UiO : Universitetet i Oslo

Rollefordeling og begrepsforståelse ved UiO etter nytt personvernregelverk

NARMA vårkonferanse 2019

Maren Magnus Voll
Personvernombud

UiO – en stor virksomhet
GDPR – et kjent regelverk

- Ca. 13 000 årsverk
- Ca. 30 000 studenter
- millioner av forskningssubjekter

UiOs mål - nytt personvernregelverk for forskningsprosjekter

- Være åpne om at det medfører endringer og utfordringer for UiO
- Sikre ivaretakelse av nytt regelverk, UiOs ansvar
- Sikre at forskningen ikke stopper opp
- Sikre at forskerne får enklest mulig overgang og gi bistand underveis
- Gi god informasjon til forskerne og forskningsrådgivere

Rammene for forskning ved UiO

- Alt relevant lovverk
  - herunder blant annet personopplysningsloven, personvernforordningen, helseforskningsloven, forskningsetikkloven etc.
- Kvalitetssystem for medisinsk og helsefaglig forskning
- Interne rutiner, sjekklister for øvrig forskning på personopplysninger
- Etiske retningslinjer
- Under arbeid: overordnet kvalitetssystem for forskning på personopplysninger

Forskningsansvarlig – helseforskningsloven § 4 (e)

- «institusjon (…) som har det overordnede ansvaret for forskningsprosjektet, og som har de nødvendige forutsetningene for å kunne oppfylle den forskningsansvarliges plikter etter denne loven»

Forskningsansvarlig ved UiO

- Overordnet ansvarlig: universitetsdirektøren
  - ansvaret for prosjektledere med institusjonstilknytning, systemansvar for organisering og gjennomføring av aktuelle forskningsprosjekter
- Det daglige ansvaret: delegert til fakultetene ved dekan
  - Ordinær ansvarsdelegering ved fakultetene følger: instituttleder er ansvarlig for enhetens prosjekter ved hvert enkelt institutt
  - Instituttleder: ansvar for etterlevelse av rutinene ved egen enhet. Kan igjen delegere til daglig ansvarlig som ofte vil være avdelingsleder i faglig linje/forskningsleder/forskningsgruppeleder
- UiO kan delegere oppgaver til eksterne, men kan aldri delegere bort ansvaret

Behandlingsansvarlig – GDPR art. 4 (7)

- «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»

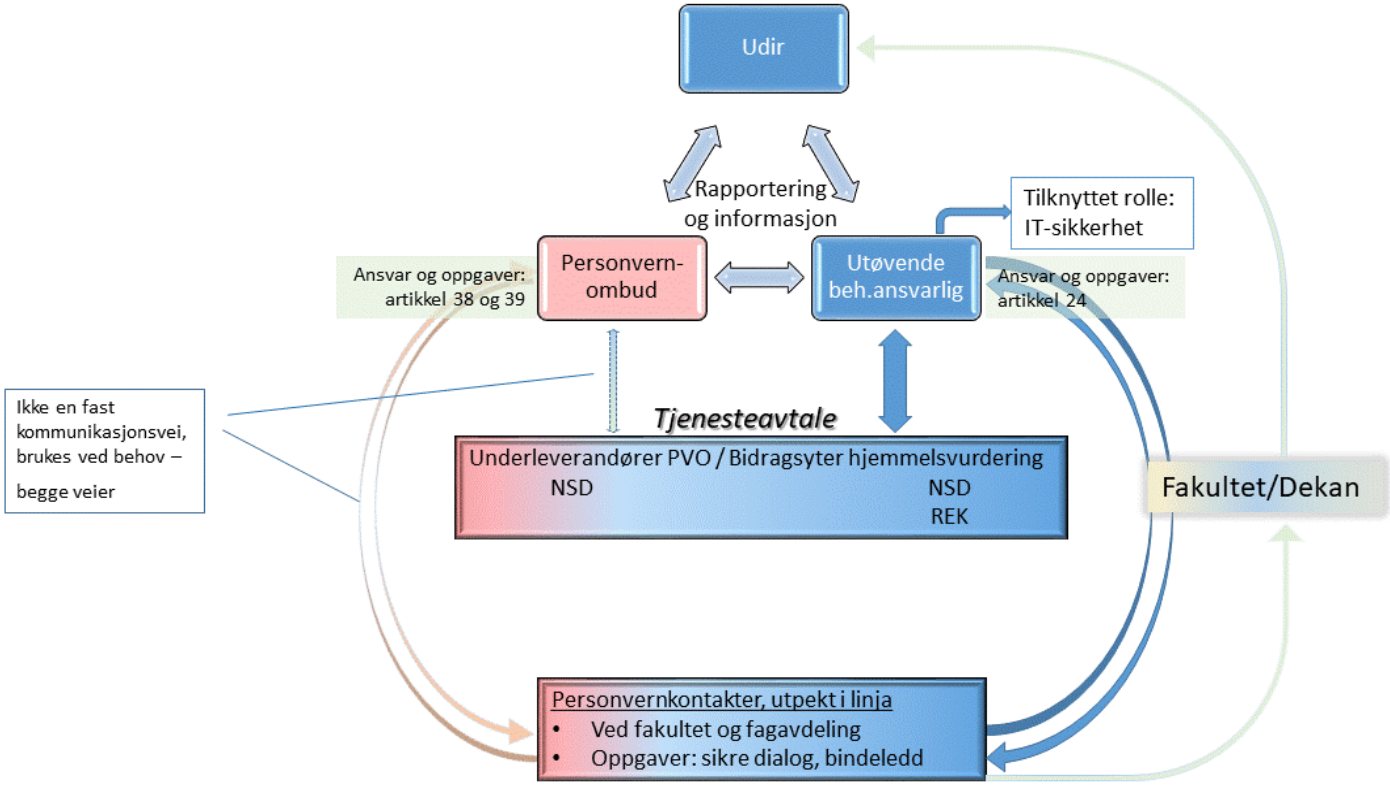
Behandlingsansvaret ved UiO

- Formelt ansvar: styret ved rektor
- Daglig ansvar: universitetsdirektøren
  - Følger tilsvarende linje som for forskningsansvarlig
  - Utøver av det daglige behandleransvaret: IT-direktøren og hans jurister
    - Rådgivende og kontrollerende rolle

- Behandlingsansvarlig er ansvarlig for det våre studenter og forskere gjør. Skal kunne påvise at UiO følger alle prinsippene og kravene etter GDPR.
  - Inkluderer personopplysningssikkerheten
    - Blant annet: Konfidensialitet, integritet og robusthet i systemene og tjenestene som brukes i forskningen
- Annen terminologi
  - Databehandlingsansvarlig, dataansvarlig

Andre relevante roller ved UiO

- Personvernkontakter ved enhetene
  - Opprettet for å sikre god dialog og et bindeledd mellom enhetene, utøver av behandleransvaret og personvernombudet. Kommunikasjon, opplæring og mottak av henvendelser.
- Personvernombud
  - Hovedoppgaven er å informere og gi råd om de forpliktelsene virksomheten har etter personvernlovgivningen til den behandlingsansvarlige eller databehandleren, samt til de ansatte som utfører behandlingen av personopplysninger.
- NSD (Norsk senter for Forskningsdata)
  - Leverer personvernrådgivningstjenester til UiO etter avtale


Udir
Rapportering og informasjon
Tilknyttet rolle: IT-sikkerhet
Ansvar og oppgaver: artikkel 38 og 39
Personvern-ombud
Utøvende beh.ansvarlig
Ansvar og oppgaver: artikkel 24
Ikke en fast kommunikasjonsvei, brukes ved behov – begge veier
Tjenesteavtale
Underleverandører PVO / Bidragsyter hjemmelsvurdering
NSD
NSD
REK
Fakultet/Dekan
Personvernkontakter, utpekt i linja
• Ved fakultet og fagavdeling
• Oppgaver: sikre dialog, bindeledd

Utfordringer fra nytt regelverk og lovproposisjonen

- «som et utgangspunkt [bør] gjeldende konsesjoner ikke videreføres ved ikrafttredelse av ny personopplysningslov.»
- «REKs forhåndsgodkjenning vil ikke lenger utgjøre et nødvendig og tilstrekkelig behandlingsgrunnlag»
- UiO må selv godkjenne forskningsprosjekter som behandler personopplysninger

Hvordan det ble løst - behandlingsgrunnlag

- Universitetsdirektøren fattet et vedtak for eksisterende forskning:
  - Eksisterende konsesjoner fra Datatilsynet videreføres
  - Eksisterende vedtak fra REK videreføres
  - Eksisterende tilrådinger fra NSD videreføres

  På følgende vilkår:
  - Har tilsvarende behandlingsgrunnlag i GDPR art. 6 og 9
  - Følger fastsatte vilkår
  - Skal igjen vurderes ved utløp av frister eller ved endringer i prosjekt

- UiO har vurdert at personvernet er tilstrekkelig ivaretatt ved tidligere godkjenninger med de vilkår som ble satt

Tidligere regelverk

Andre myndigheter og institusjoner godkjente på vegne av UiO

- Medisinsk og helsefaglig forskning – REK
  - REKs vedtak hadde tidligere både personvernrettslig betydning og forskningsetisk betydning
    - Vedtakene har nå kun forskningsetisk betydning
- Forskning som faller utenfor REK
  - NSD var tidligere personvernombud for forskning
    - Kunne godkjenne/tilrå prosjekter
  - NSD er ikke lenger personvernombud
  - Personvernombudet har ikke lenger tilrådingsmyndighet
- Enkelte typer forskning måtte få konsesjon fra Datatilsynet
  - Datatilsynet gir ikke lenger konsesjoner

Nytt regelverk

- UiO er formelt ansvarlig for å vurdere og godkjenne forskningen selv

  – Der forskningen innebærer en høy risiko for den registrertes rettigheter og friheter krever GDPR en personvernkonsekvensvurdering (data protection impact assessment - DPIA)
    - Kan også være tilfeller som krever forhåndsdrøftelse med Datatilsynet

  – Basert på vurderingen må UiO avgjøre om personvernet og rettigheter og friheter er tilstrekkelig ivaretatt og vi kan godkjenne forskningen

Vurdering av medisinske og helsefaglige forskningsprosjekter

- Midlertidig prosedyre
  - UiO og forsker mottar vedtak fra REK
  - REKs etiske vurdering skal i henhold til helseforskningsloven sammenfalle med en DPIA på flere punkter
  - Vedtak og forskningsprosjekt gås igjennom av personvernombudet og utøver av behandleransvaret
    - Vurderes
    - Utføres DPIA sammen med forsker ved behov
  - Forsker får beskjed om utfall og kan starte forskningen

Vurdering av øvrig forskning på personopplysninger

- NSD leverer personverntjenester til UiO for prosjekter som behandler personopplysninger (og som ikke er omfattet av helseforskningsloven)
- Prosess
  - NSD vurderer prosjektene og gir forsker sin vurdering med kopi til UiO
  - For forskning som krever DPIA, gjør NSD dette og sender sin vurdering til UiO
    - Vurderingen gjennomgås av personvernombud og utøver av behandleransvaret
  - NSD får beskjed om utfall – NSD videreformidler beskjed til forsker
  - Forsker forholder seg (stort sett) kun til NSD

- For forsker: I praksis likt som etter tidligere regelverk

Hvorfor midlertidig løsning?

- REK
  - UiO skal kartlegge hva som må vurderes i tillegg til REKs vurdering for å oppfylle krav til en DPIA
  - Arbeidet skal legges til grunn for arbeid med «Kvalitetssystem for behandling av personopplysninger i forskning»
  - Må godkjenning gjøres sentralt, eller vil enhetene enkelt kunne godkjenne egen forskning?
  - Har UiO riktig og nok kompetanse til å gjøre vurderingene?

- NSD
  - UiO vurderer hvordan godkjenningen av prosjekter fungerer og eventuelt foreslå endringer internt og i dialog med NSD

UiOs mål fremover

- Ha færrest mulige «postkasser» for forskerne
- Sikre god flyt ved oppstart, underveis og ved avslutning av forskningsprosjekter
- All forskning registreres ett sted
- Mindre prosjekter (inkludert BA/MA-oppgaver) bør kunne vurderes og godkjennes lokalt på enheten
- Fortsette arbeidet med å utarbeide gode sjekklister og gi informasjon til studenter og forskere

personvernombud@uio.no