UiO : USIT

Innføring av ny personvernforordning (GDPR) på universitetet

Styringsdokument

Styringsgruppemøte 16. april 2018

Innhold

Sak 1: Godkjenning av referat

- Godkjenning av referat fra 19.3.18

Sak 2: Lovproposisjon fremlagt

- Konsesjon bortfaller
- Unntak fra registrertes rettigheter for enkelte forskningsprosjekter
- Helselovgivningen
- Ytrings- og informasjonsfrihet
- Personvernombud
- Kameraovervåkning/adgangskontroll
- Innsyn i e-postkasse mv.

UiO : USIT

Sak 3

Organisering av personvernombudsrollen ved UiO etter GDPR

Delleveranse GDPR-prosjektet

Morten Opsal

Enhet for Intern Revisjon

16.04.18

Momenter

- Ny forordning for hele EU/EØS fra 25. mai 2018
  - krav om personvernombud i offentlig virksomhet
  - Ny personopplysningslov i Norge, 2 hoveddeler: 1) forordningen, 2) supplerende bestemmelser
- UiO har frivillig hatt 2 personvernombud
  - Forskning/utdanning: NSD – stykkfinansiert, kostet 2,5 millNOK i 2017
  - Adm.behandlinger: Morten Opsal, 20 %, via EIRs budsjett (PVO/A)
  - Samarbeid PVO/A og utøvende behandlingsansvarlig
    - Møter om aktuelle problemstillinger
    - Team for å utføre stedlige kontroller
    - Svært gunstig, kompetansehevende og kvalitetssikrende.
- REK
  - etisk forhåndsgodkjenning har hittil gitt behandlingsgrunnlag, opphører fra ny personopplysningslov
- Største endringer
  - Melde- og konsesjonsplikt til DT/PVO bortfaller, institusjonen må sikre etterlevelse av loven selv – og PVO har ikke noe ansvar i det!
  - Vurdering av personvernkonsekvenser

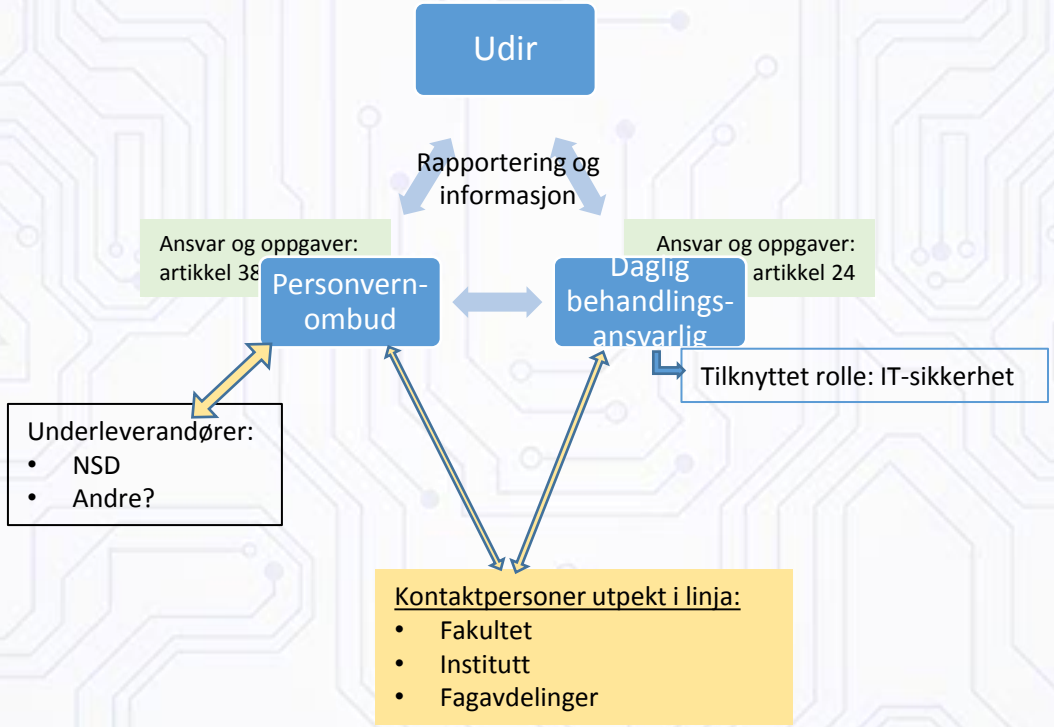
Momenter (2)

- 3 artikler i forordningen angir rollen til personvernombudet
  - 37:
    - må ha faglige kvalifikasjoner/dybde om personvernlovgivning
  - 38:
    - uavhengig rolle, rapportere direkte til øverste ledelse
    - involveres i alle spørsmål om vern av pers.oppl., på riktig måte og til rett til
  - 39, 1: minst ha følgende oppgaver
    a) Informere og gi råd til institusjonen om de forpliktelser som de har ihht forordningen
    b) Kontrollere overholdelse av forordningen og institusjonens personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring
    c) På anmodning, gi råd om vurdering av personvernkonsekvenser
    d) Samarbeide med tilsynsmyndigheten
    e) Fungere som kontaktpunkt for tilsynsmyndighetene ved spørsmål om behandlingen, herunder forhåndsdrøftinger
  - 39, 2: ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlings art, omfang, formål og sammenhengen den utføre i .

Kriterier for plassering

- Ut fra hensiktsmessighet
  - Faglig fellesskap for å kunne diskutere problemstillinger og få innsikt
    - Personvernrelaterte forhold
    - Informasjonssikkerhet, IT-sikkerhetsforståelse
    - Internkontroll/risikostyring virksomhetsnivå
    - UiOs kjerneaktiviteter (forskning, utdanning, formidling + adm.forhold)
    - Prosedyrer (systemeierskap, avvikssystemer)
- Involvering av PVO i org. ut fra plassering
  - Organisatorisk: Liten grad av betydning.
    - Rutiner for involvering for å favne hele org. PVO må selv opptre aktivt.
  - Fysisk: Noen grad av betydning
    - Bredere innsikt

Modell for rapportering og samhandling



Forslag

- Tilsette ett personvernombud i 100 % stilling med helhetlig ansvar for å dekke området, jf artiklene 38 og 39
  - Juridisk master, og dybdekompetanse personvernlovgivning
  - Kan være flere som bidrar for å dekke rollen, men en ansvarlig
  - Innkjøp av underleverandør NSD, og evt andre, avtalebasert – ny avtale!!
  - 100 % stilling som ombud fjerner interessekonflikter
- Organisatorisk plassering av rollen
  - I vurdering, men jeg synes EL eller EHMSB peker seg ut.
  - Hos USIT blir det for nære behandlermiljøet og avvikshåndteringsregimet.
- Utarbeide instruks/mandat for nytt personvernombud
  - Artikkel 39 beskriver minimumsoppgavene
  - Andre faktorer:
    - Rapporteringsstruktur og –frekvens
    - Samhandlingsrelasjoner
      - NSD, behandlingsansvarlig, IT-sikkerhet, fakulteter og institutter, fagavdelinger, stedlige kontroller, rolleavklaring
    - Andre oppgaver kan avtales/innplasseres

Sak 4: Informasjonsskriv til universitetsstyret

- Ikke egen sak, men del av universitetsdirektørens informasjon til styret
- Gjennomgang av informasjonsskrivet

Sak 5: Status for prosjektarbeidet

- Framdrift
  - Stor arbeidskapasitet i prosjektet
  - Uventede utfordringer
  - Noen forsinkelser

- Ressursbruk
  - Juristene og IT-sikkerhetssjef bruker mer enn antatt
  - Øvrige prosjektdeltakere holder prosent avsatt

- Synlige og mulige risiko
  - Håndtering av rettslige grunnlag
    - Bortfall av konsesjon
    - Nye behandlinger (forskning og administrativt)

Sak 5: Status for prosjektarbeidet

- Besøk hos fakultetene, UB og museene er i gang og avtalt møtetidspunkt
- Prosesser med fagavdelingene
- SUM, STK og ISS er tatt inn i kommunikasjonsplanen
- Behandleransvaret for Uniforum, Apollon, UiOs AS og randsoneenheter
- Forslag til organisering av personvernombudsrollen fremlegges universitetsdirektøren 20. mars

Sak 5: Status systemkartlegging SKAIT

- 31 leverte svar
- Mangler kun ett system
- Ingen alvorlige avvik eller regelbrudd avdekket pt.
- Basert på innmeldte svar så er disse de første kandidatene til personvernkonekvensanalyse:
  - SAP, FS, ePhorte, Urkund, OA
  - Trolig noen flere når vi går gjennom det i detalj

Sysetmkartlegging USIT

- 44 leverte svar
- Ikke avdekket alvorlige avvik så langt
- En del mangler på gjennomført ROS-analyse
  - fokus har vært på ROS ved innføring av nye systemer og ved endring
- Mangler kartlegging av en del små-tjenester / systemer

Noen betraktninger så langt (SKAIT)

- 6 av 31 har ikke vurdert hvilket grunnlag vi har for å kunne behandle personopplysninger i systemet (samtykke, lovhjemmel)
  - Finnes trolig i data fra ROSA-prosjektet
- 5 av 30 systemer behandler sensitive personopplysninger
- 90% har foretatt ROS-analyse
- 60% av systemene lagrer personopplysninger i mer enn 5 år etter at formålet med behandlingen er avsluttet
  - Ca.10 systemer begrunner lagringstiden utfra en lovhjemmel
- 26 av 31 systemer har rutiner for tilgangskontroll

Databehandleravtaler / innebygget personvern

- Forslag til brev sendes ut til systemeierne innen utgangen av uke 16. Ber leverandører redegjøre for hvordan de følger de nye reglene.
  - Systemeierne har ansvar for å sende ut brev til databehandlere.
- Oppdatert mal for databehandleravtale klar før 25.mai
- Møte med innkjøp fredag 20. april
  - Tar inn krav om innebygget personvern i nye innkjøp

Oppgaver fremover

- Starte personvernkonsekvensanalyse så fort mal er klar – for systemene til SKAIT / USIT
- Starte kartlegging for forskning / utdanning
  - Starte med to enheter
  - Evt. også kartlegge de “opplagte” systemene der de finnes.
- Avdekke hvor det mangler rutiner for sletting / retting / innsyn

Sak 6: Nye prosjektmedarbeidere og ressurser

- Behov for mer ressurser på forskningssiden i prosjektet
  - Johannes Elgvin, seksjonsleder ved SV-fakultet
  - Ilze Gehe, rådgiver ved ISV/SV
- Deler av midlene fra SKAIT er brukt for å styrke ressursene for juristene
  - Jurist Trine Smedbold ansatt i seks måneders engasjement i IT-direktørens stab

Sak 7: Neste møte i styringsgruppen

- Forslag: uke 19 eller 20

Sak 8: Eventuelt