**Forslag til mandat og organisering av prosjektgruppe for forberedelse til ny personvernforordning (GDPR) og nytt personvernregelverk –**

1. **Bakgrunn** 
   1. *Nytt personvernregelverk*

Den 25. mai 2018 trer EUs nye personvernforordning («General Data Protection Regulation» - GDPR) i kraft. Personvernforordningen er foreslått inntatt i norsk rett som del av ny personopplysningslov (inkorporasjon via henvisningsbestemmelse). Forslaget til ny personopplysningslov var på høring med høringsfrist i oktober, og ligger nå til behandling i Justisdepartementet. Regelverket vil tre i kraft i Norge fra samme dato som i EU.

Personvernforordningen viderefører mange av bestemmelsene i gjeldende lovgivning, men innebærer også flere nye og til dels strengere krav til behandling av personopplysninger. Ved NTNU som øvrige institusjoner i UH-sektoren, behandles personopplysninger i stort omfang for flere formål. Innenfor personal- og studieadministrasjon og i forskning, er omfanget av behandling av personopplysninger særlig omfattende.

Manglende etterlevelse av ulike deler av personvernforordningen vil medføre at NTNU ikke behandler personopplysninger på en lovlig måte; knyttet til lovgrunnlag for selve behandlingen, informasjonssikkerhet, oppfyllelse av registrertes rettigheter, mv. Mangelfull behandling av personopplysninger kan ha store konsekvenser for enkeltpersoner, hvis opplysningene eksempelvis kommer på avveie som følge av at NTNU ikke overholder sine forpliktelser. Det vil også være en rekke konsekvenser for universitetet selv. Omdømmetap vil være nærliggende i slike situasjoner, og kan gå ut over samfunnets tillit til universitetet, både som institusjon og offentlig myndighetsorgan, men også som forskningsaktør.

Økonomiske konsekvenser kan ha direkte form av administrative bøter ilagt av Datatilsynet, inntil 4 % av årlig omsetning, men også i form av at eksempelvis forskningsprosjekter blir forsinket eller stengt ned, at doktorgradsprosjekt må avbrytes eller at doktorgrader trekkes tilbake, noe som også vil kunne ha store personlige konsekvenser for de det gjelder.

*1.2. Tilnærming*

Selv om reglene i all hovedsak videreføres, innebærer det nye regelverket en del endringer, ved for eksempel at meldeplikt og konsesjonsplikt bortfaller og erstattes med en institusjonell plikt til internkontroll, herunder krav til risikovurderinger og vurdering av personvernkonsekvenser. I tillegg stilles det klare krav til dokumentasjon, oversikt over behandlinger av personopplysninger, bestemte krav til innhold i databehandleravtaler (avtaler med leverandører som behandler personopplysninger på vegne av NTNU), frister for varsling til Datatilsynet ved avvik ved håndteringen av personopplysninger, og krav til informasjon og varsling til de registrerte, mv. Dette nødvendiggjør behovet for et eget prosjekt for personvern, noe flere av andre institusjoner innen UH-sektoren er i ferd med å etablere eller allerede har etablert.

|  |
| --- |
| Ved NTNU er mye er på plass, ved innføring av et ledelsessystem for informasjonssikkerhet. Like fullt er det mye som må kartlegges, utarbeides og vurderes innen mai 2018. For NTNU som andre virksomheter er det påkrevet å ha en fullstendig oversikt over hvilke system vi behandler personopplysninger i.  Det vises videre til forordningens innskjerpelse av dokumentasjon på etterlevelse av regelverket.. Dette gjelder både på systemnivå, på policynivå samt på rutinenivå. |
| *1.2.1 Styrings- ledelsessystem for informasjonssikkerhet*  Offentlige virksomheter skal i henhold til eforvaltningsforskriften §15 etablere mål og strategi for informasjonssikkerhet og et tilfredsstillende system for internkontroll. NTNU har et pågående prosjekt om innføring av et ledelsessystem for informasjonssikkerhet, i tråd med ISO 27001:13.  Det vil være viktig å implementere ledelsessystemet og se på nye krav til behandling av personopplysninger i sammenheng, en del vil være overlappende, og mandat til GDPR-prosjekt må ta hensyn til dette.  *1.2.2.Sektorielt samarbeid/BOTT/Uninett*  Prosjektet bygger på og gjennomfører deler av prosjektet i samarbeid med BOTT og i samarbeid med sekretariatet for informasjonssikkerhet i Uninett. |
| *12.3. IT-politiske føringer*  IT-avdelingen har nedsatt internt prosjekt for å se nærmere på kravene i nytt personvernregelverk. Dette arbeidet må koordineres med dette forslaget til prosjekt. |
|  |
|  |

1. **Mandat til prosjekt**

På ovennevnte bakgrunn bes det om at rektor oppretter et prosjekt som skal gjennomføre kartlegging og nødvendige tiltak for at NTNU som organisasjon oppfyller kravene etter den nye personopplysningsloven (inkludert personvernforordningen).

Formålet med prosjektet er at NTNU skal ivareta ansattes, studenters og øvrige registrertes interesser og personsikkerhet gjennom lovlig, god og sikker behandling av personopplysninger

Prosjektet skal sørge for at det iverksettes nødvendige tiltak slik at alle behandlinger av personopplysninger ved NTNU skal være i samsvar med nytt personvernregelverk i mai 2018. Det er viktig at NTNU gjennom prosjektet opplever og tar eierskap til oppfølging av personvernregelverket.

II

*Utkast/Foreløpig mandat for personvernprosjektet:*

1. Skaffe oversikt og kartlegge behandlinger av personopplysninger
2. se på alle behandlinger av personopplysninger i virksomheten, herunder formålet med innsamlingen. Prosjektet skal undersøke om bruken av opplysningene har gyldig hjemmel
3. peke på aktuelle behandlinger der det må gjennomføres personvernkonsekvensvurdering etter kriteriene fastsatt i personvernlovgivningen, eller av tilsynsmyndighetene.
4. utarbeide nye retningslinjer for behandling av personopplysninger
5. sørge for plan for gjennomføring av risiko- og sårbarhetsvurdering samt verdivurdering av større, aktuelle systemer, prosesser og behandlinger
6. sikre/fullføre tilpasning av avvikssystemet til de nye kravene
7. identifisere nødvendige systemer for å sikre dokumentasjonsplikt, kontroll-/samsvarsplikt
8. påse at interne instrukser, reglementer, retningslinjer, veiledere, mv., for NTNU harmoniseres og oppdateres til å etterleve personvernforordningen.
9. påse at personvernerklæringer utarbeides der det er nødvendig
10. fremme forslag for ivaretakelse av personvernrådgiverrollen (ombud); sett i sammenheng med forskning, eget personvernombud og NSD.
11. identifisere opplæringsbehov og sørge for plan for nødvendig opplæring for å bevisstgjøre ansatte og studenter, og sette de i stand til å etterleve de krav som stilles i lovverket
12. identifisere behov knyttet til kompetanseutvikling og bemanning for å ivareta forpliktelsene etter forordningen

1. påse at styringssystemet for informasjonssikkerhet implementeres i tråd med personvernregelverket
2. vurdere hvordan de registrertes rettigheter, herunder krav om innsyn, kan imøtekommes, herunder svarfrist på 1 måned.
3. sørge for oversikt over av databehandleravtaler og påse at enhetene ved NTNU er kjent med sitt ansvar for at det finnes avtalerder slike skal være på plass.
4. oppdatere/lage maler/sjekklister (feks. Mal for databehandleravtaler, ol.).
5. identifisere behov knyttet til infrastruktur; endringer, behov for ny teknologi, utstyr mv., og fremme forslag til utbedring
6. **Mål for prosjektet**
   1. **Resultatmål:**

Overordnet formål med prosjektet er at NTNU skal ivareta ansattes, studenters og forskningsdeltakeres og øvrige registrertes interesser og personvern gjennom lovlig, god og sikker behandling av personopplysninger gjennom:

* Ledere, ansatte og studenter skal etter endt prosjekt ha økt kunnskap om krav til behandling av personopplysninger og kunnskap om hvordan personverninformasjon skal sikres.
* Ny retningslinje for behandling av personopplysninger skal være utarbeidet, og i tråd med nytt personvernregelverk.
* NTNU skal ha oversikt over systemer der personopplysninger behandles, og ha en risikobasert tilnærming på sikring av opplysningene.
* Registrerte ved NTNU skal ha gjennom utarbeidelse av personvernerklæringer skal kunne vite hvordan personopplysninger om dem behandles
* NTNU skal kunne oppfylle sine forpliktelser til å gi innsyn i de registrertes rettigheter
* Databehandleravtaler skal være inngått og systematisk gjennomgått for å oppfylle krav i regelverket
  1. **Effektmål:**

Ledere, ansatte og studenter i NTNUs virksomhet skal ha økt forståelse av verdien av personopplysninger og bevissthet til hvordan personopplysninger håndteres i det daglige.

1. **Gjennomføring av prosjektet - ressursbehov og tidsramme**
   1. **Tidsplan**

Prosjektet vil ha hovedtrykk på arbeid frem til 25. mai 2018, men vil løpe ut året 2018.

Det skal utarbeides en detaljert framdrifts- og milepælsplan. Denne skal legges fram for og godkjennes av styringsgruppen i første møte.

Arbeidsgruppen organiserer selv arbeidet i prosjektet og trekker inn andre ressurspersoner ved behov. Arbeidsgruppen kan pålegge NTNUs enheter å foreta nødvendige gjennomganger og endringer for at NTNU skal være i samsvar med personvernregelverket. Prosjektet og framdriften i dette skal dokumenteres.

Lederen kaller inn til møter i arbeidsgruppen, koordinerer gruppens arbeid, og sikrer oppfølging av bestillinger gjort til medlemmer av gruppen eller andre ressurspersoner og rapporterer til styringsgruppen.

Arbeidsgruppen skal starte med planlegging og involvering av de rette ressursene. Rett system for kartlegging må vurderes og identifiseres.

Kartleggingen må sendes ut til miljøene, og koordineres. Etter innsamling må arbeidsgruppen ha særlig oppmerksomhet på områder der det oftest forekommer brudd på personvernreglene, eventuelt der personvernkonsekvensene av behandlingen er størst for de registrerte.

Kartlegging av behandlinger skal være gjennomført i løpet av april måned. Vurderinger skal skje i etterkant og håndteres der man finner avvik.

Ved nedsettelse av prosjekt om internkontroll, vil dette prosjektet ha overordnet og koordinerende status for personvernprosjektet. Styringsgruppen for herværende prosjekt vil fungere midlertidig inntil prosjektet for internkontroll er operativt.

**Prosjektet vil omfatte følgende faser:**

1. **Planleggingsfasen**: omfatter bl.a. å definere omfang/planlegge, allokere ressurser, utarbeide fremdriftsplan, og angi risikonivå (risikoen for selve gjennomføringen av prosjektet)
2. **Kartleggingsfasen**: kartlegge personopplysninger som behandles, behandlingsmåte, informasjonssystemer, bruk av leverandører/underdatabehandlere, overføring til tredjeland, rutiner og prosedyrer, dokumentasjon mv.

(Kartleggingsfasen skal være gjennomført senest innen 25. mai.)

1. **Vurderingsfasen**: Vurdere behandlingen av data og informasjon, identifisere avvik fra regelverket og akseptert risikonivå og tilhørende risikoelementer
2. **Utbedringsfasen**: håndtere eventuelle avvik og utbedre disse. Se på bakenforliggende faktorer for hvorfor aktuelle avvik oppstår. Endre rutiner ved behov. Sørge for tilstrekkelig dokumentasjon i henhold til nye regler og utarbeide sjekklister og maler. Videre etter mai, se på etterlevelsen.
   1. **Ressursbehov**

Prosjektet vil kreve ressurser. Det er viktig at det settes av tilstrekkelig med ressurser i prosjektet, og at avtaler med den enkelte prosjektdeltaker inngås, slik at man sikrer ressursen. Prosjektdeltakernes innsats vil være regnet til minimum 50 prosent, og opp mot100 prosent frem til utløpet av mai.

Ressurser knyttes til timeverk i gjennomføringen, og eventuelt også til direkte kostnader knyttet til eventuelle anskaffelser og utbedringer. Sistnevnte vil måtte samkjøres langt på vei med arbeidet med informasjonssikkerhet.

*4.2.2 Er anskaffelse(r) av varer og tjenester aktuelt?*

I hovedsak bør prosjektet kunne gjennomføres med interne ressurser.

Eventuelt behov for IT-løsninger/system eller justeringer av slike må vurderes, for å utbedre eller forhindre avvik mot de nye reglene, og sikre innebygd personvern.

Det vil være aktuelt med kjøp av eksterne tjenester, f.eks. juridiske tjenester for vurdering og håndtering i forbindelse med avtaler og vurdering av behandlingsgrunnlag.

* 1. **Prosjektorganisering og ansvar**

Riktig sammensetning av prosjektgruppen er avgjørende. Prosjektgruppen bør bestå av ressurspersoner med juridisk, organisatorisk og teknisk kompetanse.

Det er nødvendig å være kjent med eller gjøre seg kjent med personvernregelverket på variert nivå, samt at gruppen må dekke kunnskap om NTNUs IT-systemer og informasjonssikkerhet, forskningsprosessen, studiesiden og ha organisasjonsforståelse. Det er også viktig at gruppen skal ha kraft til jevnlige møter og jobbe systematisk og kunne være leveringsdyktig. Gruppen må ikke være større enn seks personer.

**Prosjektgruppen**

1. Prosjektleder (Åshild Margrethe Revhaug, Avdeling for virksomhetsstyring)
2. Forskningsadministrativ støtte, gjerne fra fak. SU/MH
3. En fra IT-avdelingen
4. En fra studieavdelingene
5. En fra HR/HMS-avdelingen, evt. tilsvarende kompetanse fra fak.
6. En fra dokumentasjonsforvaltning
7. Personvernombudet fra mars.

**Styringsgruppen (midlertidig sammensetning)**

Styringsgruppen fungerer midlertidig inntil styringsgruppe for Internkontrollprosjektet er etablert og operativt.

Styringsgruppen består av:

Ida Munkeby, organisasjonsdirektør, Bjarne Foss, prorektor for forskning, Dekan for SU, Knut Veium avdelingsdirektør for studieadministrasjon, Roar Tobro, avdelingsdirektør for virksomhetsstyring, Arne Hestnes, avdelingsdirektør for HR/HMS, Håkon Alstad, IT-direktør, Lisbeth Viken, avdelingsdirektør dokumentnasjonsforvaltning.

**Referansegruppe/workshops**

Det er ønskelig å nedsette en referansegruppe(r) som kan vurdere behovet/brukervennlighet fra forsknings – og studiesiden, og administrativ side, som trekkes inn fra miljøer som behandler personopplysninger i betydelig omfang. Her er det viktig å inkludere brukerperspektivet, og hvordan rutiner/systemer vurderes å fungere i praksis. Dette for å sikre etterlevelsen. En leder fra instituttsiden (kontorsjef) bør med fordel inkluderes, samt en studentrepresentant og studentombudet.