kan ha. Dersom utredningen viser at risikoen er stor og UiA selv ikke kan redusere denne, skal Datatilsynet kontaktes.

Spørsmål som må vurderes før oppstart:

- Hva er formålet med systemet
- Hva slags personopplysninger er nødvendige å behandle
- Hvordan kan personopplysningene sikres mot autorisert innsyns?
- Hva slags sikkerhet er det ellers behov for ved behandlingen?

Det må gis grundig opplæring til de databehandlerne/ansatte som skal arbeide med systemene. Databehandlere/ansatte må gjøres oppmerksom på at de har taushetsplikt.

5. Organisering av personvern på UiA

UiA er behandlingsansvarlige for alle personopplysninger som benyttes i undervisning, administrasjon, forskning og formidling. Dette gjelder også når driften av systemer eller andre tekniske løsninger hvor personopplysninger behandles er satt ut til eksterne aktører.

UiA er ansvarlig for personopplysninger som behandles om ansatte, studenter og samarbeidspartnere samt om eventuelle kontaktpersoner/andre hos leverandører og andre forbindelser (behandlingsansvarlig). UiA har ansvaret for å overholde de plikter som er angitt i eller fastsatt i medhold av personopplysningsloven. Det daglige behandlingsansvaret har universitetsdirektøren. Assisterende universitetsdirektør er delegert ansvaret for den praktiske utførelsen av personvernansvaret.

Det forventes at ledere og fagansvarlige på alle nivåer ivaretar ansvaret for håndtering av personopplysninger og internkontroll i alle prosesser og aktiviteter innenfor eget ansvarsområde. Dette innebærer også ansvar for at medarbeiderne har tilstrekkelig kompetanse og kunnskap om de policyene, retningslinjene og rutinene som er relevante for deres arbeidsoppgaver. Ansvaret innebærer blant annet å påse at avvik, feil og mangler blir håndtert på en tilfredsstillende måte, og å legge til rette for kontinuerlig forbedring og læring.

5.1 Roller og ansvar

5.1.1 Overordnet ansvar

Universitetsdirektøren skal sørge for at:

- arbeidet med personvern og behandling av personopplysninger er hensiktsmessig organisert
- det stilles krav til arbeidet med personvern og behandling av personopplysninger
- arbeidet med personvern og behandling av personopplysninger prioriteres og tilføres tilstrekkelige ressurser
- arbeidet med personvern og behandling av personopplysninger følges opp og kontrolleres

Universitetsdirektøren har et særlig ansvar for informasjonssikkerheten til personopplysninger som behandles. Dette er beskrevet i ledelsessystem for informasjonssikkerhet.

5.1.2 Det daglige ansvaret for arbeidet med personvern

Assisterende universitetsdirektør følger opp og kontrollerer arbeidet med personvern og behandling av personopplysninger i fellesadministrasjonen og ved fakultetene.

Assisterende universitetsdirektør skal påse og legge til rette for at fellesadministrasjonen og fakultetene ivaretar:

- de lover og regler som gjelder for personvern og behandling av personopplysninger

- de krav som styret og rektor stiller til arbeidet med personvern og behandling av personopplysninger

Assisterende universitetsdirektør oppfølgings- og kontrollansvar utøves gjennom internkontrollen på følgende måter:

- Gjennom årlig egenkontroll og rapportering
- Gjennom informasjon om hvilke rutiner og regler som gjelder for behandling av personopplysninger på overordnet nivå (se også personvernombudets oppgaver)
- Gjennom støtte og veiledning til avdelinger og enheter ved behov (se også personvernombudets oppgaver)
- Gjennom rapportering av funn fra årlig internkontroll, stedlige kontroller og alvorlige avvik til universitetsdirektøren

5.1.3 Ansvaret for personvern i administrasjonen

Direktører i fellesadministrasjonen og fakultetsdirektørene er utpekt som eiere av systemer og tjenester innenfor sine respektive ansvarsområder og fagområder. System- og tjenesteeiere har ansvaret for enkelte personvernoppgaver ved behandling av personopplysninger i sine systemer eller tjenester. I dette inngår:

- Innkjøp/utvikling av systemet eller tjenesten
- Før bruken av systemet eller tjenesten starter
- Mens systemet eller tjenesten er i bruk
- Ved avvikling av systemet eller tjenesten
- Register for personopplysninger (ut i fra kartleggingsskjema)

Systemadministratorer har en operativ utførerrolle på vegne av systemeier og vil i det daglige sikre at personvernet blir ivaretatt i systemene.

Fagansvarlige for saksbehandling har ansvaret for enkelte personvernoppgaver ved behandling av personopplysninger. Dette gjelder både i fellesadministrasjonen og ved fakultetene. Teamledere/enhetsledere har ansvaret for enkelte personvernoppgaver ved behandling av personopplysninger innenfor for sitt team/enhet.

Dette ansvaret utføres gjennom:

- Gjennom utarbeidelse av rutiner og regler for behandling av personopplysninger

- Gjennom informasjon om hvilke rutiner og regler som gjelder for behandling av personopplysninger
- Gjennom håndtering av avvik

Alle saksbehandlere har et selvstendig ansvar for personvern når de håndterer personopplysninger, både elektronisk og manuelt.

5.1.4 Fordeling av utførende oppgaver i det daglige

Håndtering av henvendelser fra de registrerte (innsyn, sletting o.l.) fra ansatte, studenter, gjesteforskere og andre eksterne utføres og håndteres av IT. Henvendelsene meldes inn via Service Now og går direkte til IT som organiserer innhenting av opplysningene og sender informasjonen ut med et standard svarbrev via Digi post.

5.1.5 Ansvaret for personvern i forskningen

Medisinsk og helsefaglig forskning er underlagt helseforskningsloven og andre særlover på helseområdet. Forskere skal følge de rutiner og retningslinjer som gjelder for personvern og behandling av personopplysninger innenfor disse fagområdene.

All øvrig forskning ved UiA skal skje i henhold til våre rutiner for personvern i forskning.

Ansvaret for personvern og behandling av personopplysninger i forskning som ikke regnes som medisinsk eller helsefaglig, er organisert på følgende måte:

- Prosjektledere i forskning har et selvstendig ansvar for personvernet til respondenter eller informanter i forskningsprosjekter (ph.d.-studenter regnes som prosjektledere for sine ph.d.-prosjekter)
- Studentveiledere har ansvar for personvernet til respondenter eller informanter i studentforskning på bachelor- og masternivå
- Studenter har et selvstendig ansvar for personvernet til respondenter eller informanter i studentforskning på bachelor- og masternivå
- Fakultetsdirektøren skal sikre at den enkelte forsker eller veileder er informert om UiAs rutiner for behandling av personopplysninger i forskning
- Det daglige behandleransvaret for personopplysninger i forskning ligger hos forskningsadministrativ avdeling (FAA)

5.2 Personvernombud

I offentlig sektor er det et krav til personvernombud.

Personvernombudets oppgaver utøves:

- Gjennom juridisk rådgiving, og rådgivning i vurdering av personvernkonsekvenser
- Gjennom opplæring av ledere/ansatte og kompetanseheving (seminar og kurs)
- Gjennom stedlige kontroller i fellesadministrasjonen og ved fakultetene av behandling av personopplysninger

6. Informasjonssikkerhet

Ledelsessystemet for informasjonssikkerheten skal sørge for at personopplysninger som behandles ved UiA er beskyttet mot brudd på konfidensialiteten, integriteten og tilgjengeligheten.

7. Internkontroll

Assisterende universitetsdirektørens ansvar for internkontroll som skal utføres i avdelinger og fakulteter og utøves på følgende måte:

- Årlig egenkontroll av behandling av personopplysninger
- Gjennom ROS analyser av systemer, ref. Ledelsessystem for informasjonssikkerhet
- Gjennom utarbeidelse av rutiner og retningslinjer for behandling av personopplysninger
    - Oppdatering av rutiner og retningslinjer for personvern skal gjennomgås/oppdateres ved endring av behandlinger, endring i lover og regler, forbedringsarbeid og ved endring av risiko
- Gjennom håndtering av avvik
- Gjennom rapportering av funn, kontroller, avvik og tiltak til universitetsdirektøren

8. Eierskap og implementering av retningslinje

Universitetsdirektøren, som eier av denne retningslinjen, er ansvarlig for utforming og implementering av denne retningslinjen og for at den til enhver tid er oppdatert. Det utførende arbeidet kan delegeres.