GDPR- hva betyr dette for NTNU

- NTNU behandler personopplysninger i stort omfang.
- GDPR stiller skjerpede krav til behandling av personopplysninger og styrker de registrertes rettigheter.
- NTNU skal ivareta ansattes, studenters og øvrige registrertes interesser og personsikkerhet gjennom lovlig, god og sikker behandling av personopplysninger.

Hva har skjedd på NTNU

- personvernombud på plass – Thomas Helgesen
- nytt styringssystem for informasjonssikkerhet - behandling av personopplysninger inngår som en del av informasjonssikkerhet
- kartlagt behandlingsaktiviteter som inneholder personopplysninger ved NTNU
- rutine for innsyn (digitalt)
- rutine for sletting
- retningslinje for behandling av personopplysninger
- rutine for samtykke
- Retningslinjer for personvernkonsekvensvurderinger (DPIA)
- maler for databehandleavtale
- felles/overordnet personvernerklæring for NTNU
- avvikshåndteringsrutiner og rutiner for å gjennomføre risikovurderinger

Men gjenstår å operasjonalisere og tydeliggjøre og finne de gode praksisene.

Videre arbeid på NTNU

Behandlingsaktiviteter og systemoversikt

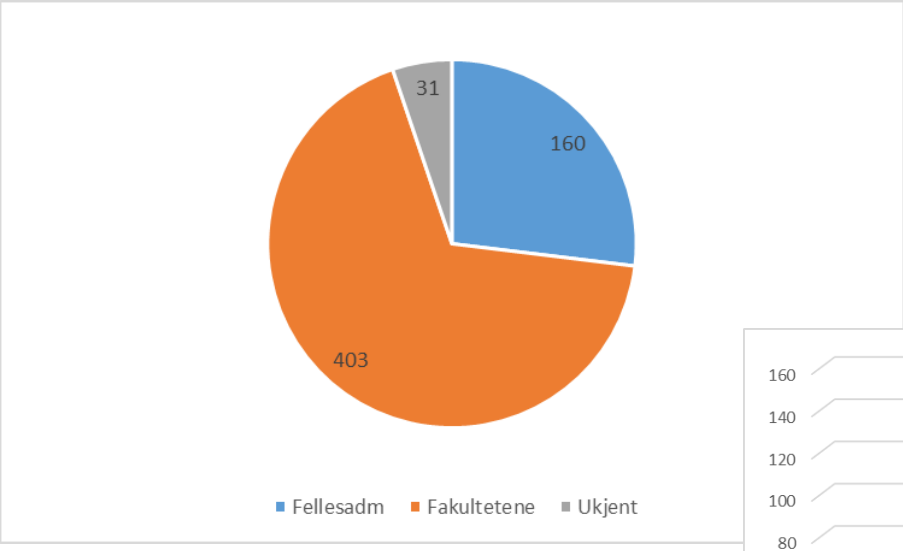
- ca 600 stk behandlingsaktiviteter – se neste foil
- ca 650 systemer
- prioriterte systemer/behandlinger gjennomgås nå (juridisk- og IT – kompetanse)
- enhetsledere og systemeiere må kobles på
  - sørge for forsvarlige systemer og behandlinger
  - enhetsledere i FA e fellesnevnere slik at vi får
    - enhetlige gjennomgående arbeidsprosesser på NTNU

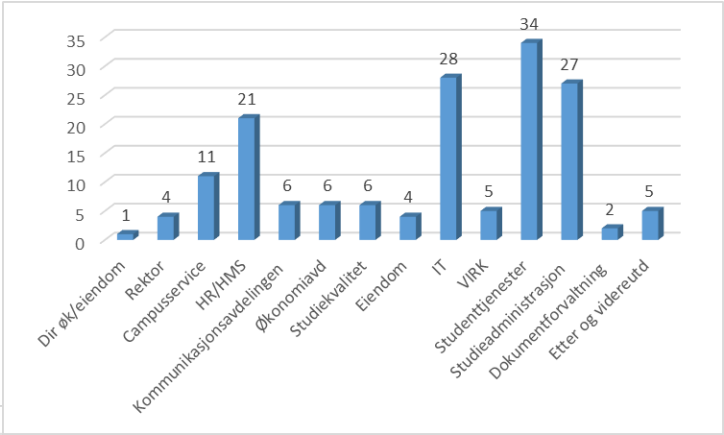
Kartlegging av behandlingsaktiviteter – helseforskning

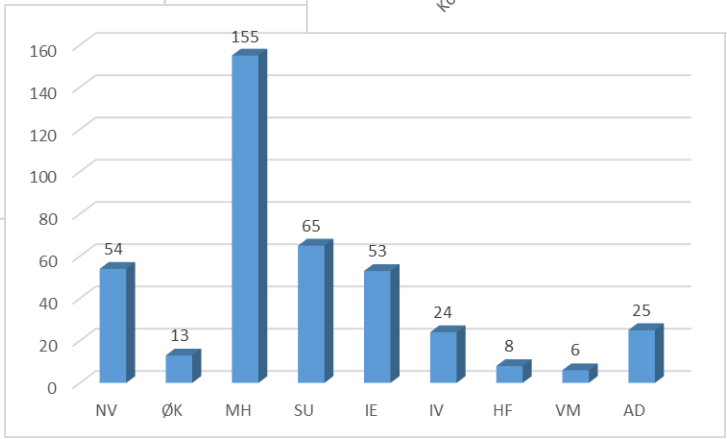
- er sendt ut med frist 14.12.18
- MH og SU har deltatt i utformingen av kartleggingsverktøyet

Etablert en ressursgruppe med personvernkontakter fra fakultet og enheter i FA deltar

Behandlingsaktiviteter







Databehandleravtaler

- Inngås mellom behandlingsansvarlig og databehandler
- Når NTNU som behandlingsansvarlig setter ut deler av behandlingen til en annen virksomhet, må det inngås databehandleravtaler.
- En databehandler er en ekstern leverandør som behandler personopplysninger på vegne av NTNU.
- NTNUs mal for databehandleravtaler skal som hovedregel benyttes

Avvikshåndtering

Vi har en plikt til å varsle DT ved brudd på personopplysningssikkerheten

- hvis risiko for den registrertes rettigheter eller friheter

- uten ugrunnet opphold og senest 72 timer etter at de ble kjent med bruddet

Vi må underrette den registrerte ved høy risiko

Opplæring

- operasjonalisering av forordningen og de nye retningslinjene ved NTNU, dvs avklare hvilken betydning har regelverket for NTNU.

- Har ikke kommet så langt som ønskelig

- Det er behov for opplæring på tre nivåer
  - Basis innføring og opplæring i gdpr/informasjonssikkerhet (standard informasjon som finnes i markedet for offentlig sektor)
  - Hvordan benytte eksisterende systemer ved NTNU for sikker håndtering av informasjon som er underlagt personvern. Opplæring i hvordan vi kan ta i bruk de løsninger som allerede finnes – (finnes allerede etablerte kurs på NTNU og ute i sektoren som kan benyttes)
  - Fagspesifikk opplæring/praksiskunnskap knyttet til ulike virksomhetsprosesser (må utvikles)

  Det skal etableres rollestyrt opplæring dvs sette sammen pakker for de ulike rollene (ledere, veiledere, studenter, ansatte, osv)

Risikovurdering/avvikshåndtering

- gode rutiner og holdninger må etableres

- Sikker forsendelse – trygg og sikkert (arbeidsavtaler). Få dokumentene ut til både eksterne og interne. NTNU ønsker raskere tilsettingsprosesser - post til utlandet tar TID – hva skal vi gjøre - praktisk
- Epost – forsendelse – intern og ekstern og arkivering av e-post – ikke arkivverdig post.
- E-post - korrespondanse med studenter
- Usikkerhet ift sikkerhet av sending av intern epost - gir ulik informasjon ! Bidrar til forvirring
- Tilrettelegging for studenter – helse opplysninger - hvordan jobber vi sikkert med det.
- Ulike portaler – inn og ut av studiet - opplastingsfunksjoner - koordinering av systemer - eks opptak på særskilt grunnlag - og videre til tilrettelegging - ingen kobling - integrerte systemer som snakker sammen
- Sporing i bygg av både ansatte og utstyr – infrastruktur
- Sikker skanning av post som skal arkiveres
- Lagring – arkiv
- Deling av dokumenter
- Håndtering, lagring og behandling av konfliktsaker, varslingssaker osv
- Risikovurdering – rutine som ligger på Innsida er for omfattende – vi må ha en rutine som ivaretar helheten ved NTNU – dvs både enkle risikovurderinger og opp til ROS-analyser
- Hvordan innhente samtykke – rutine – enhetlig måte å gjøre det på
- SAMTYKKE
- Opplæring IT-avdelingen – Innebygd personvern
- Koordinering IT og innkjøp - innebygd personvern

- Studieveiledning – kommunikasjonskanaler
- Digitale skjema – sikker måte
- Ekskusjoner - påmeldingslister – feltkort - administrasjon – sikker løsning
- Opponenter - kopi av pass - sikker løsning
- Vurdering av utenlandske vitnemål – går i dag på e-post
- Veiledning og oppfølging internasjonale studenter generelt
- Avvik – hva er et avvik og hvordan melde og følge opp

- Medarbeidersamtaler – arkivering – HR har utarbeidet rutine
- Arbeidsflate for råd og utvalg - hvordan dele info sikkert til ansettelsesutvalg og tilsettingsråd, styrer, ledergruppe, osv

- Rutiner for behandling av filer og e-post ved brukers dødsfall
- strømme/videofilme forelesninger
- Innsyn i egen personalmappe
- Streame en video av et seminar/workshop på UB sine Facebook-side
- Definere hva er hva av dokumenter ved NTNU - eksempler på klassifisering
- Dokumentmaler og klassifisering av informasjon
- Se også kommentarer på Innsida ang opplæring ifm sikkerhetsmåneden

Opplæring

- Jobbes med
  - Info til studenter
  - Innebygd personvern i systemer (utvikling og anskaffelse)
  - Aktivitet; Sikker forsendelse
    - E-post
    - Skjema
    - Skanning
  - Forskning
    - Personopplysninger
    - Helseopplysninger
    - Lagring
  - Behandlingsaktivitet; Strømming, videofilming, foto
  - Lederopplæring
  - Sikkerhetsmåneden
  - Lagring og klassifisering

Kryptering av informasjon i e-post

Hva skal krypteres;

- avhenger av hva du skal sende – dokument/informasjon må klassifiseres. Se; https://innsida.ntnu.no/wiki/-/wiki/Norsk/Informasjonsklassifisering+-+informasjonssikkerhet

Eksempel;

- karakterutskrifter er å regne som "opplysninger om personlige forhold" så er disse taushetsbelagte og må klassifiseres som fortrolig

Seksjon for Digital Sikkerhet har skrevet en veiledning på hvordan du kan kryptere informasjon for sending av e-post, se; https://innsida.ntnu.no/wiki/-/wiki/Norsk/Sikker+e-post

1. Selve e-posten kan krypteres, men dette krever at både du og mottaker har installert digitale sertifikater.
2. Kryptering av Office-dokumenter: Alle Office-dokumenter har innebygget en krypteringsfunksjon som kan enkelt kan brukes ved å sette et sterkt passord.
3. Kryptering vha 7-zip. Her kan du lage deg et arkiv med filer og zippe de ned med passordbeskyttelse.

Alle disse tre tilnærmingene til kryptering benytter sterke krypteringsalgoritmer og anses som sikre nok til å sende fortrolig og strengt fortrolig informasjon. Det viktige her er at du setter et sterkt passord og sender dette via en annen kanal enn e-post. For eks. via SMS.

Sensitive opplysninger

Sensitive personopplysninger (kalt særlige kategorier i loven)(datatilsynet)

I loven er det definert en rekke kategorier av opplysninger som det skal mer til å kunne behandle enn andre opplysninger (artikkel 9 og 10):

1. opplysninger om rasemessig eller etnisk opprinnelse
2. opplysninger om politisk oppfatning
3. opplysninger om religion
4. opplysninger om filosofisk overbevisning
5. opplysninger om fagforeningsmedlemskap
6. genetiske opplysninger
7. biometriske opplysninger med det formål å entydig identifisere noen
8. helseopplysninger
9. opplysninger om seksuelle forhold
10. opplysninger om seksuell legning
11. opplysninger om straffedommer
12. opplysninger om lovovertredelser

Spørsmål

- Hvem er ansvarlig for event brudd mot GPDR? Individuell saksbehandler eller NTNU enhet

- Hvordan sikrer vi at våre søknadsskjema følger reglene ?