Implementering av det nye personvernregelverket ved UiB

Læringsdag MatNat 31.01.2019

Spørsmål?

- Hvordan har UiB fulgt opp kravene i det nye personvernregelverket i datasystemene vi bruker
  - Hva bør lokale enheter og saksbehandlere være klar over?
- Forklar kravene spesielt for EU prosjekt
- Kva bør vi tenke på når vi lagra studieadministrative opplysningar i nettsky ift til GDPR?
- Er det enkelte opplysningar vi framleis bør kun lagre på server pga at nettsky er mindre sikkert?

Bakgrunn

- EUs forordning om behandling av personopplysninger – personvernforordningen / General Data Protection Regulation (GDPR). Gjelder i hele EU/EØS-området.
- Trådte kraft i EU 25. mai 2018 – *ingen overgangsbestemmelser!*
- Gjennomføres i norsk rett ved innføring av ny personopplysningslov, som inkorporerer forordningen i sin helhet.
- Ny personopplysningslov vedtatt av Stortinget 22. mai 2018
- Vedtaket innebærer også endringer i mange andre lover, bl.a. helseforskningsloven, helseregisterloven, m.v.
- Ny personopplysningslov trådte i kraft Norge: **20. juli 2018**

Personvernforordningen + personopplysningsloven

= personvernregelverket

GDPR: 'en evolusjon, ikke en revolusjon'

- Mye av innholdet i GDPR er videreføring av gjeldende rett.
- Meldeplikt og konsesjonsplikt oppheves - systematiske tiltak skal erstatter forhåndsgodkjennelse fra Datatilsynet.
- Styrkede rettigheter for de registrerte
- Forsterket plikt til internkontroll / økt tilsynsaktivitet
- Plikt til å ha **personvernombud** for offentlige myndigheter og visse private behandlingsansvarlige
- vesentlig høyere bøtenivå!

Merk …

- Forordningens regler vil som hovedregel måtte anvendes slik de står
- Dels **pålegger** og dels **åpner** forordningen for nasjonale regler på en rekke områder
  - Gjelder særlig for behandling av personopplysninger i offentlig sektor og i forskningsvirksomhet
- Der det foreslås nasjonale regler, tas det i hovedsak sikte på å videreføre gjeldende rett

Hva er personopplysninger?

Informasjon som både direkte og indirekte kan knyttes til en fysisk person, f.eks.

- Navn
- Fødselsnummer
- adresse
- Bilde, video, lydopptak
- E-postadresse, IP-adresse
- Bilnummer

Hva er særlige kategorier personopplysninger? (’Sensitive’)

- Helseforhold
- Seksuelle forhold
- Politiske, religiøse oppfatninger, livssyn
- Fagforeningstilhørighet
- Etnisk eller rasemessig bakgrunn
- Genetiske og biometrisk opplysninger
- Opplysninger om straffbare forhold

Generelle prinsipper for behandling av personopplysninger – GDPR art. 5:

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

Hva betyr dette for UiB?

- Krav til innebygd personvern i IKT-løsninger. UiB må ta hensyn til personvern i alle utviklingsfaser av et system eller løsning
- Generell plikt til å vurdere risiko og personvernkonsekvenser i alle sammenhenger hvor personopplysninger behandles, og til å involvere personvernombudet ved behov (ref. at melde- og konsesjonsplikten oppheves)
- Personopplysninger skal kun behandles for det formål de er innsamlet for. Nye formål må ikke være uforenlig med det opprinnelige.

Hva har vi gjort ved UiB?

- Forberedende internrevisjon (GAP-analyse) V2017
- GDPR-prosjekt (prosjektleder Janecke Veim)
- Utviklet registreringsverktøy for oversikt over alle behandlingsaktiviteter (tk.app.uib.no/gdpr) for administrative formål
- kartlegging og registrering av behandlingsaktiviteter (protokoll) – formål, behandlingsgrunnlag, lagring, IT-sikkerhet mv
- Oppnevning av personvernombud
- Samarbeid i UH-sektoren (BOTT og Uninett)
- Utarbeidet **personvernerklæring** i klart og forståelig språk

Hvordan best å informere om GDPR?

- Pop-ups?
- Brev fra rektor til alle ansatte?
- Eller kanskje som dette?
- Eller i UiBs personvernerklæring - som her

Hva må dere gjøre?

- Alle enheter må kartlegge sin **egen behandling** av personopplysninger f.eks.
  - Lister med navn som brukes til utsendelse av nyhetsbrev, oversikter over kontaktpersoner og databaser må kartlegges og registreres
  - Saksbehandlingsrutiner ved egen enhet
  - Studentadministrasjon, utveksling med andre institusjoner, personalsaker?
  - Annet?
  - Labsystemer som ikke driftes av IT?

Mer om protokollen, GDPR artikkel 30: tk.app.uib.no/gdpr

- Navn på og kontaktopplysninger til den behandlingsansvarlige
- Formålene med behandlingen
- kategoriene av registrerte
- Kategoriene av personopplysninger
- Databehandler, overføring til 3. land
- Sletterutiner
- Beskrivelse av tekniske og organisatoriske tiltak

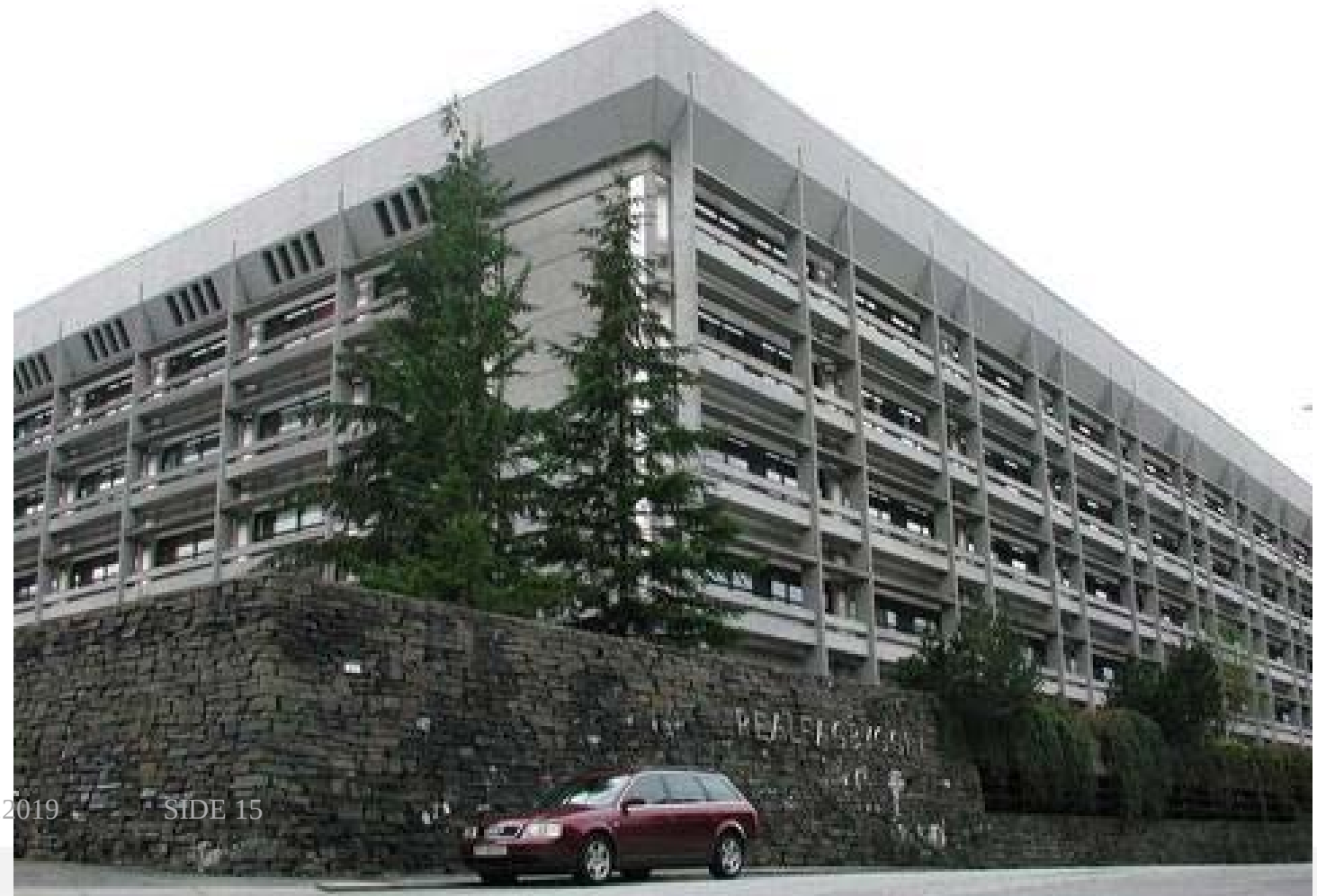
Hvordan registrere en behandling?

- Alle behandlingsaktiviteter skal registreres i GDPR-oversikten: tk.app.uib.no/gdpr

- Oversikten er knyttet til UiBs tjenestekatalog for systemer, men også behandlingsaktiviteter utenfor UiBs IT-systemer skal inn i oversikten
- For å få tilgang eller hjelp til registrering ta kontakt med Gisle Aas (IT-avd) eller Janecke Veim

Og vinneren er ....

(bilde lånt fra UiBs billedarkiv)



10 steg på veien til GDPR-etterlevelse

1)	Dedikerte og tilstrekkelige ressurser
2)	Kartlegg alle systemer som behandler personopplysninger
3)	Avklare om behandlingsansvarlig eller databehandler
4)	Dokumenter behandling av personopplysninger i systemene
5)	Ha kontroll på slettefrister og rutiner
6)	Ha kontroll på overføring av data
7)	Hvordan oppfylle de registrertes rettigheter?
8)	Ved samtykke – er det opt-in løsning?
9)	Ivareta kravet til informasjonssikkerhet
10)	Rutiner for å oppdage og rapportere avvik

Personvern og forskning

- Nye nettsider: https://www.uib.no/personvern
- Alle som behandler **særlige kategorier** personopplysninger i forskning får rådføringsplikt med personvernombud (unntak: alminnelige personopplysninger, helseforskning, hvis allerede utført personvernkonsekvensvurdering/DPIA)
- Prosjektleder har ansvar for å dokumentere at det er søkt råd hos personvernombud
- Unntatt fra særskilt rådføringsplikt – prosjekter som involverer alminnelige personopplysninger, helseforskningsprosjekter
- Skal alltid gjøres en vurdering om det bør gjennomføres en personvernkonsekvensvurdering, også der behandlingen ikke omfatter sensitive personopplysninger

EU prosjekter

Ethics and data protection

UiBs ansvar som forskningsansvarlig

- Må ha oversikt over alle forskningsprosjekter som behandler personopplysninger, inkl helseforskning
- Forsterket ansvar for systematisk oppfølgning av forskningsprosjekter (internkontroll)
- RETTE – prosjekt for å utvikle system for oversikt, risiko og etterlevelse av forskningsprosjekter utvikles v/UiB
- Alle forskningsprosjekter skal etter hvert registreres i RETTE – med integrasjon mot CRIStin og NSD
- Skal utarbeides kommunikasjons- og implementeringsplan for innføring av RETTE

Personvernombud for forskning-

- Premiss: En institusjon kan kun ha ett personvernombud etter regelverket.
- Kan kjøpe inn personvernrådgivningstjenester etter tjenesteavtale.
- Rådføringsplikt med personvernombud for forskningsprosjekter.
- UiB-ledet arbeidsgruppe for UHR – utredet ulike løsninger for personverntjenester i forskning
- Revisjon og videreføring av avtalen med NSD for forskning
- Sannsynligvis en løsning der NSD fortsetter sin virksomhet ved siden av den ordningen som reguleres av forordningen, slik at behandlingsansvarlige innhenter råd fra NSD.

Forventninger til fakultetene:

Administrativt

- Oppfølgning av arbeidsgiveransvaret går stort sett som i dag

Særlig oppmerksomhet på oppgaver henger sammen med forskningsansvaret, herunder oppfølgning av:

- veileders ansvar for studentprosjekter
- Utenlandske stipendiater

Internkontroll i forskningsprosjekter:

- ***RETTE*** (system for å sikre oversikt, etterlevelse og kontroll med forskningsprosjekter) skal implementeres
- Opplæring og informasjon til forskere / forskningsadm.
- Når innhente råd fra ekstern personvernrådgiver – rutiner og samarbeid med NSD

Helseforskning

Helseforskning ser ut til å kunne gå som før, men merk:

- Behandling av personopplysningene må være forankret i forordningen, ikke i 'annen lov' som i dag (helseforskningsloven)
- Fremdeles krav om etisk vurdering for helseforskningsprosjekter etter helseforskningsloven,
- Unntak fra den særskilte rådføringsplikten for helseforskningsprosjekter - forskningsansvarlig kan legge REK sin vurdering av personvernmessige forhold til grunn
- Krav om at behandlingsansvarlig skal ha oversikt – helseforskningsprosjekter må inn i den samlede forskningsprosjektoversikten

UNIVERSITETET I BERGEN

Miljøfyrtårn®