Årsrapport for oppfølging av personvern og informasjonssikkerhet i forskningsprosjekter ved fakultet/senter X
Studieåret 20X – 20X

Hvem rapporterer vi fra og til?

**Overordnede mål**

# OsloMets forskningsvirksomhet skal være i overensstemmelse med gjeldende lover og retningslinjer for forskning, og skal skje i henhold til OsloMets mål for informasjonssikkerhet og personvern. Både **student- og forskningsprosjektene skal gjennomføres i henhold til gjeldende personvernregelverk, helseforskningsloven m.m.** Målene for personvern og informasjonssikkerhet er nedfelt i [Policy for informasjonssikkerhet og personvern.](https://ansatt.oslomet.no/policy-for-informasjonssikkerhet-og-personvern)

**Mål for oppfølging og kontroll**

**OsloMet skal ha et** [internkontrollsystem](https://ansatt.oslomet.no/retningslinje-for-behandling-av-personopplysninger#Form%C3%A5l) **(med en styrende, gjennomførende og kontrollerende del) som ivaretar ansvaret.**

[Internkontrollen for forskning utføres i Forskningsdatabasen og Personverntjenester (Sikt)](https://ansatt.oslomet.no/rutine-meldeplikt-nsd) **sitt meldingsarkiv.**

**Oversikt over utført internkontroll for det enkelte prosjekt er registrert i Forskningsdatabasen i fanen Internkontroll. Denne rapporten gir en oppsummering av internkontrollen som er utført i løpet av året. Målet med oppsummeringen er å ha oversikt over risiko og behov for forbedringer og tiltak.**

**Antall forsknings- og studentprosjekter som er kontrollert**

**Aktiviteten i løpet av 20X/20X.**

**Hvor mange prosjekter har man sjekket?**

* **Sjekk alle nye prosjekter som behandler sensitive personopplysninger**
* **Ta en stikk-kontroll av prosjekter som behandler alminnelige personopplysninger.**

**Tabell Fordeling av forsknings- og studentprosjekter på institutt.** *Skriv inn antall forsknings- og studentprosjekter som har blitt sjekket og antall av dem som inneholder sensitive personopplysninger osv.*

|  |  |  |
| --- | --- | --- |
|  | **I**nstitutt x | **I**nstitutt x |
|  | *Student* | *Forskning* | *Student* | *Forskning* |
| Antall som har blitt sjekket |  |   |  |   |
| Antall prosjekter som er aktive |  |  |  |  |
| Sensitive personopplysninger |  |  |  |  |
| Risikovurdering |  |  |  |  |
| DPIA |  |   |  |   |
| Endringsmeldinger |  |   |  |   |

**Sjekkliste: Sett opp en kolonne for hvert institutt**

***Svar i prosent i tabellen.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Institutt X** | **Institutt X** | **Institutt x** | **Institutt X** | **Institutt X** | **Resultat for fakultet/senter** |
| **Er samtykke innhentet?**  |  |  |  |  |  |  |
| **Er det gitt informasjon til de registrerte?**  |  |  |  |  |  |  |
| **Er REK -prosjekter registrert i Forskningsdatabasen?** |  |  |  |  |  |  |
| **Brukes godkjente elektroniske systemer for behandlingen.**  |  |  |  |  |  |  |
| **Er det gjort en risikovurdering?** |  |  |  |  |  |  |
| **Er nødvendige personvernavtaler signert (roller og ansvar avklart)?**  |  |  |  |  |  |  |
| **Blir prosjektet truffet av retningslinje for eksportkontroll?** |  |  |  |  |  |  |
| **Er krav i evt. tillatelser fulgt opp?** |  |  |  |  |  |  |
| **Har det forekommet noen avvik og er disse meldt ledelse og** sikkerhet@oslomet.no **?** |  |  |  |  |  |  |
| **Har det skjedd noen endringer i prosjekter, og er disse fulgt opp?** |  |  |  |  |  |  |
| **Er statushenvendelser og avvik registrert i Sikt sitt meldearkiv fulgt opp?** |  |  |  |  |  |  |
| **Slettes/anonymiseres data i henhold til Sikt og evt. REK sin vurdering?** |  |  |  |  |  |  |
| **Arkiveres data etter prosjektslutt i henhold til krav fra REK eller ekstern som finansierer prosjektet og i så fall hvor?** |  |  |  |  |  |  |

**På bakgrunn av de ovenfor nevnte funn skal du gi en litt mer utførlig beskrivelse av følgende punkter:**

**Behandlingens lovlighet**

**Det vanligste lovlige grunnlaget i forskning er «samtykke». Ellers er alternativet «i allmennhetens interesse. Uansett lovlig grunnlag skal det gis tilstrekkelig informasjon til de registrerte. *Beskriv funnene, f.eks. hvordan informasjonen normalt gis.***

**Sikkerhet ved behandlingen:**

***Beskriv funnene, f.eks. Hva bruker studentene av elektroniske løsninger, hva bruker forskere av elektroniske løsninger, er det behov for andre elektroniske løsninger, følges Lagringsguiden…., gjøres normalt risikovurderinger, kan du se noe av problemet hvis ikke.***

**Avtaler med samarbeidspartnere**

***Beskriv funnene, f.eks. Er riktig avtale inngått med samarbeidspartnere? Er det inngått avtaler med underleverandører? Overføres det personopplysninger til tredjeland, slik at det er nødvendig med et overføringsgrunnlag? Foreligger det et overføringsgrunnlag? Er det tatt avsjekk vedrørende eksportkontroll? Er det inngått avtale med transkriptører som ikke er student eller ansatt ved OsloMet?***

**Endringer i prosjektet**

***Beskriv funnene, f.eks. hvordan endringer i prosjektet følges opp.***

**Avvik/Statushenvendelser (NSD)**

***Beskriv funnene, f. eks. hvilke typer avvik er det mest av og gjenopprettes kontakten mellom Sikt og forsker/student.***

**Avslutning av prosjektet**

***Beskriv funnene, f.eks. slettes eller anonymiseres data normalt ved prosjektslutt i henhold til Sikt og REK sin vurdering? Har OsloMet kontroll over dataene? Hvor mye er veileder involvert i prosjektavslutningen? Ved arkivering av forskningsdata etter prosjektslutt, hvor arkiveres normalt dataene?***

**Avvik**

**Tabell over avvik.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dato** | **Avviket** | **Meldt** **sikkerhet@oslomet.no** | **Meldt Datatilsynet** | **Tiltak** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Oppsummering av aktiviteter i løpet av året**

***Beskriv hvilke aktiviteter som gjøres generelt i løpet av året og hva man har lagt vekt på i internkontrollen? Hvordan har internkontrollen blitt utført og hvor ofte?***

*Har personvernkontakt FoU/FoU-rådgiver hatt tilstrekkelig tid til å utføre internkontroll på vegne av instituttleder/instituttdirektør/senterleder? Er det gjennomført orienteringsmøter med instituttleder/instituttdirektør/senterleder? Hvis ikke hvorfor?*

**Erfaringer som er gjort og forslag til forbedringer, både tekniske tiltak og prosessforbedringer**

**‘Tiltak**

*Beskriv om det er behov for tiltak og hvilke, hvilke tiltak som bør prioriteres, samt om det er behov for hjelp utenfra eller lengre opp i systemet for å få gjennomført nødvendige tiltak (f.eks. når det gjelder kostnader til innføring av et bestemt system eller en annen form for involvering/hjelp?*

|  |  |
| --- | --- |
| **Tiltak planlagt for 20X-20X** | **Gjennomføring** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

*Personvernkontakten avdekker hvordan tilstanden er og instituttleder/instituttdirektør/dekan/senterleder beslutter hvilke tiltak som er nødvendige for å forbedre og å nå målene om å gjennomføre forsknings- og studentprosjekt i henhold til personvernregelverket.*

*Har tidligere planlagte tiltak blitt gjennomført? Beskriv effekten av gjennomførte tiltak.*

**Gjennomført opplæring/bekjentgjøring av rutiner**

1. Hvordan er bevissthet/kompetanse om personvern innenfor FoU på ditt fakultet/senter (evt. institutt) fra 1 til 10?
2. Har det skjedd en utvikling/forbedring av bevisstheten/kompetansen i løpet av året? I så fall, hva skyldes det?
3. Hvilke spørsmål har man veiledet på, og hva er det mest behov for opplæring i?

Dato: \_\_\_\_\_\_\_\_\_\_

­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Instituttleder/instituttdirektør/senterleder*  *Personvernkontakt*