



Dette har vi gjort for å påstå at vi er GDPR-ready!

Dagfinn Bergsager
Leder for (web og) mobilapputvikling



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

-fordi vi har innebygd personvern!

...overalt

Nettskjema

- Datainnsamling på nett
- Sektortjeneste for UH
- Stor bruk fra FHI og OUS
- Mottar 2000 – 20 000 svar per dag
- Mobilapper og webpper kan levere data via Nettskjema
- UiO utvikler og drifter
- Kan samle inn sensitive personopplysninger



Mobilapper i forskning

- Har utviklet omlag 20 apper for forskningsprosjekter
- Drifter (MDM) iPads for forskning på skoler og sykehus + **ambulanser** i Oslo
- Nettskjema er backend for alle apper
- Alle prosjekter får ROS med fokus på hvilke data som ligger igjen på telefonen
 - Utfordring med kliniske apper på åpne telefoner...

Design

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

(slik som Vipps ligger oppå UNIX)

Prioriteringer for all utvikling

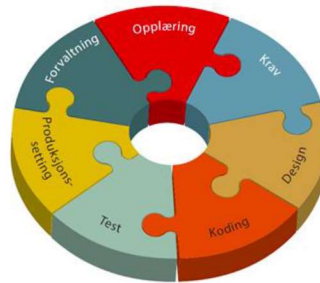
1. Sikkerhet og personvern
2. Bruksopplevelse for den som skal levere data
3. Funksjonalitet for den som samler inn data

-Vi skal alltid være best på sikkerhet og personvern!
 -og fungere på alt utstyr for alle personer
 -og være enkel og bruke for datainnsamler

Veileder fra Datatilsynet

Oppsummering: Programmer seriøst!

- Rutiner for metode
- Regler for koding
- Verktøyvalg
- Gjennomtenkt testing
- Gjør nødvendige sikkerhetstiltak



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.

Artikkel 5

Prinsipper for behandling av personopplysninger

1. Personopplysninger skal
 - a) behandles på en lovlig, rettferdig og gjennomsiktig måte med hensyn til den registrerte («lovlighet, rettferdighet og gjennomsiktighet»),
 - 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 korrigeres («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 utilsikket tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og fortrolighet»).
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
- Åpne [ROS-analyser](#)



- Nettskjema mottar daglig mellom 2000 og 10 000 svar
- Spesialisert for forskning og studieadministrasjon
- Sektortjeneste fra UiO



«Formålsbegrensning» (‘purpose limitation’)

- Forskere er obs på dette; vil tilrettelegger for dem
- Overvåker at andre som samler inn holder seg til formålet

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

24.04.2018

Neste Avbryt

demo

Nytt skjema

Formålet med behandlingen ?

Studie- eller undervisningsrettet

Ansattrelatert

Forskning

Annet

Beskriv behandlingsformålet

Behandles sensitive opplysninger? ?

Ja

Nei

Uteleveres personopplysningene til andre utenfor UiO?

Ja

Hvem uteleveres personopplysningene til?

Oppgi hvem

Nei

Forrige Opprett Avbryt

15

Tjenester for sensitive data



- Sikker, skalerbar forskningsplattform for UiO og andre offentlige forskningsinstitusjoner.
- Alle prosjekter får sin egen sikre server
 - En server per godkjenning (REK/NSD)
- Begrensa mulighet for eksport av data og behandling av data skjer på serveren inne i TSD (SPSS/Excel, HPC, backup)
- Kan motta data fra åpen webside via Nettskjema

Skanner jevnlig data utenfor TSD

- 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

Personinformasjon om innlogget bruker og tidspunkt for levering blir lagret. [Les mer.](#)

Scanning av kode

- Alle kode (i all utviklet software) og underliggende biblioteker og avhengigheter scannes hver natt for sårbarheter
 - Basert på top ten OWASP
- Skanner all kode i GIT (Bitbucket) etter hemmeligheter
 - Nøkler
 - Passord
 - Personnummer



Dependency-Check is an open source tool performing a best effort analysis of third party dependencies. false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the resulting generated vulnerability assessment reports are an AG-OS activities, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the resulting problem is at the user's risk. We do not share the copyright holder for OWASP but hold liable for any damages whatsoever arising out of or in connection with the use of the tool, the analysis performed, or the resulting report.

[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 (139 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:httplib:3.1	commons-httpclient:commons-httpclient:3.1	Medium	3	LOW	13
esapi-2.0.1.jar	cpe:/a:owasp:esapi-esapi: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 HTTP 1.0, 1.1 (H1/H1.1) and HTTP 2.0 (H2/H2.1), several related specifications (H2-C 2109 (Cookies), H2-C 2617 (H1/H1 Authentication), etc.), and provides a framework by which new request types (methods) or HTTP extensions can be created easily.

License:

Public Domain: [http://www.apache.org/licenses/LICENSE-2.0](#)

«Dataminimering» (‘data minimisation’)

- Minimalt logges og slettes etter 3 mnd
 - Egne verktøy for å se trender
- Krever at skjemaer registrerer ekstra info om de skal samle inn personopplysninger
- Oversikt over skjema som samler personinfo gjennomgå med ansvarlig enhet årlig

«Riktighet» (‘accuracy’)

- Kun lenker til personkatalog –ikke import av kontaktinfo
- Grunndata om personer hentes fra SAP eller FS (StudentWeb)
- Forskningsprosjekter kan bruke IDporten
 - Forskjellige nivå
- Tydelig for bruker hvilke data som lagres
 - Må ha en ID til respondent for å kunne fjerne data...

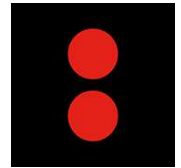
«Lagringsbegrensning» (‘storage limitation’)

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

24.04.2018

22

Nye utfordringer med mobilapper



- Mobilappen må lagre noe data
 - Når du leverte data sist
 - ID på hvem som har levert svaret
 - Ev. noe tilbakemelding på trend
- At du har installert appen kan kobles til at du har en diagnose
- Dersom appen mister nett, legges data i kryptert kø
- Data på mobiler blir ofte sikkerhetskopiert til Apple/Google

24.04.2018

23

The screenshot shows the iTunes Preview page for the app 'MittBlikk'. At the top, there are navigation tabs for Mac, iPad, iPhone, Watch, TV, Music, and Support. The main heading is 'iTunes Preview' with sub-tabs for 'Oversikt', 'Musikk', and 'Video'. The app name 'MittBlikk' is prominently displayed, followed by 'By Universitetet i Oslo' and a note that it is only available on the App Store for iOS devices. A description states that the app is for data collection for a research project at UiO, requiring a study ID. A 'What's New in Version 1.0.2' section mentions bug fixes and design adjustments. The app is listed as 'Free' and 'Designed for both iPhone and iPad'. A 'Screenshots' section shows three preview images of the app on different devices.

The screenshot shows the 'Min SAFEStart' app interface. At the top, it displays 'UiO : Universitetet i Oslo' and the status bar with 'iPhone', '4:21PM', and '100%' battery. The app title 'Min SAFEStart' is at the top of the content area. Below it is the SAFE logo and a large 'Velkommen!' (Welcome!) message. The text explains that the app is for pregnant women who want to log symptoms and receive an overview of pregnancy symptoms. It also mentions that the app is part of a study at UiO. A large purple button labeled 'Neste' (Next) is at the bottom. The footer shows 'UiO : Universitetet i Oslo'.

24.04.2018

25

iPhone 4:21PM 100%

Min SAFESTart

Logg inn

For å kunna skille dine data fra andres trenger vi ditt fødselsnummer

Bekreft fødselsnummer

Neste

24.04.2018

UiO : Universitetet i Oslo

26

iPhone 4:21PM 100%

Introduksjon

Hvor langt er du på vei?

- Beregn fra første dag i siste menstruasjon
- Beregn fra terminsdato

Første dag i siste menstruasjon

Du er nå i uke: 10 (9 + 4 dager)

Neste

24.04.2018

27

iPhone 4:21PM 100%

Min SAFESTart

Hvor mange timer i løpet av de siste 24 timene har du følt deg kvalm eller uvel i magen?

- Ingen
- Mindre enn 1
- 2 - 3
- 4 - 6
- Mer enn 6

Angi antall timer mer nøyaktig:

Neste

24.04.2018

28

iPhone 4:21PM 100%

Min SAFESTart

Du er i uke **10** (+ 4 dager)

Din kvalmegrad er **Moderat**

Hva skjer med barnet? →

Se dine målinger →

Logg din kvalme >

Hjem Målinger Livstilsråd Barnet

24.04.2018

29

iPhone 4:21PM 100%

Min SAFESart

Har du fått diagnosen
Hyperemesis gravidarum
av lege?

Ja

Nei

Forrige Fullfør

iPhone 4:21PM 100%

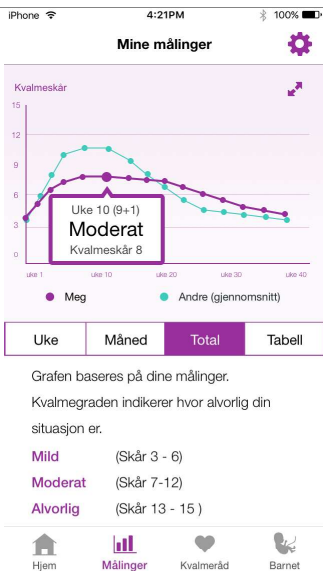
Min SAFESart

Din kvalme

Basert på målingene dine har du hatt
kvalmeskår på **13** eller over, 1 uke i
strekk. Dette regnes som **Alvorlig**
svangerskaps-kvalme.

Vi anbefaller at du oppsøker legen din.

OK



«Integritet og fortrolighet» (‘integrity and confidentiality’)

- Egne driftsbrukere for personer med ekstra tilgang
 - Full logging
- 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

«Ansvaret»

(‘accountability’)

- Jevnlige varslinger til de som samler inn data om de har skjema som bør ryddes /slettes
- Tar ansvar for alle forskningsprosjekter
- 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
- Alle som samler inn persondata må registrere det

Det viktigste er at alle i organisasjonen forstår at innebygd personvern og innebygd sikkerhet er noe alle er ansvarlig for