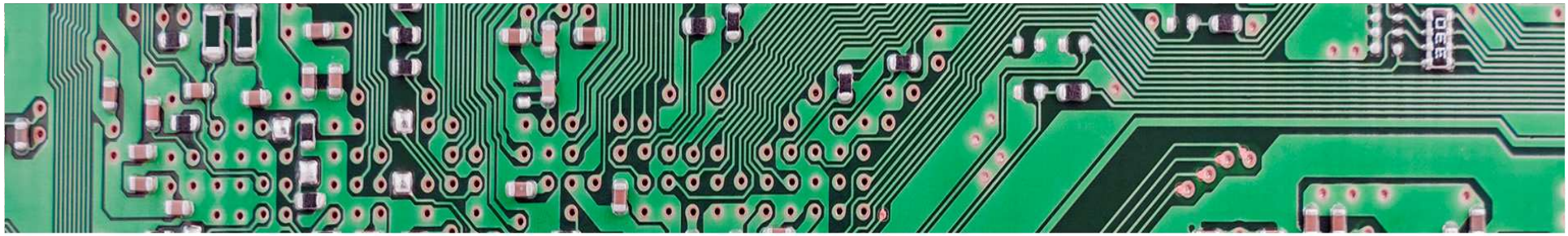

UiO : USIT

Innføring av nytt personvernregelverk ved UiO

PK-nettverket 25.04.2018

Asbjørn Tingulstad Hem – juridisk rådgiver USIT

Nytt regelverk

- EU har vedtatt ny personvernforordning
  - General Data Protection Regulation (GDPR)
- Trer i kraft 25. mai 2018
- Lovproposisjon fremlagt for Stortinget av Justisdepartementet
  - særlovgivning

Felles europeisk regelverk

- GDPR er et felles europeisk regelverk for personvern og skal styrke europeiske borgeres personvern.

- Global verden: Forordningen skal også styrke tilliten til digitale tjenester og samtidig gjøre det lettere å utveksle personopplysninger over landegrenser.

Personvern generelt – prinsippene GDPR art. 5

- Lovlighet, rettferdighet, åpenhet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet
- Ansvar

Hva er nytt?

- Konsesjonsplikten / tilråding fra REK/personvernombud bortfaller
  - blir erstattet av en personvernkonsekvensanalyse
- Økt dokumentasjonskrav
  - også for samtykke
- Sikkerhetsbrudd
- Straffen
- Oppmerksomheten

UiOs GDPR-prosjekt

- Mandat

  Prosjektet skal utrede konsekvensene av det nye regelverket og sikre at UiO følger ny lov ved å foreslå endringer i gjeldende rutiner og retningslinjer der det er nødvendig.

Prosjekt for innføring av nytt regelverk

- Organisert som et UiO-prosjekt under IT-direktøren
- Tverrfaglig sammensatt prosjektgruppe
  - Avdeling for fagstøtte
  - Avdeling for administrativ støtte
  - USIT
  - Personvernombudet
  - Det medisinske fakultet
  - Det samfunnsvitenskapelige fakultet
- Stort omfang av interessenter
  - Følger allerede etablerte nettverk og møtefora
- Beslutninger og oppfølging skal følge linjen

Hvor er vi/hva må jobbes med?

- Har allerede rutiner som i stor grad er dekkende
  - Må gjennomgås
    - Gjøres sammen med fagavdelingene
  - Må gjøres bedre kjent
- Krav om overordnet protokoll/oversikt over personopplysninger vi sitter på
  - Hva har vi i dag?
  - En systemoversikt- og kartlegging
  - Kartlegging av rettslig grunnlag

- **Personvernkonsekvensvurdering**
  - Foreta personvernkonsekvensvurdering av tre store systemer som behandler personopplysninger på UiO
  - Utarbeide retningslinjer for når og hvordan slike analyser skal gjennomføres

- **Personvernombud**
  - Gjennomgå UiOs ordning for personvernombud og sikre at den er i tråd med nye krav
  - Foreslå eventuelle nødvendige endringer

Involvering fagavdelingene

Prosjektet skal sammen med de relevante fagavdelingene utarbeide planer for å sikre at nye retningslinjer blir fulgt opp når det nye personvernregelverket er innført.

Dette innebærer bl.a. at det skal lages planer for utarbeidelse av opplæringsopplegg for universitetets ansatte og studenter.

Opplæring

- Prosjektet utarbeider planer for opplæring sammen med fagavdelingene
- Tar sikte på at opplæring innføres i allerede etablerte kurs og opprettes nye opplæringsarenaer i løpet av høsten 2018
- Ønskelig at personvernansvarlige på enhetene får en sentral rolle

Hva treffer personal?

?

(Michael Rosskothen / Shutterstock)

MYE videreføres

- Allerede gode etablerte rutiner - mye på plass allerede

https://www.uio.no/for-ansatte/arbeidsstotte/personvern/leder-saksbehandler/index.html

- Som nevnt er oppmerksomheten ny - kjenn dagens rutiner

LSIS

- «Ledelsessystem for informasjonssikkerhet»
- Revisjon og utvidelse av IT-sikkerhetshåndboka
- Basert på ISO27001 og veiledere fra UNINETT
- Godkjent av universitetsledelsen
- Tre deler - 14 kapitler
  - Styrende del
  - Gjennomførende del
  - Kontrollerende del

Innholdet i vår LSIS

- Bør leses av tjenesteeiere, IT-folk og ledere
- Stort fokus på informasjonssikkerhet - hvordan beskytte dataene våre
- Mye fokus på kontroll og ettersyn
- Plassering av ansvar for tjenester
- Oppgave- og rollebeskrivelser
- ROS-analyser sammen med teknisk grunnsikring

- https://www.uio.no/tjenester/it/sikkerhet/lsis/

Personvern generelt – prinsippene GDPR art. 5

- Lovlighet, rettferdighet, åpenhet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet
- Ansvar

Si ifra!

UNIVERSITAS

Millionbot: På grunn av slurvete omgang med data, kan UiO måtte belage seg på flere millioner i bot. Bildet viser Eilert Sundts hus tidligere i vinter. Illustrasjonsfoto: Erlend Dalhaug Daae

UiO risikerer millionbot

Datatilsynet mistenker at UiOs håndtering av sensitiv persondata har vært for slepphendt. I en lignende sak fikk helseforetakene bøter på til sammen 7,2 millioner kroner.

Aftenposten A-magasinet Osloby Sport Meninger Bli abonnent Meny

NTNU-ansatt trykket «svar alle» ved et uhell – delte konfidensielle opplysninger

Hele kullet kunne lese om en hvorvidt medstudent var skikket til psykologiyrket.

Universitets-institutt drev klinikk i 42 år – ble stengt på dagen

I 42 år har Institutt for psykologi drevet et klinikktilbud som del av undervisningen. Tirsdag stengte universitetsdirektøren klinikken på dagen. Hun hevder det kan være begått lovbrudd med driften.

Hva mer betyr GDPR for de ansatte?

- Mer fokus på personvern
- Personvernerklæring for ansatte
- Opplæring
  - etablerte opplæringsarenaer og e-læringskurs
- Noen endringer i arbeidshverdagen
- Forbedret håndtering av brukerdata

http://www.uio.no/for-ansatte/arbeidsstotte/prosjekter/gdpr/

gdpr-prosjekt@uio.no