UiO : Universitetet i Oslo

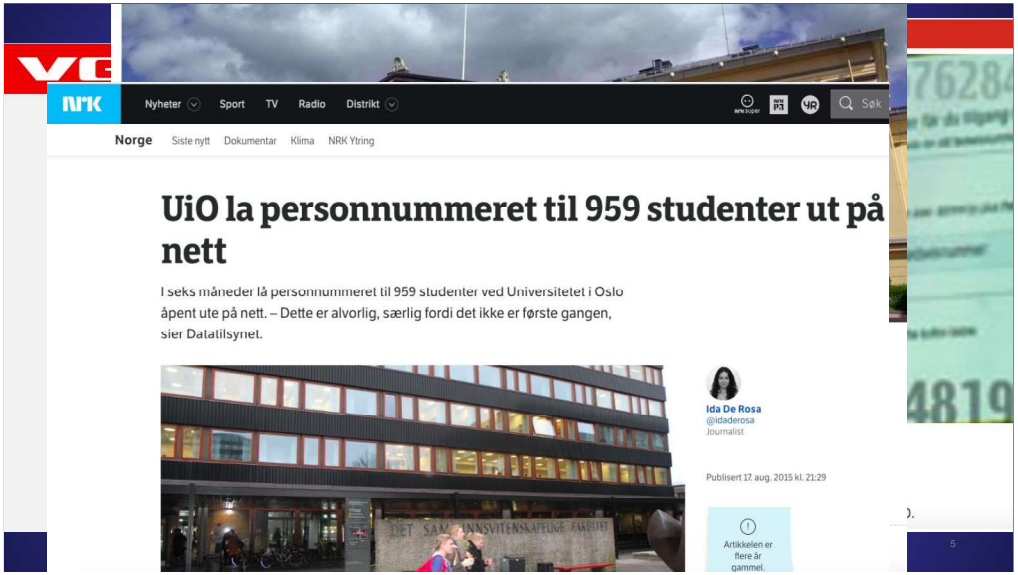
# Privacy by design

UiO : Universitetet i Oslo

# Programutvikling med innebygd personvern

UiO : Universitetet i Oslo

# Slik ble vi GDPR-ready






UiO : Universitetet i Oslo

## Nettskjema i finalen

5. mars vart pris for beste innebygde personvern delt ut av Datatilsynet. Blant dei tre finalistane var Nettskjema.

Finalistane på rekke og rad. Nummer to frå venstre er USIT sin Dagfinn Bergsager. Foto: Veronica Jarnskjold Buer/Datatilsynet



UiO : Universitet

NorSIS
Norsk senter for informasjonssikring

Hjem - Finalistene til Fidusprisen 2018

## Finalistene til Fidusprisen 2018

Lytt til teksten  Skriv ut  Del på facebook

Fidusprisen er en pris som deles ut av NorSIS til en virksomhet som ha
informasjonssikkerhet, og som innehar høy tillit i samfunnet.

Fidusprisen er en pris som deles ut av NorSIS til en virksomhet som har utmerket seg m
Formålet er å skjerpe bevisstheten hos privatpersoner og i virksomheter om behovet for
samarbeid mellom NorSIS og YouGov. Navnet er hentet fra latin og betyr "tillit"/"tiltro".

Årets finalister er Sbanken, Brønnøysundregistrene og Universitetet i Oslo. Disse har kor
spørreundersøkelse der forbrukere har blitt bedt om å rangere virksomheter og bransje
personopplysninger. Vinneren blir bestemt av en jury, bestående av representanter fra [



Denne USIT-gjengen utvikler apper til forskere: Fra venstre Paul Philip Mitchell, Mikael Olausson, Ida Krüger, Dagfinn Bergsager, Martine Eklund, Pål Fugelli, Kien Vu og Espen Adrian Jones. Foto: Gunhild M. Haugnes/UiO Bruk bildet.

Titan.uio.no
...ny kunnskap hver dag!

## De utvikler apper som gjør forskningen bedre

**Målgruppen er forskere som har behov for å samle inn sensitive persondata. Dette kan være første steg på veien mot at hver og en kan overvåke sin egen helse på en app – på en sikker måte.**

av Gunhild M. Haugnes – 30. april, 2018

– Vårt app-miljø er unikt i Skandinavia, kanskje i også i verden, mener prosjektlederne Dagfinn Bergsager og Pål Fugelli fra USIT (Universitetets senter for informasjonsteknologi).

Som den eneste aktøren er USIT-gruppen sertifisert av TSD (Tjenester for Sensitive Data til å kunne utvikle apper hvor svært sensitive persondata er involvert – som blant annet helseopplysninger.

Denne USIT-gjengen utvikler apper til forskere: Fra venstre Paul Philip Mitchell, Mikael Olausson, Ida Krüger, Dagfinn Bergsager, Martine Eklund, Pål Fugelli, Kien Vu og Espen Adrian Jones. (Foto: Gunhild M. Haugnes/UiO)

UTVIKLER APPER SOM GJØR FORSKNINGEN BEDRE

## Tar hele utviklingen. En ferdig app koster 200.000 kroner: – Vårt miljø er unikt i Skandinavia, kanskje i hele verden

GUNHILD M . HAUGNES - TITAN.UIO.NO | UTVIKLING | PUBLISERT: 3. MAI 2018 - 05:00

digi.no
IT- bransjens nettavis





versionen IT-NYHEDER BLOGS DEBAT IT-JOB SEKTIONER MERE

## Lowcost: En færdig app til forskere koster her 150.000 kroner

**Portræt: norsk udviklergruppe udvikler apps, som hjælper med at gøre forskning bedre.**

Gunhild M. Haugness / titan.iou.no / digi.no Torsdag, 3. maj 2018 - 11:20 1

FØLG

»Vores app-miljø er unikt i Skandinavien, måske også i verden,« mener projektlederne Dagfinn Bergsager og Pål Fugelli fra det norske Universitetets senter for informasjonsteknologi (USIT).

Som den eneste aktør er USIT-gruppen certificeret af norske Tjenester for Sensitive Data (TSD) t at kunne udvikle apps, hvor meget sensitive persondata er involveret – blandt andet sundhedsoplysninger.

TSD giver forskere en platform, som opfylder lovens strenge krav til behandling og lagring af sensitive forskningsdata.



NRK Nyheter Sport TV Radio Distrikt

Sørlandet TV Radio Tips Feature

## App skal hjelpe mot morgenkvalme

Gravide som sliter med kvalme kan snart få hjelp av en app. Den skulle gjerne de nybakte mødrene Charlotte og Marthe Moland Rui hatt tilgang på i sine svangerskap.

Heidi
Journa

Publis





**Hvordan klarer vi å utvikle mobilapper som samler inn sensitive personopplysninger?**

**-fordi vi har innebygd personvern!**

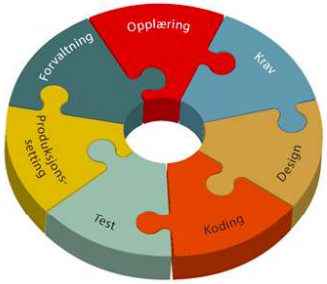
**…ikke omvendt**

## Programutvikling med innebygd personvern

***Veileder fra Datatilsynet med internasjonal oppmerksomhet***

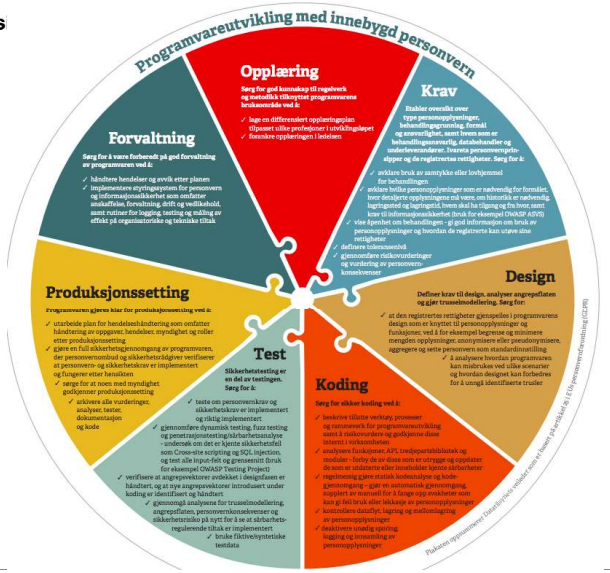
Oppsummering: Programmer seriøst!

- Bruk en metode
- Regler for koding
- Verktøyvalg
- Gjennomtenkt testing
- Gjør nødvendige sikkerhetstiltak












## Prioriteringer for all utvikling

1. **Sikkerhet og personvern**
2. **Bruksopplevelse for den som skal levere data**
   → **Universell utforming**
3. **Funksjonalitet for den som samler inn data**

-Vi skal alltid være best på sikkerhet og personvern!

-og fungere på alt utstyr for alle personer

-og være enkel og bruke for datainnsamler





## Nettskjema

- Datainnsamling på nett
- Nasjonal tjeneste
- Mottar 2000 – 50 000 svar per dag
- Mobilapper og webapper kan levere data via Nettskjema
- UiO utvikler og drifter
- Kan samle inn sensitive personopplysninger

## Tjenester for sensitive data

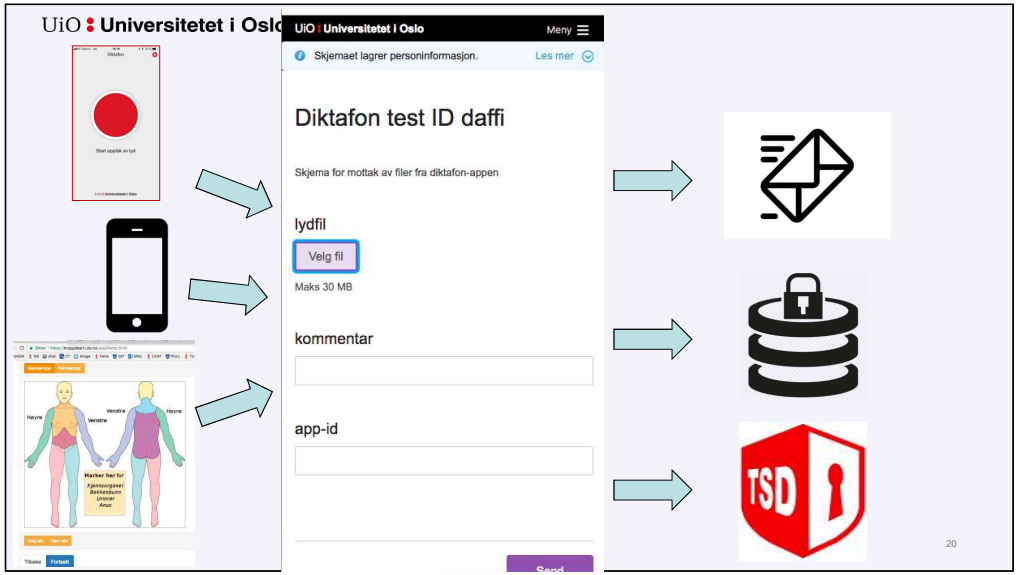
- Sikker, skalerbar forskningsplattform for UiO og andre offentlige forskningsinstitusjoner.
- Alle prosjekter får sin egen sikre virtuelle server
- Begrensa mulighet for eksport
- Behandling av data skjer på serveren inne i TSD
  - Statistikk og lagring
  - Tungregning
  - Lyd -og videoredigering..+++



*TSD – Services for Sensitive Data*

*An infrastructure for high security data*










## Mobilapper i forskning

- Har utviklet omlag 20 apper for forskningsprosjekter
- Nettskjema /TSD er backend for alle apper
- Alle prosjekter får ROS med fokus på hva som er unikt med dette prosjektet
  - Baserer ROS på andre ROS

UiO : Universitetet i Oslo

# (Rask) Gjennomgang av GDPR



Art. 25 GDPR

## Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. [1] The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. [2] That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [3] In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.



LOVDATA | Søk etter lover, forskrifter, dommer og stortingsvedtak | Logg inn

Rettskilder

- Lover
- Stortingsvedtak
- Sentrale forskrifter
- Lokale forskrifter
- Norsk i utvidend
- Norges traktater
- Dommer
- Statens personalhåndbok
- Oversatte lover / Translated Acts

Lov om behandling av pers... | Innholdsfortegnelse | Lovens forskrifter

**Artikkel 25.** ***Innebygd personvern og personvern som standardinnstilling***

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.

2. Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.

3. En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.

LOVDATA | Søk etter lover, forskrifter, dommer og stortingsvedtak | Logg inn

Mer

- RSS-feed
- Lenker
- European Legislation Identifier (BETA)
- Eksamen

Lov om behandling av personopplysninger (perso... | Innholdsfortegnelse | Lovens forskrifter

**Artikkel 5.** ***Prinsipper for behandling av personopplysninger***

1. Personopplysninger skal
   a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),
   b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenlig med de opprinnelige formålene («formålsbegrensning»),
   c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),
   d) være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),
   e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),
   f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»).

2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar»).

## «Lovlighet, rettferdighet og gjennomsiktighet»
(lawfulness, fairness and transparency)

- Kan bli (og blir) sett i kortene på alle ledd i dataflyten
- Åpen kildekode og sikkerhetsdokumentasjon
- Jevnlig dialog med Datatilsynet, Personvernombud som OUSPVO, REK, NSD
- All kode gjennomgås av 2 personer
- ROS-analyser for alle prosjekter og systemer som bruker vår løsning





## Bug bounty hunt i Nettskjema

- www.uio.no/bounty

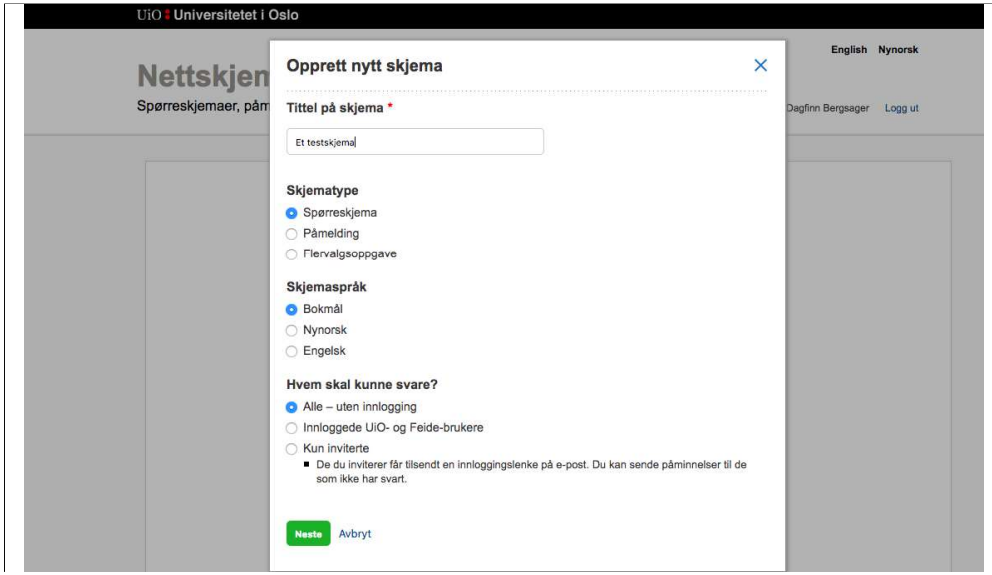


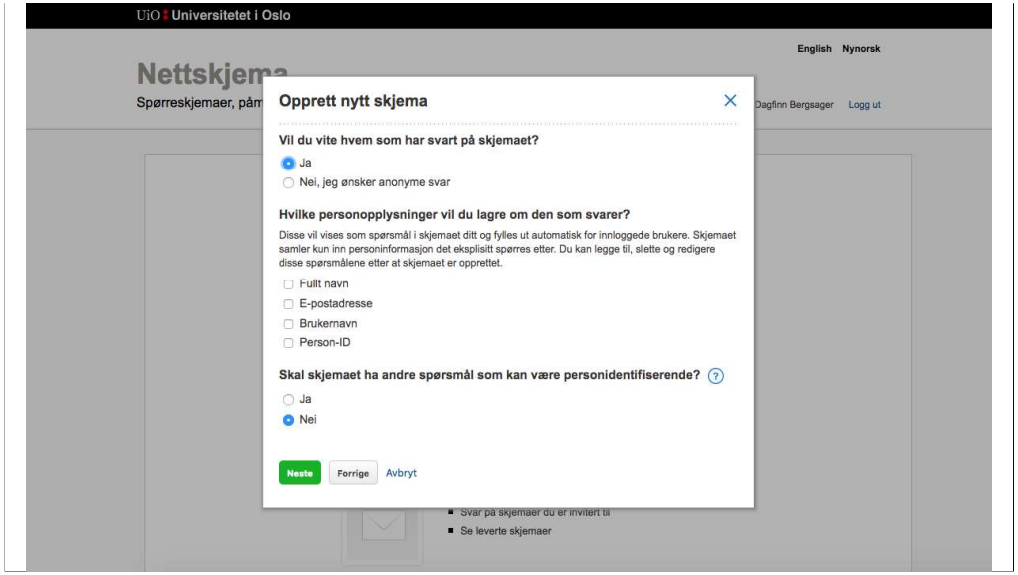


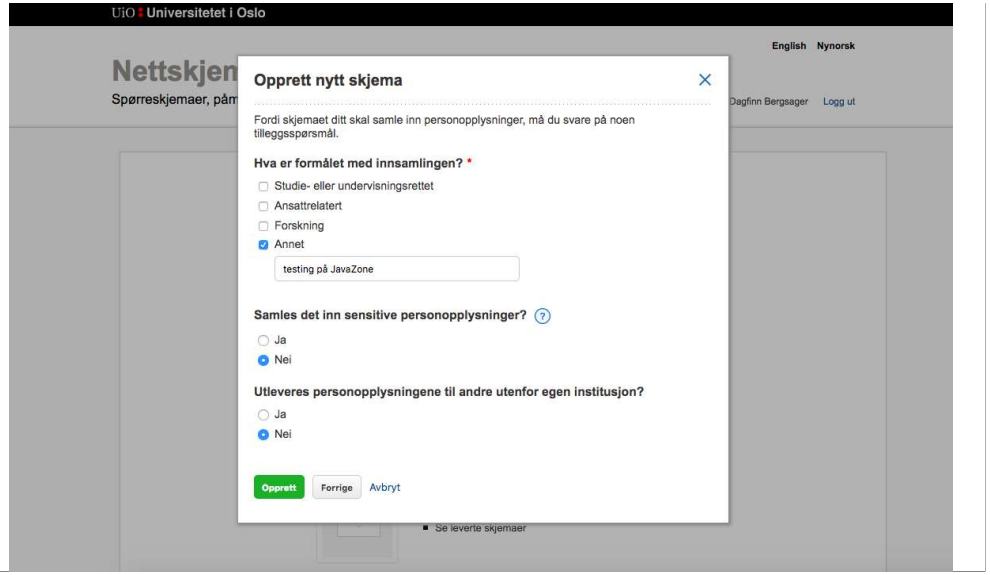
## «Formålsbegrensning»
(Purpose limitation)

- Forskere er obs på dette; vil tilrettelegger for dem
  - Alle med rette godkjenninger (REK/NSD) får egen sikker server
  - Lett å hente inn men vanskelig å få data ut av serveren
  - Data slettes når godkjenning utgår
- Overvåker at andre som samler inn holder seg til formålet










## «Riktighet»
(Accuracy)

- Kun lenker til personkatalog –ikke import av kontaktinfo
- Grunndata om personer hentes fra SAP eller FS
- Flere nivåer av IDporten (BankID)
  - Dersom det er ekstra viktig å være sikker på hvem som svarer
- Løsning for digitalt signerte sensitive dokumenter
- Tydelig for bruker hvilke data som lagres





## «Lagringsbegrensning»
(Storage limitation)

- Nøye gjennomgang av hva som lagres på telefonen
- Vi merker skjema som samler inn persondata
  - Avansert algoritme fjerner persondata automatisk når vi vurderer innsamlingen som irrelevant
- Forskningsprosjekter må sette sluttdato for server i TSD og plan for sletting av data

## «Integritet og fortrolighet»
(Integrity and confidentiality)

- (Vanvitting) streng tilgangstyring til TSD
  - Eksportrettigheter revideres jevnlig
- Kun forsker har tilgang i TSD
  - Ikke IT-drift…
- Eks.: Påbegynte forskningsprosjekter får ikke endre skjema
  - Unngå juks
  - Dataintegritet
- Kun UiOs Apple /Google –konto legger ut apper





## «Ansvar»
(Accountability)

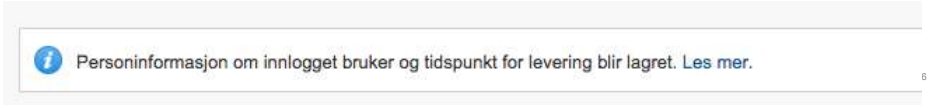
- Jevnlig varsling til de som samler inn data om de har skjema som bør ryddes /slettes
- Egne strenge krav til hva vi krever om vi skal ta et oppdrag
- Rutiner for avvikshåndtering – god erfaring!
- Hjelper forskere med å ROS for alle prosjekter
  - All data samles og lagres i samme løsning
  - Baserer ROS på eksisterende ROS
- Krever NSD/REK –godkjenning for alle prosjekter





## «Dataminimering»

- Markerer alle skjema som samler inn personinformasjon
- Fjerner automatisk persondata som vi vurderer som lite relevante
- Varsler bruker om hvilke personopplysninger som blir lagret








## Logging og scanning

- Logger 3 mnd
  - Gjelder ikke kliniske data
  - Gjelder ikke TSD
- Egne verktøy for å se trender
- Skanner jevnlig kode etter topp10-OWASP
- Skanner BitBucket og Jira etter hemmeligheter

## Hva gjør vi med Testdata?

- Vi *måtte* ha skarpe data i testmiljø fordi vi var så spesielle…
  - Umulig å fjerne alle spor uansett..
- Løsning
  - Kjører nesten all testing på tom database
  - Lager data vi trenger i testingen
  - Vasker bort personopplysninger fra data vi gjenbruker



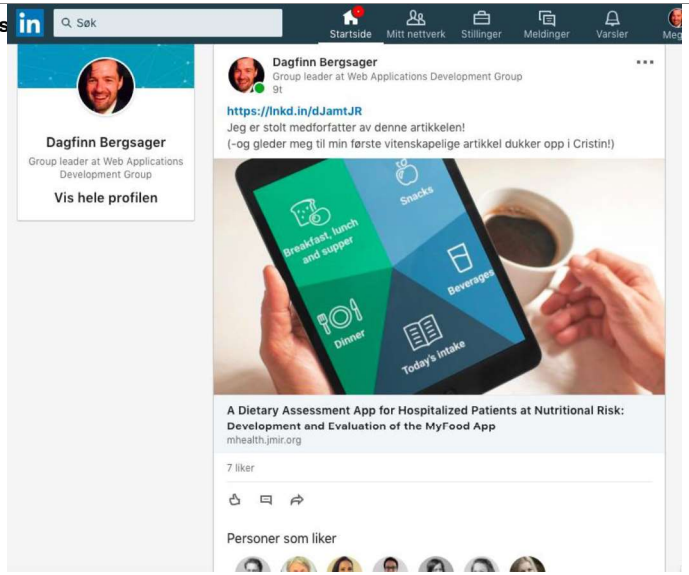


**Det viktigste er at alle i teamet forstår at innebygd personvern og innebygd informasjonsikkerhet er noe alle er ansvarlig for**

**-det svakeste punktet…**

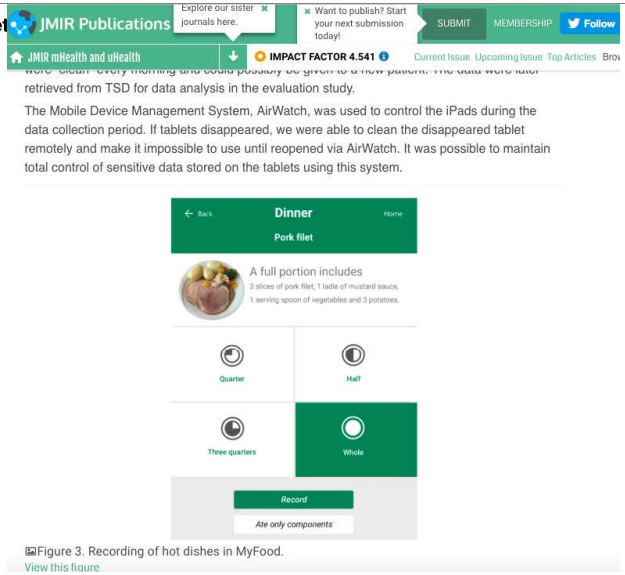










# Demo…