UiO : Universitetet i Oslo

Vi er GDPR-ready!

Dagfinn Bergsager
Leder for webutvikling og mobilapputvikling
USIT/UiO

linkedin.com/in/bergsager

Dagfinn Bergsager

- Leder utviklerteam på 12
- Lager løsninger for forskning og annen datainnsamling via web og apper
- Ansvarlig for verktøyvalg på UiO
- Deltager i prosjekt for ny veileder fra datatilsynet

UiO og USIT

- 27 000 studenter
- 6 613 årsverk ansatte og 7,8 mrd i omsetning
- Rangert som nr 62 i verden

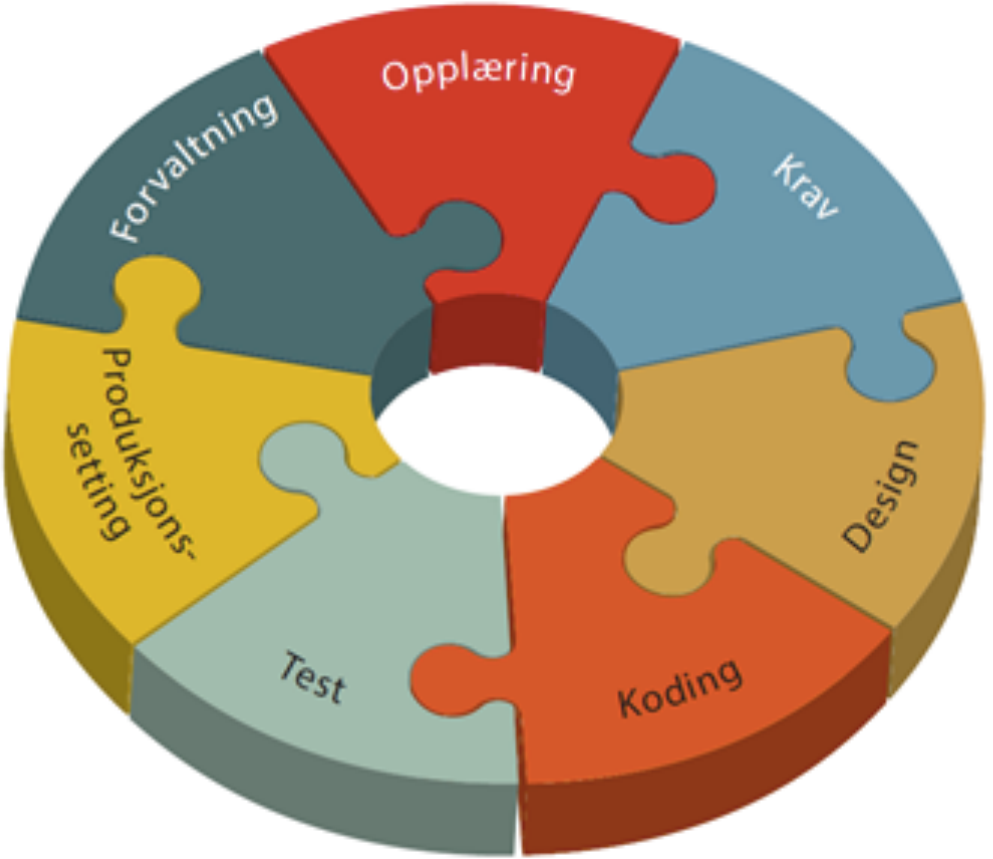
- USIT har ca 240 ansatte
- Drifter og utvikler sentrale løsninger for UH-Norge

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

-jo, vi koder med og tenker innebygd personvern!


Programvareutvikling med innebygd personvern
Opplæring
Sørg for god kunnskap til regelverk og metodikk tilknyttet programvarens bruksområde ved å:
✓ lage en differensiert opplæringsplan tilpasset ulike profesjoner i utviklingsløpet
✓ forankre opplæringen i ledelsen
Krav
Etabler oversikt over type personopplysninger, behandlingsgrunnlag, formål og ansvarlighet, samt hvem som er behandlingsansvarlig, databehandler og underleverandører. Ivareta personvernprinsipper og de registrertes rettigheter. Sørg for å:
✓ avklare bruk av samtykke eller lovhjemmel for behandlingen
✓ avklare hvilke personopplysninger som er nødvendig for formålet, hvor detaljerte opplysningene må være, om historikk er nødvendig, lagringssted og lagringstid, hvem skal ha tilgang og fra hvor, samt krav til informasjonssikkerhet (bruk for eksempel OWASP ASVS)
✓ vise åpenhet om behandlingen - gi god informasjon om bruk av personopplysninger og hvordan de registrerte kan utøve sine rettigheter
✓ definere toleransenivå
✓ gjennomføre risikovurderinger og vurdering av personvernkonsekvenser
Design
Definer krav til design, analyser angrepsflaten og gjør trusselmodellering. Sørg for:
✓ at den registrertes rettigheter gjenspeiles i programvarens design som er knyttet til personopplysninger og funksjoner, ved å for eksempel begrense og minimere mengden opplysninger, anonymisere eller pseudonymisere, aggregere og sette personvern som standardinnstilling
✓ å analysere hvordan programvaren kan misbrukes ved ulike scenarier og hvordan designet kan forbedres for å unngå identifiserte trusler
Koding
Sørg for sikker koding ved å:
✓ beskrive tillatte verktøy, prosesser og rammeverk for programvareutvikling samt å risikovurdere og godkjenne disse internt i virksomheten
✓ analysere funksjoner, API, tredjepartsbibliotek og moduler - forby de av disse som er utrygge og oppdater de som er utdaterte eller inneholder kjente sårbarheter
✓ regelmessig gjøre statisk kodeanalyse og kodegjennomgang – gjør en automatisk gjennomgang, supplert av manuell for å fange opp svakheter som kan gi feil bruk eller lekkasje av personopplysninger
✓ kontrollere dataflyt, lagring og mellomlagring av personopplysninger
✓ deaktivere unødig sporing, logging og innsamling av personopplysninger
Test
Sikkerhetstesting er en del av testingen. Sørg for å:
✓ teste om personvernkrav og sikkerhetskrav er implementert og riktig implementert
✓ gjennomføre dynamisk testing, fuzz testing og penetrasjonstesting/sårbarhetsanalyse - undersøk om det er kjente sikkerhetsfeil som Cross-site scripting og SQL injection, og test alle input-felt og grensesnitt (bruk for eksempel OWASP Testing Project)
✓ verifisere at angrepsvektorer avdekket i designfasen er håndtert, og at nye angrepsvektorer introdusert under koding er identifisert og håndtert
✓ gjennomgå analysene for trusselmodellering, angrepsflaten, personvernkonsekvenser og sikkerhetsrisiko på nytt for å se at sårbarhetsregulerende tiltak er implementert
✓ bruke fiktive/syntetiske testdata
Produksjonssetting
Programvaren gjøres klar for produksjonssetting ved å:
✓ utarbeide plan for hendelseshåndtering som omfatter håndtering av oppgaver, hendelser, myndighet og roller etter produksjonssetting
✓ gjøre en full sikkerhetsgjennomgang av programvaren, der personvernombud og sikkerhetsrådgiver verifiserer at personvern- og sikkerhetskrav er implementert og fungerer etter hensikten
✓ sørge for at noen med myndighet godkjenner produksjonssetting
✓ arkivere alle vurderinger, analyser, tester, dokumentasjon og kode
Forvaltning
Sørg for å være forberedt på god forvaltning av programvaren ved å:
✓ håndtere hendelser og avvik etter planen
✓ implementere styringssystem for personvern og informasjonssikkerhet som omfatter anskaffelse, forvaltning, drift og vedlikehold, samt rutiner for logging, testing og måling av effekt på organisatoriske og tekniske tiltak
Plakaten oppsummerer Datatilsynets veileder som er basert på artikkel 25 i EUs personvernforordning (GDPR)

Opplæring



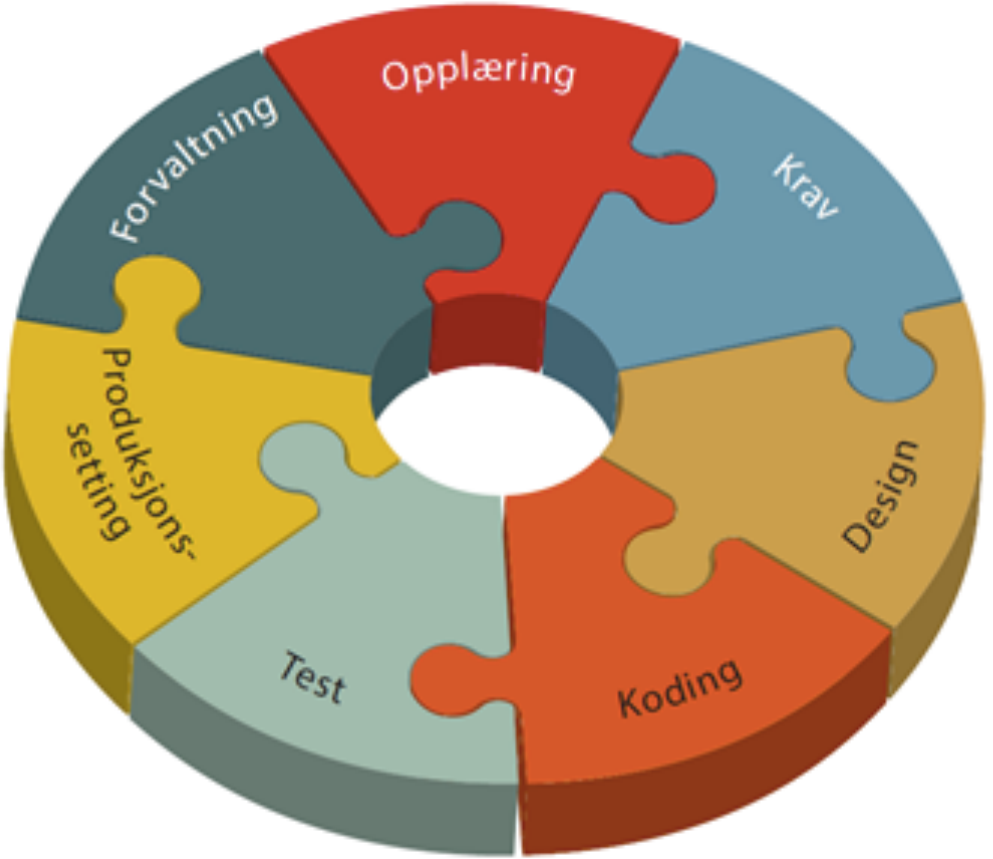
Illustrasjon hentet fra www.datatilsynet.no

Opplæring

- Før: gjennomgang med sikkerhet og jus en gang i året
- Nå: alle må ha et forhold til sikkerhet og jus

- Utviklerforum med jevnlig fokus på personvern og sikkerhet
- Sjekklister for utvikling av nye applikasjoner
- I gang med ”obligatoriske” kurs for alle utviklere og driftere høsten 2017/våren 2018

Krav



Illustrasjon hentet fra www.datatilsynet.no

Prioriteringer for all utvikling

1. **Sikkerhet og personvern**
2. **Bruksopplevelse for den som skal levere data**
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

Åpenhet

- Åpen kildekode
- Vilkår for bruk
- Personvernerklæring
- Vi forteller om sikkerhetstiltak og arkitektur
- Åpne ROS-analyser som kan brukes som dokumentasjon for andre prosjekter
- Tett dialog med Datatilsynet og personvernombud på OUS
- REK og NSD kjenner godt til våre løsninger

Eksempel på ROS

Nye utfordringer med mobilapper

- Mobilappen må lagre noe data
  - Når du leverte data sist
  - ID på hvem som har levert svaret
- At du har installert appen kan kobles til at du har en diagnose
- Dersom appen mister nett, kan det være behov for å legge data i kø
- Data på mobiler blir ofte sikkerhetskopiert til Apple/Google

MittBlikk

View More by This Develope

By Universitetet i Oslo

This app is only available on the App Store for iOS devices.

This app is designed for both iPhone and iPad

Free

Category: Lifestyle
Updated: 20 June 2017
Version: 1.0.2
Size: 20.5 MB

Description

Dette er en mobilapp for innsamling av data til et forskningsprosjekt ved Universitetet i Oslo. For å bruke appen må ha fått utdelt en studieID av forsker.

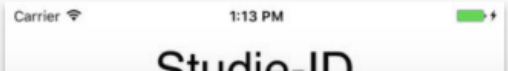
Universitetet i Oslo Web Site ▸ MittBlikk Support ▸

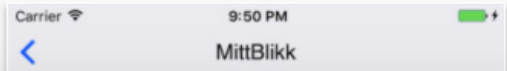
What's New in Version 1.0.2

Bugfiks og mindre designjusteringer

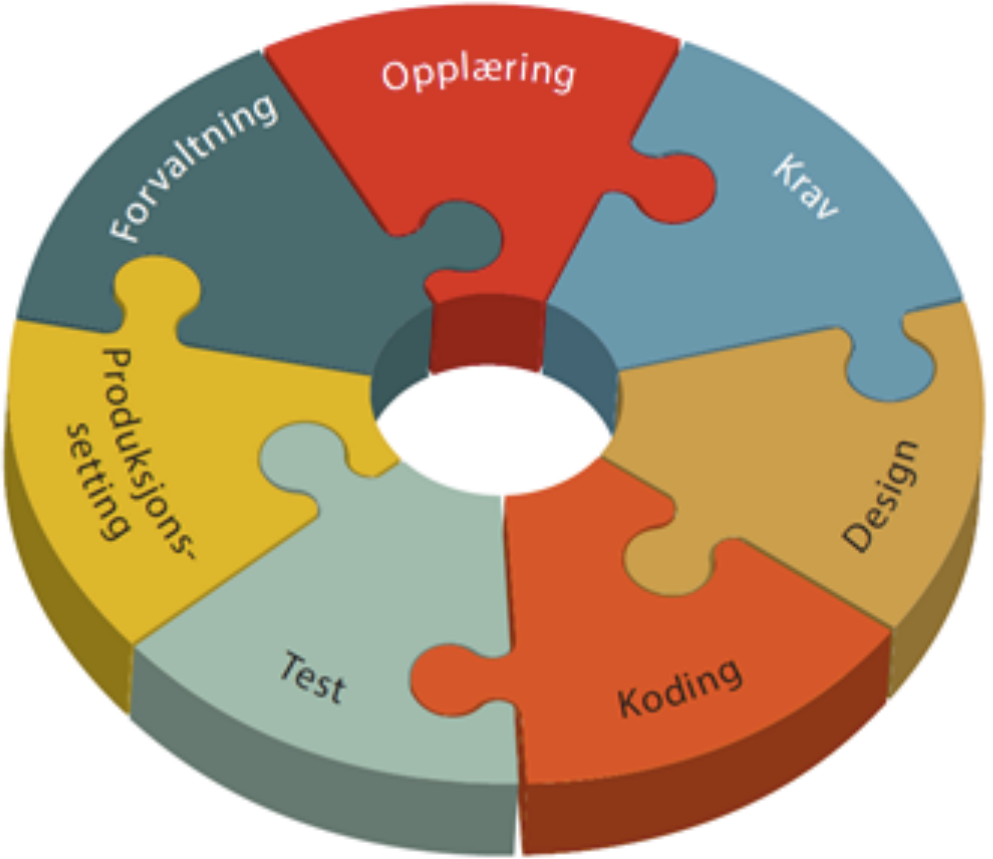
Screenshots

iPhone | iPad





Design



Illustrasjon hentet fra www.datatilsynet.no

Design

Vi lager moderne mobilapper og legger det oppå eksisterende infrastruktur for forskning med Nettskjema og TSD.

(slik som Vipps ligger oppå UNIX)

Tjenester for sensitive data

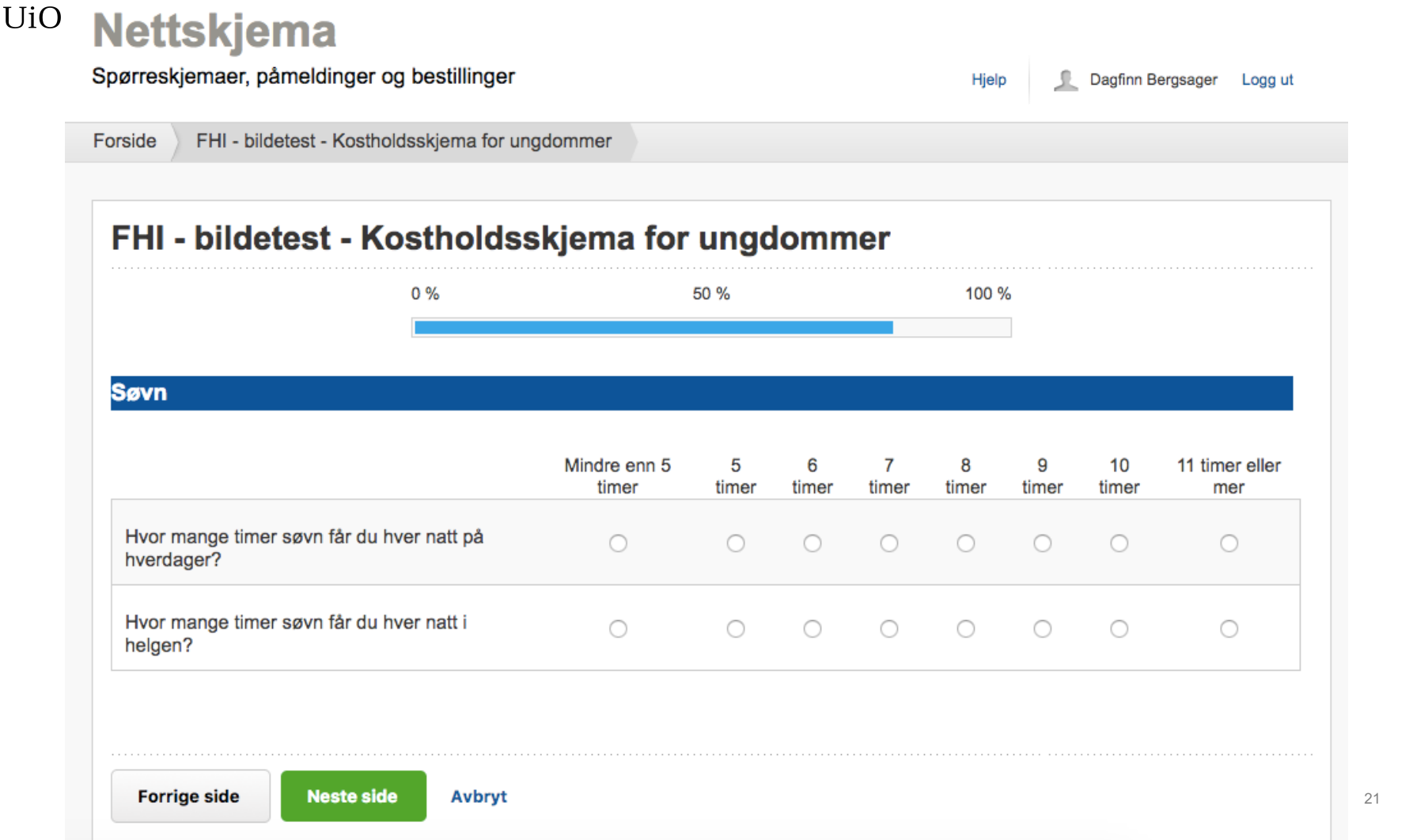
- Sikker forskningsplattform for UiO og andre offentlige forskningsinstitusjoner.
- Alle prosjekter får sin egen sikre server
  - Logger inn remote på windows-server
  - En server per godkjenning (REK/NSD)
- Egen brukerdatabase med 2 faktor innlogging
- Begrensa mulighet for eksport av data

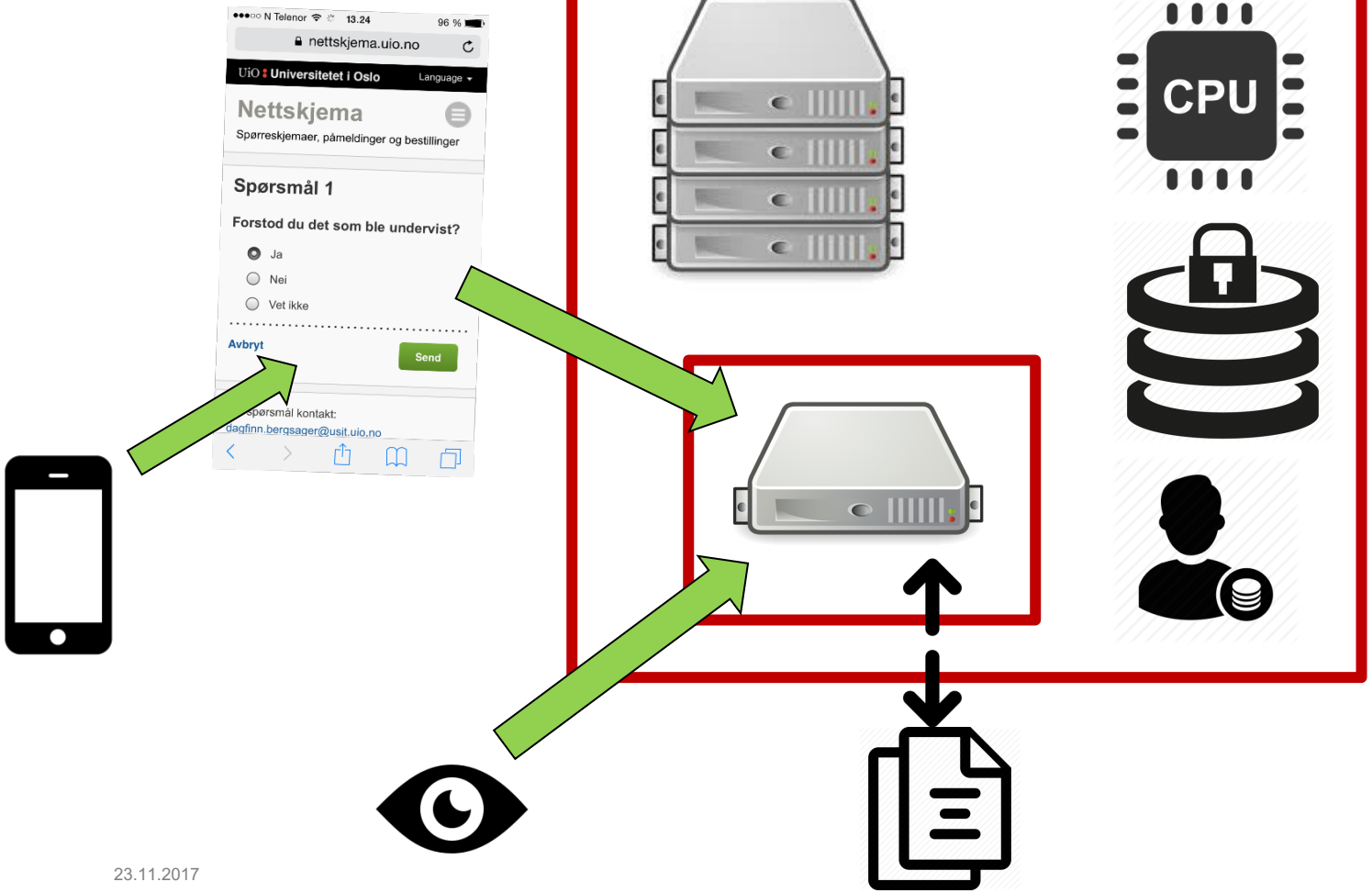
Tjenester for sensitive data

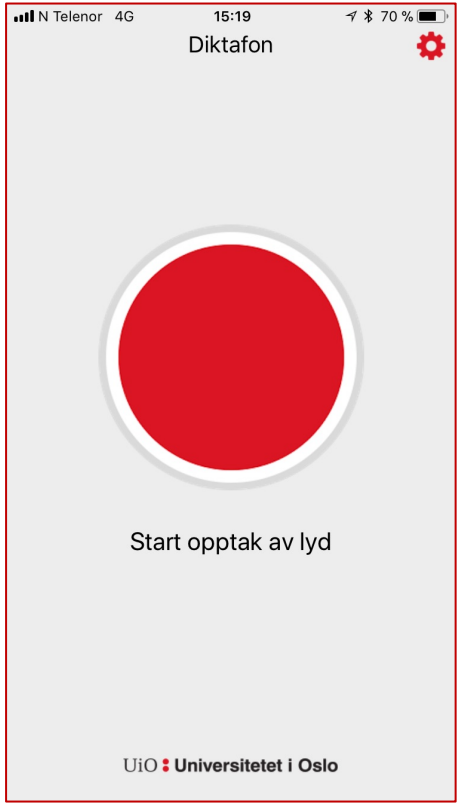
- Forsker kan laste opp data
- Arbeid med data skjer på serveren inne i TSD
  - SPSS/Excel, egen database, HPC, backup
- Kan motta data fra åpen webside via Nettskjema
- Kontinuerlig sikkerhetstestet

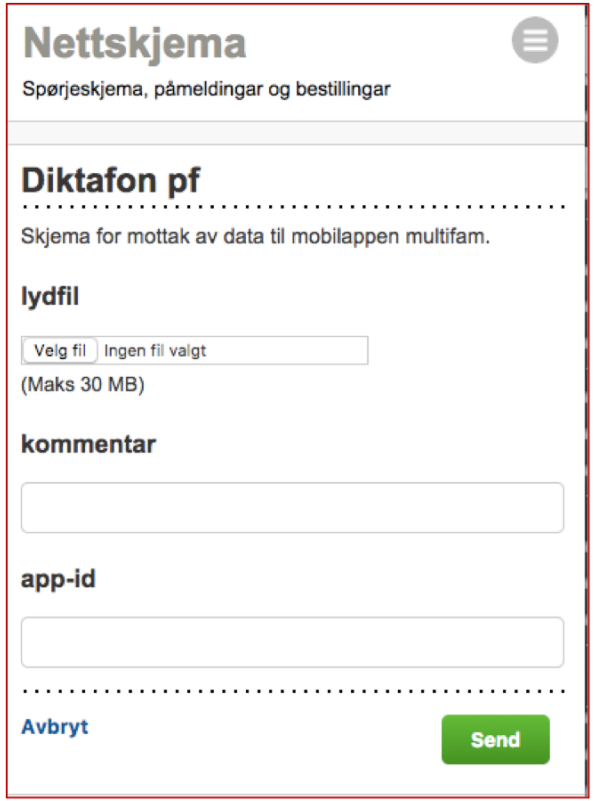
Nettskjema

- Datainnsamling via nett
- Forskjell fra QuestBack og tilsvarende
  - Vi håndterer sikkerhet og personvern
  - Gratis å bruke for de som har kjøpt den
  - Vi tilpasser den etter lokale behov
- Mobilapper kan levere data via Nettskjema
- Kan samle inn sensitive personopplysninger til TSD
- UiO utvikler og drifter


Nettskjema
Spørreskjemaer, påmeldinger og bestillinger
Hjelp
Dagfinn Bergsager
Logg ut
Forside
FHI - bildetest - Kostholdsskjema for ungdommer
FHI - bildetest - Kostholdsskjema for ungdommer
0 %
50 %
100 %
Søvn
Mindre enn 5 timer
5 timer
6 timer
7 timer
8 timer
9 timer
10 timer
11 timer eller mer
Hvor mange timer søvn får du hver natt på hverdager?
Hvor mange timer søvn får du hver natt i helgen?
Forrige side
Neste side
Avbryt

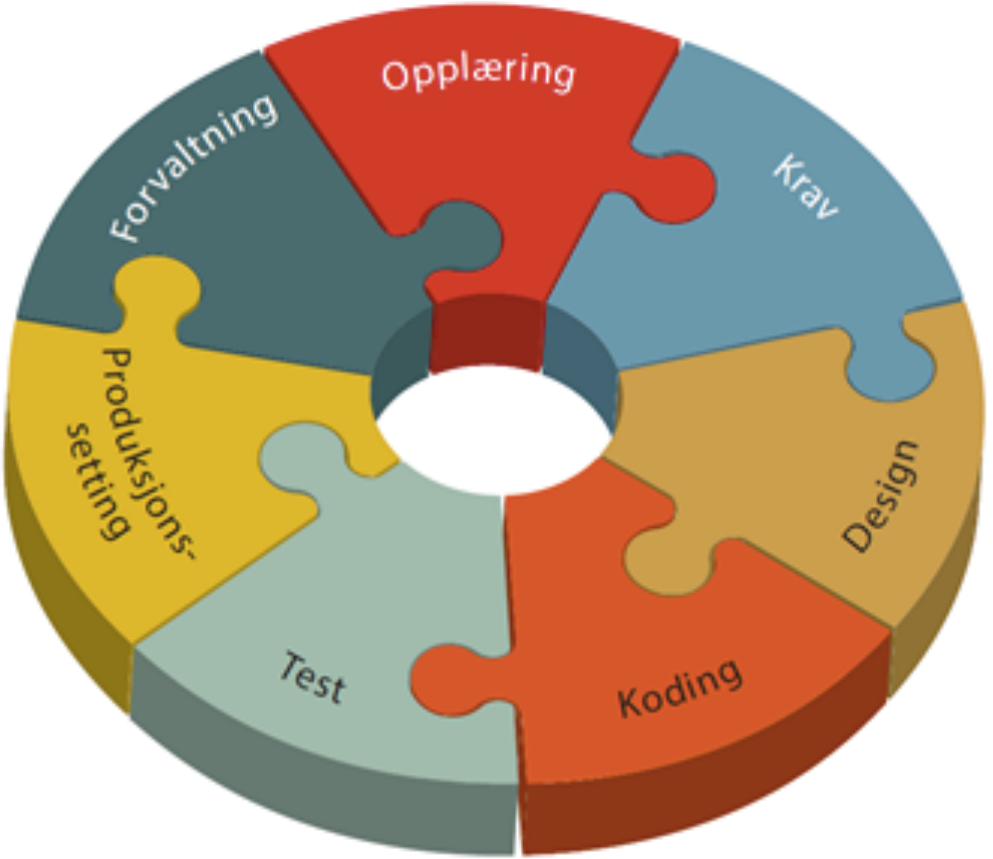

N Telenor 13.24 96 %
nettskjema.uio.no
UiO : Universitetet i Oslo
Language
Nettskjema
Spørreskjemaer, påmeldinger og bestillinger
Spørsmål 1
Forstod du det som ble undervist?
Ja
Nei
Vet ikke
Avbryt
Send
Spørsmål kontakt:
dagfinn.bergsager@usit.uio.no
CPU





Kommaseparert fil

Koding



Illustrasjon hentet fra www.datatilsynet.no

Vår metode: Scrumban
→ for å unngå personlig backlog

- Morgenmøter med gjennomgang av tasks i Jira
- Har en slags teamleder (faller naturlig)
- Leder av morgenmøtet baseres på loddtrekning dagen før
  - Veldig mye morsommere med ny scrummaster hver morgen!
- Hele tiden endringer i hvordan vi bruker og gjennomgår Jira
  - Hurra, vi er agile!

Vår metode: Scrumban

- **Alle** oppgaver skal i jira
- Ingen sprinter eller nøye estimering
- Alle comitts i git skal godkjennens av minst en annen utvikler
  - Mye diskusjoner i Bitbucket

Vår metode: Scrumban

- Hver story har en dedikert eier med ansvar for
  - IxD og Grafisk design
  - Sikkerhet og jus
  - Utvikling av tester
  - Produksjonsetting
    - Egen chattekanal
  - Brukerdok

Vår metode: Scrumban

- Ekstra langt morgenmøte på mandagen
  - Første 15 min kun IxD (eget møte for mobilapper)
  - Jeg forteller hva som er viktigst denne uka
    - …og hva som ikke er viktig lengre
  - Overordnet hvem gjør hva
  - Demo fra forrige ukes releaser

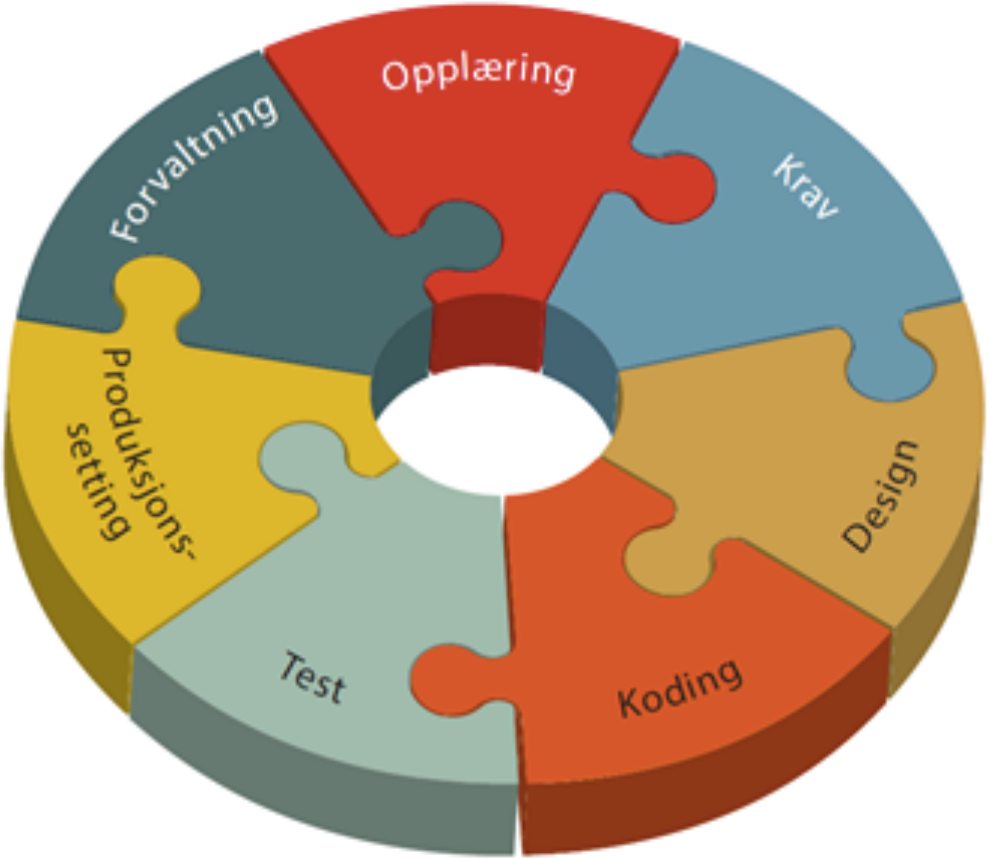
Vår metode: Scrumban

- Retrospekt en gang i måneden
  - Saker meldes inn i forkant
- Gjennomgang av **FELLES** backlog en gang i måneden
  - Populært å finne issues som kan stenges

Verktøy

- Høyere krav til at alle skal gjøre ting på samme måte
  - Programmeringspråk
  - Rammeverk
  - Software på Mac
- Lisenser blir dyrere og dyrere…og strengere innkjøpsregler
- Mye ligger i skyen med shady vilkår
- Har egne rutiner for ROS av programvare
  - Scanne endringer i TOS…+++

Test



Illustrasjon hentet fra www.datatilsynet.no

Bruk av personopplysninger i test

- Lovens krav gjelder også på testdata – det samme vil det gjøre etter GDPR
  - Hovedregel ved UiO: Testing skjer på testdata
  - Enten databaser hvor opplysningene har blitt anonymisert eller egne databaser med fiktive data
  - Tung vei å gå, men gikk gjennom til slutt

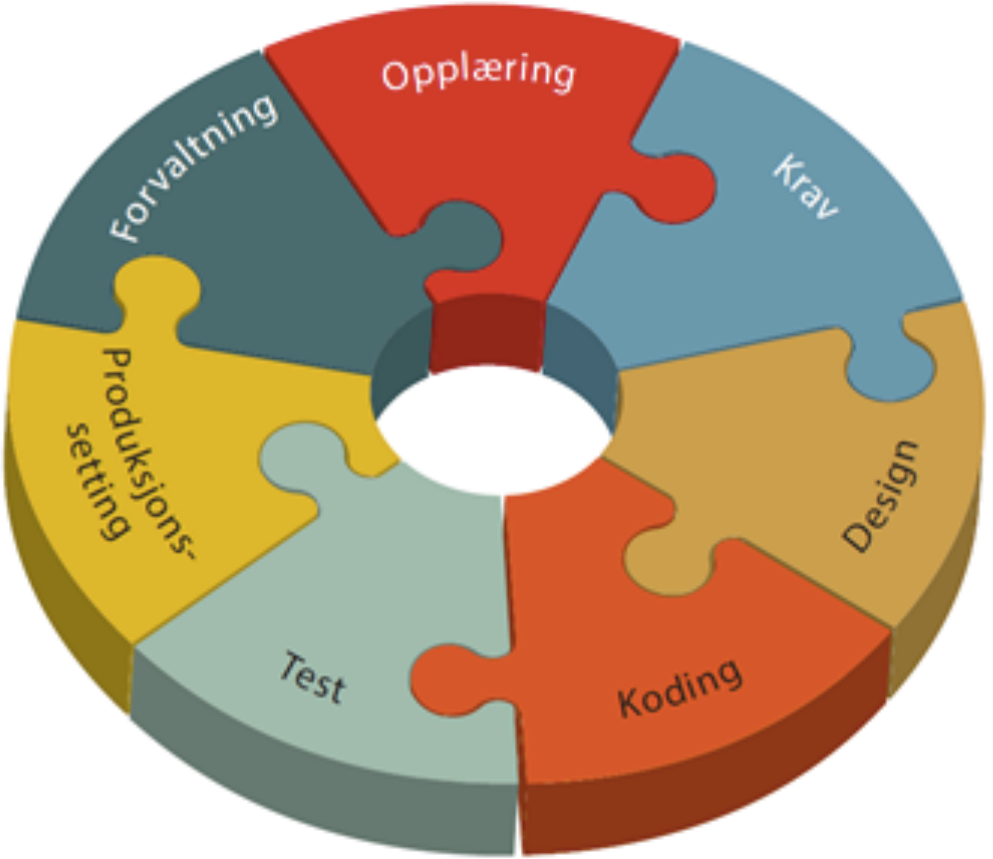
Systematisk testing

- Alle apper pentestes før produksjon
- Endringer brukertestes av UX
- Storyeier av ny feature er ansvarlig for manuell testing på browsere/mobiler

Bug Bounty

- Skal henge den opp på IFI
- Kjøpte inn premier
- Spent stemning…
- Hele teamet begynte å tette hull jeg ikke ante eksisterte…
- Allerede før vi har hengt opp plakater har vi tettet en rekke hull
- →HURRA!
- + at IT-sikkerhet ble litt redde ☺

Produksjonsetting



Illustrasjon hentet fra www.datatilsynet.no

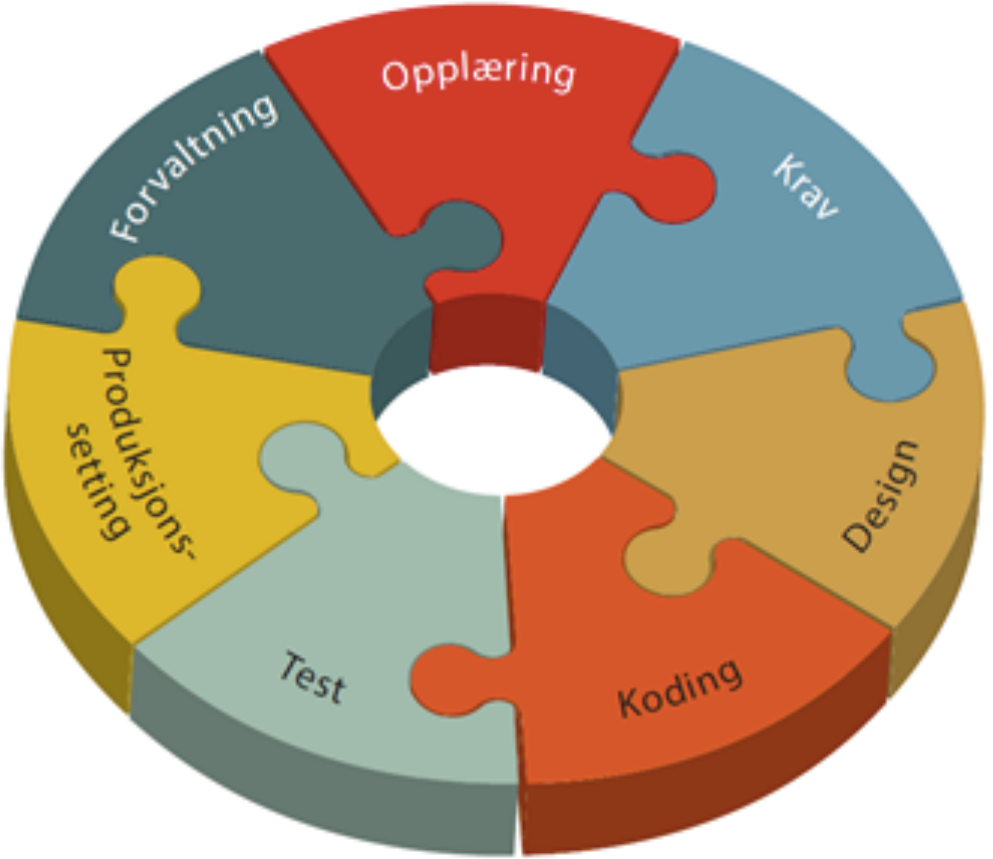
DevOps

- Produksjonsetter flere ganger om dagen uten nedetid
- Avhengige av automatiske tester som kjører hver gang
  - Gjennomtenkt testdekning (ikke fullstendig)
- Alle på teamet prodsetter

Nøye på data som lagres i mobilapp

- Risikovurdert hver app hvilke data som kan lagres i appen
- Pinkode
- StudieID håndteres som passord (Keyring)
- Bilder og lyd legges kryptert i kø dersom nett mangler
  - Data i kø er ikke lesbare i appen
- Nøye kontroll over hva som blir tatt backup av

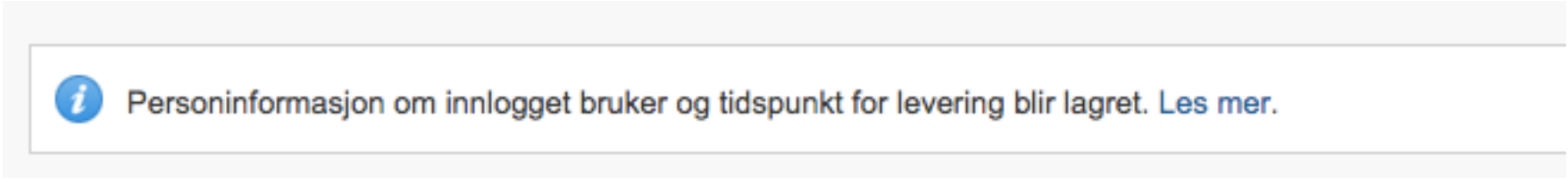
Forvaltning



Illustrasjon hentet fra www.datatilsynet.no

Skanner jevnlig data

- Leter etter publiserte fødselsnummer hver natt
- Markerer alle skjema som samler inn personinformasjon
- Fjerner automatisk persondata som vi vurderer som lite relevante
- Varsler bruker om hvilke personopplysninger som blir lagret



Scanning av kode

- Alle kode (i all utviklet software) og underliggende biblioteker og avhengigheter scannes hver natt for sårbarheter
- Basert på top ten OWASP

U

DEPENDENCY-CHECK

How to read the report | Suppressing false positives | Getting Help: google group | github issues

Project: Nettskjema

Scan Information (show all):

- *dependency-check version*: 2.0.1
- *Report Generated On*: Aug 29, 2017 at 07:01:48 +02:00
- *Dependencies Scanned*: 152 (135 unique)
- *Vulnerable Dependencies*: 4
- *Vulnerabilities Found*: 8
- *Vulnerabilities Suppressed*: 4
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
commons-httpclient-3.1.jar	cpe:/a:apache:commons-httpclient:3.1 cpe:/a:apache:httpclient:3.1	commons-httpclient:commons-httpclient:3.1	Medium	3	LOW	13
esapi-2.0.1.jar	cpe:/a:owasp:enterprise_security_api:2.0.1	org.owasp.esapi:esapi:2.0.1	Medium	2	HIGHEST	17
spring-messaging-4.2.4.RELEASE.jar	cpe:/a:pivotal:spring_framework:4.2.4 cpe:/a:pivotal_software:spring_framework:4.2.4 cpe:/a:springsource:spring_framework:4.2.4 cpe:/a:vmware:springsource_spring_framework:4.2.4	org.springframework:spring-messaging:4.2.4.RELEASE	Medium	2	HIGHEST	16
spring-oxm-4.3.4.RELEASE.jar	cpe:/a:pivotal:spring_framework:4.3.4 cpe:/a:pivotal_software:spring_framework:4.3.4 cpe:/a:springsource:spring_framework:4.3.4 cpe:/a:vmware:springsource_spring_framework:4.3.4	org.springframework:spring-oxm:4.3.4.RELEASE	Medium	1	HIGHEST	16

Dependencies

commons-httpclient-3.1.jar

Description: The HttpClient component supports the client-side of RFC 1945 (HTTP/1.0) and RFC 2616 (HTTP/1.1) , several related specifications (RFC 2109 (Cookies) , RFC 2617 (HTTP Authentication) , etc.), and provides a framework by which new request types (methods) or HTTP extensions can be created easily.

License:

Apache License, http://www.apache.org/licenses/LICENSE-2.0

Logging

- Før:
  - Logget alt evig
- Nå:
  - Logger minst mulig
  - Sletter alle logger etter 3 måneder
  - Egne verktøy for å se trender
  - Loggnivå øktes betraktelig og lagres lengre dersom du har utvidede rettigheter
    - Innlogget med driftsbruker eller er superbruker
    - Kliniske studier…

Registrere systemer som samler inn persondata

- Forskningsprosjekter kontrolleres av NSD og REK
  - Eksternt personvernombud
- Administrative systemer har måtte registrere hvilke personopplysninger de samler inn i egen webapp
  - Lansert for ca 10 år siden
  - Internt personvernombud

Behandling av personopplysninger

Innmelding og vedlikehold av administrative behandlinger av personopplysninger

Søk i Personopplysninger | Søk

Dagfinn Bergsager logg ut

Søk | Mine behandlinger | Opprett ny behandling | Hjelp

Opprett ny behandling

På denne siden skal kun admininstrative behandlinger registreres, behandlinger som ledd i forskning skal registreres hos NSD.

Lagre | Avbryt

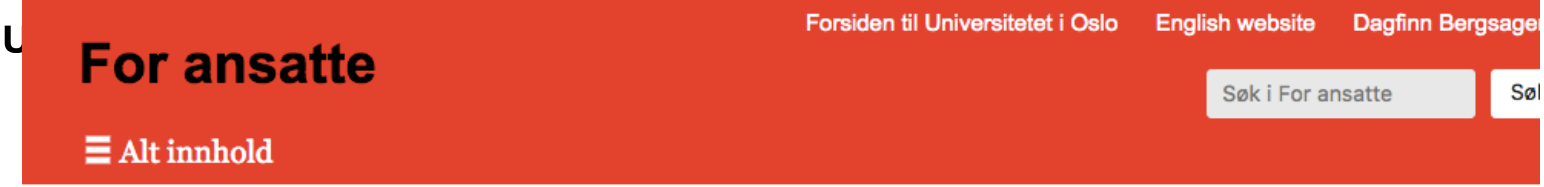
1. Behandlingsansvar

1.1 Institusjon:	Universitetet i Oslo
1.2 Adresse:	Postboks 1072 Blindern
1.3 Postnummer og -sted:	0316 OSLO
1.4 Dato for innsending:	23.10.2017

2. Daglig ansvar

2.1 Navn:	Dagfinn Bergsager
2.2 Stilling/grad:	Gruppeleder
2.3 Arbeidssted:	WAPP, WEB, UAV, USIT, LOS

Ny løsning som både har forskningsprosjekter for administrative systemer som behandler personopplysninger lansert denne høsten



Kvalitetssystem for helseforskning

Oversikt over helseforskningsprosjekter

Velg enhet

- Det medisinske fakultet
- Det odontologiske fakultet
- Det samfunnsvitenskapelige fakultet

Finn prosjekt

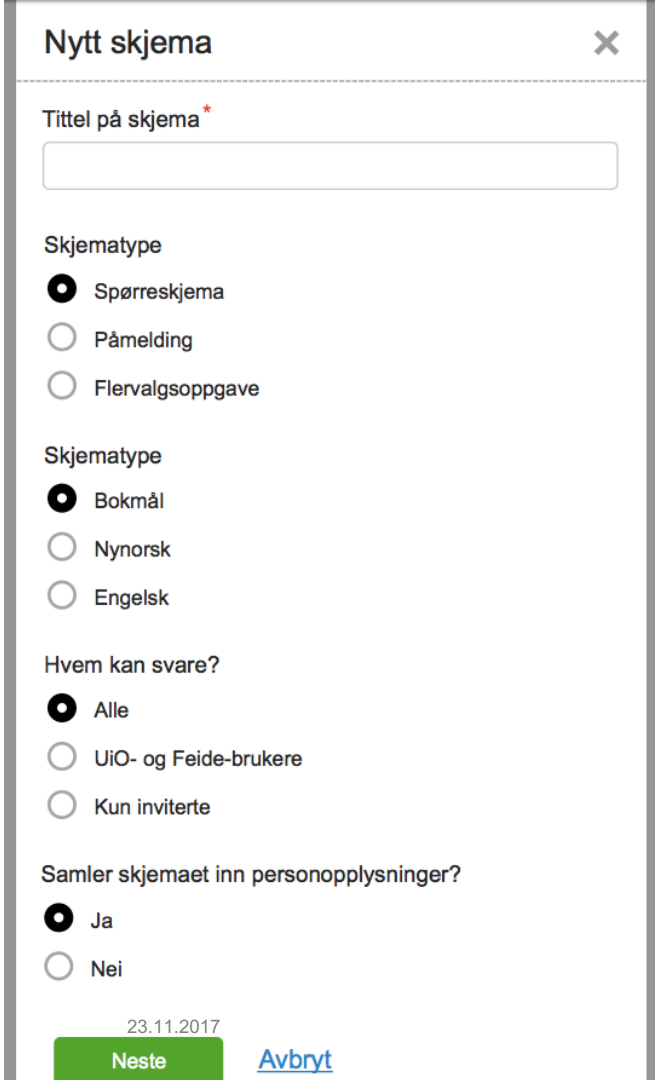
Søk

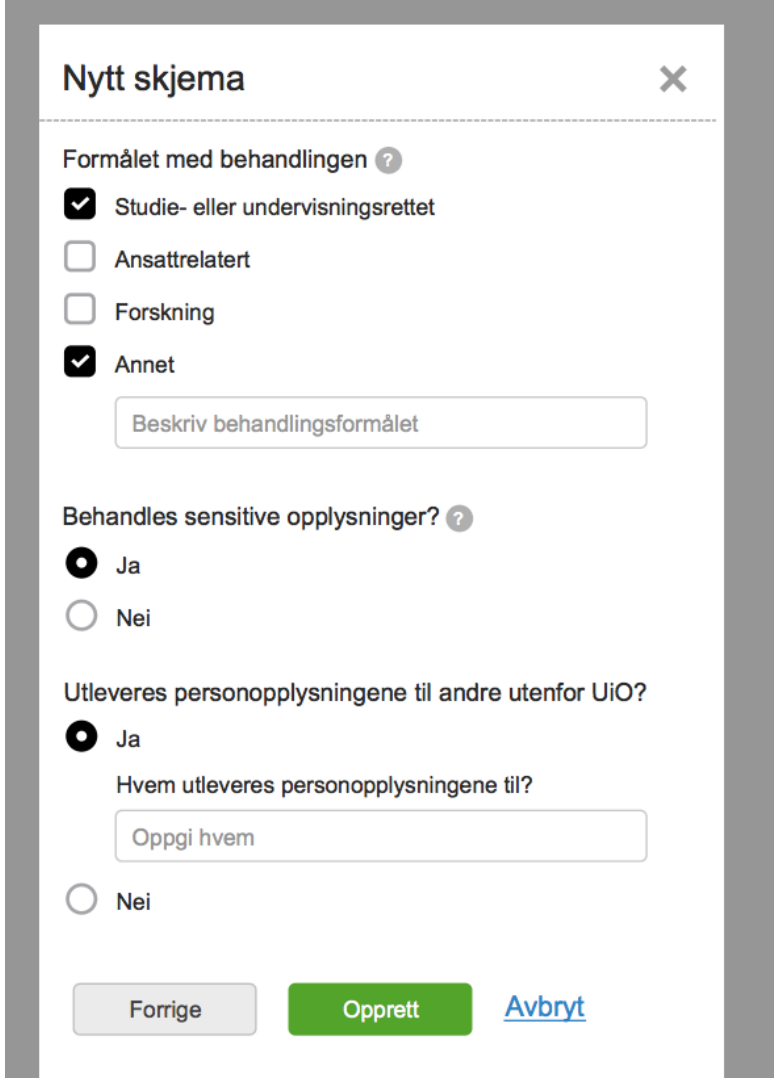
Søk på **tittel** eller **forsker**

- [x] Alle typer
- [ ] Studentprosjekt
- [ ] Ph.D.-prosjekt
- [ ] Forskerprosjekt

- [x] Alle statuser
- [ ] Oppstart
- [ ] Pågående
- [ ] Avsluttet

Registrer nytt prosjekt


Nytt skjema
Tittel på skjema *
Skjematype
Spørreskjema
Påmelding
Flervalgsoppgave
Skjematype
Bokmål
Nynorsk
Engelsk
Hvem kan svare?
Alle
UiO- og Feide-brukere
Kun inviterte
Samler skjemaet inn personopplysninger?
Ja
Nei
Neste
Avbryt


Nytt skjema
Formålet med behandlingen
Studie- eller undervisningsrettet
Ansattrelatert
Forskning
Annet
Beskriv behandlingsformålet
Behandles sensitive opplysninger?
Ja
Nei
Utleveres personopplysningene til andre utenfor UiO?
Ja
Hvem utleveres personopplysningene til?
Oppgi hvem
Nei
Forrige
Opprett
Avbryt

Hva gjør vi når vi oppdager/mistenker avvik?

- Klare rutiner for hendelseshåndtering som skal følges
  - Dedikert team som er trent for situasjonene
  - Institusjonene kjenner godt til rutinene
- Kartlegging av situasjonen og vurderer /iverksetter tekniske tiltak
  - Eks. fjerner tilganger og kartlegger hvem som har aksessert informasjonen

Hva gjør vi når vi oppdager/mistenker avvik?

- Behandlingsansvarlig vurderer hendelsen og hvem som skal kontaktes
- Informasjon til de registrerte
- Rapport sendes til personvernombudet som vurderer om Datatilsynet skal varsles

demo