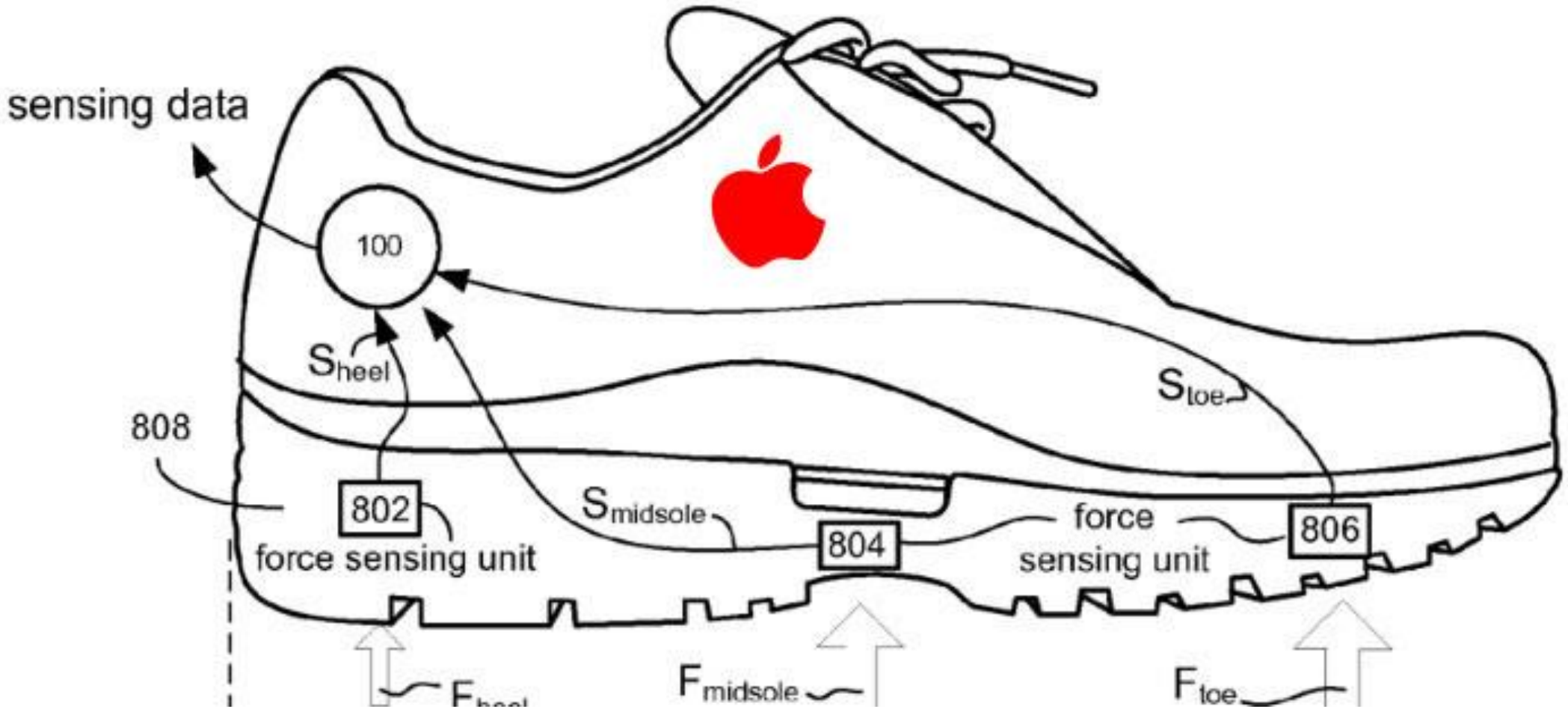
Innebygd personvern og personvern som standard

AFIN Seminar om innbygging av rettsregler

Eirin Oda Lauvset | Seniorrådgiver i Datatilsynet

27. februar 2019

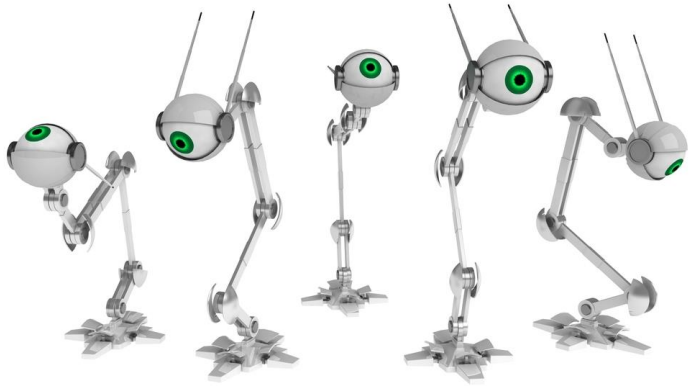
Datatilsynet


sensing data
100
S_{heel}
808
802
force sensing unit
$S_{midsole}$
804
force
sensing unit
806
S_{toe}
$F_{midsole}$
F_{toe}

Personvern i vår digitaliserte verden

- Skal vi ivareta personvernprinsippene **effektivt** må de være **inkorporert** i programvaren

- **Nøkkelpersonene** for at vår digitale verden blir personvernvennlig vil være de som bestiller og utvikler programvare



- Nødvendig med kunnskap om personvern for å bygge **personvernfremmende** applikasjoner, tjenester, roboter, algoritmer for automatiske beslutninger, kunstig intelligens, deep learning osv

Veileder for programvareutvikling med innebygd personvern.

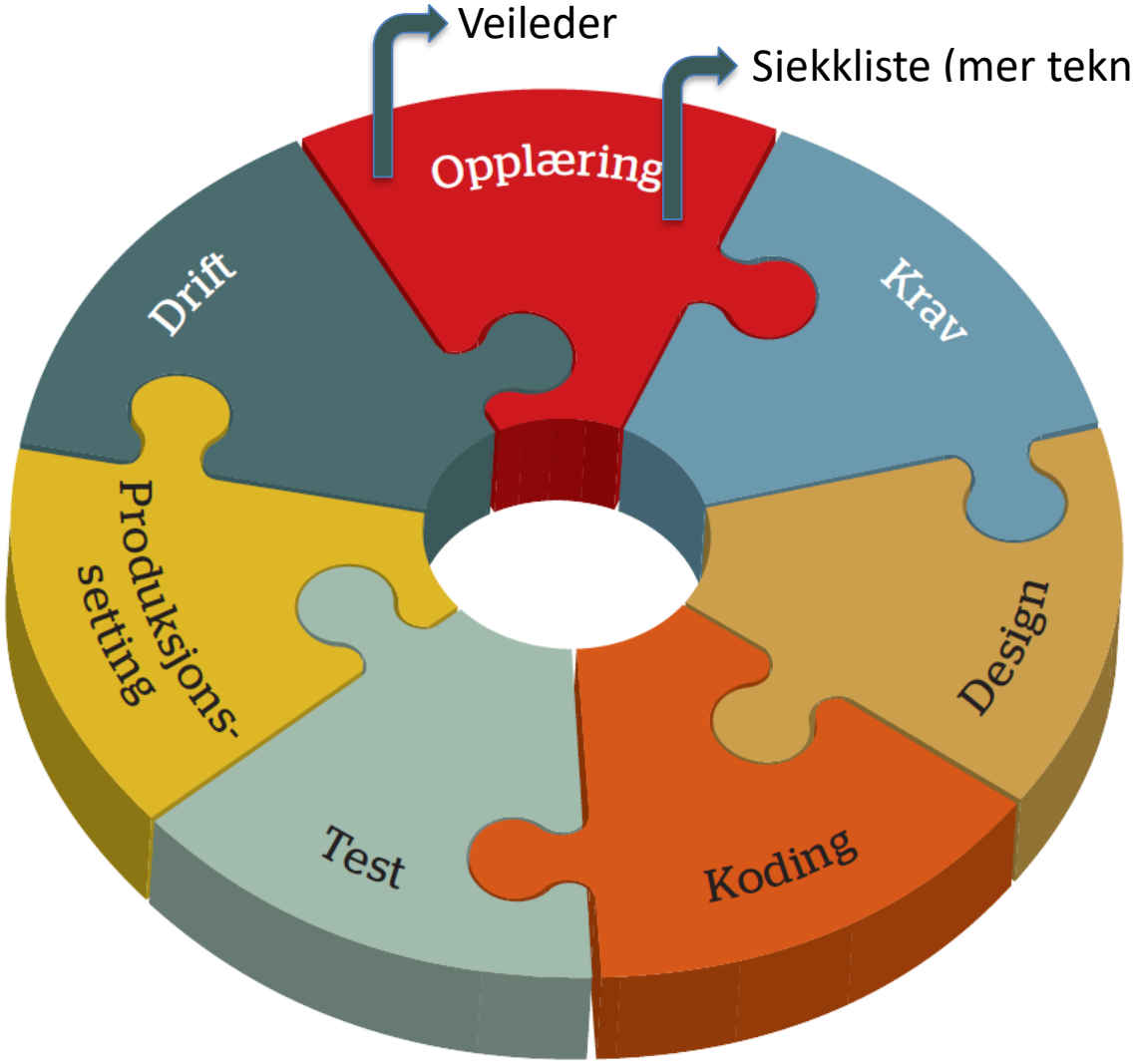
- 2017: Veileder for programvareutvikling med innebygd personvern.

- **Beregnet for**:
  programvareutviklere
  behandlingsansvarlige som bestiller eller kjøper programvare

- Beskriver **hvordan** implementere personvernprinsippene, den registrertes rettigheter og friheter, og andre forpliktelser for den behandlingsansvarlige i hver aktivitet i utviklingsprosessen

- Veilederen refererer til eksisterende rammeverk som:
  - ISO 27034 Application security, Software Development Life Cycle, Microsoft Security Development Life Cycle (SDL), Secure Software Development Life Cycle (S-SDLC), Privacy and Data Protection by Design - from policy to engineering – ENISA.

Veileder for programvareutvikling med innebygd personvern



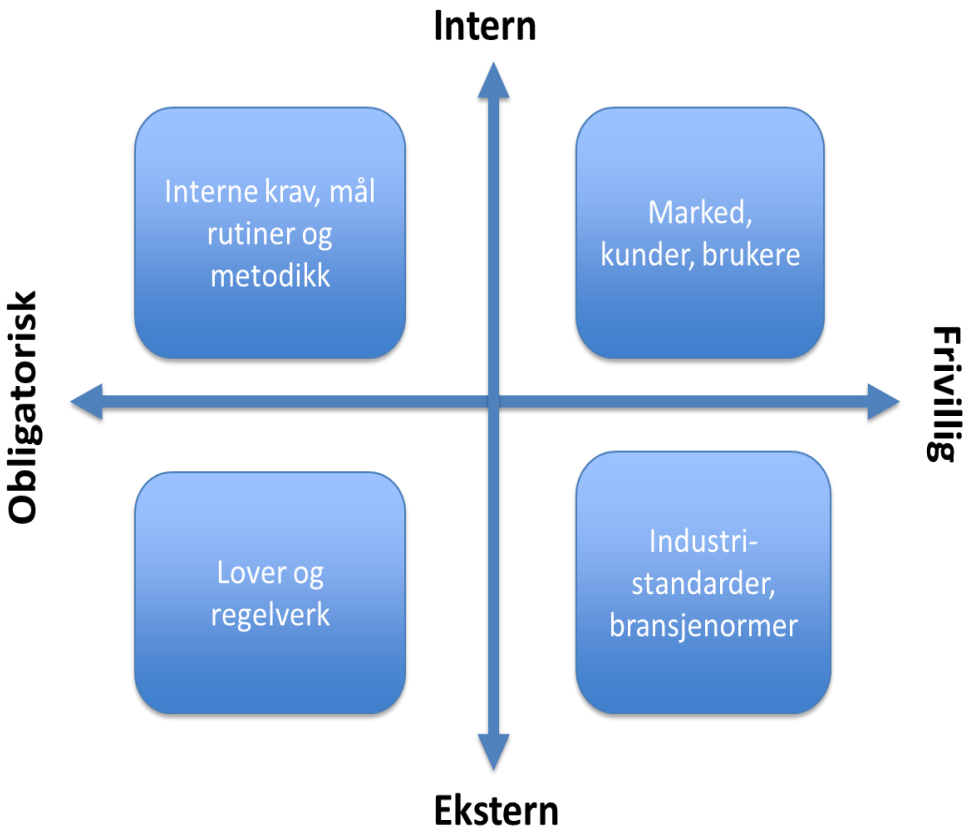
- Aktiviteter i programvareutvikling
- Et supplement til virksomhetens eksisterende metodikk.
- Eksempler på bade tekniske og organisatoriske tiltak for å være i samsvar
- Både veilederen og sjekklisten finnes på engelsk: https://www.datatilsynet.no/en/

Opplæring

- **Mål:** Basiskunnskap og forståelse for personvern og informasjonssikkerhet

- **Hva skal det gis opplæring i:**
  Når og hvorfor personvern og informasjonssikkerhet er viktig i de ansattes daglige arbeidsoppgaver

- **Suksesskriterier:**
  -etablerte retningslinjer for personvern og informasjonssikkerhet,
  -intern opplæring i retningslinjene er adressert



Kravsetting

- **Beskrivelse av den prosesseringen av personopplysninger som programvaren skal foreta**
  - Kategorier av opplysninger, kategorier av registrerte, ansvarsforhold, kilder og mottakere, etc.

- **Oversikt over hvilke lover, retningslinjer, normer etc som er relevante**

- **Prinsipper skal ha effekt**
  - Lovlig, rettferdig, åpen behandling
  - Formål, dataminimering og lagringsbegrensning
  - Informasjonssikkerhet

- **Rettighetene skal være reelle**
  - Informasjon, innsyn, korrigering, sletting, dataportabilitet, etc

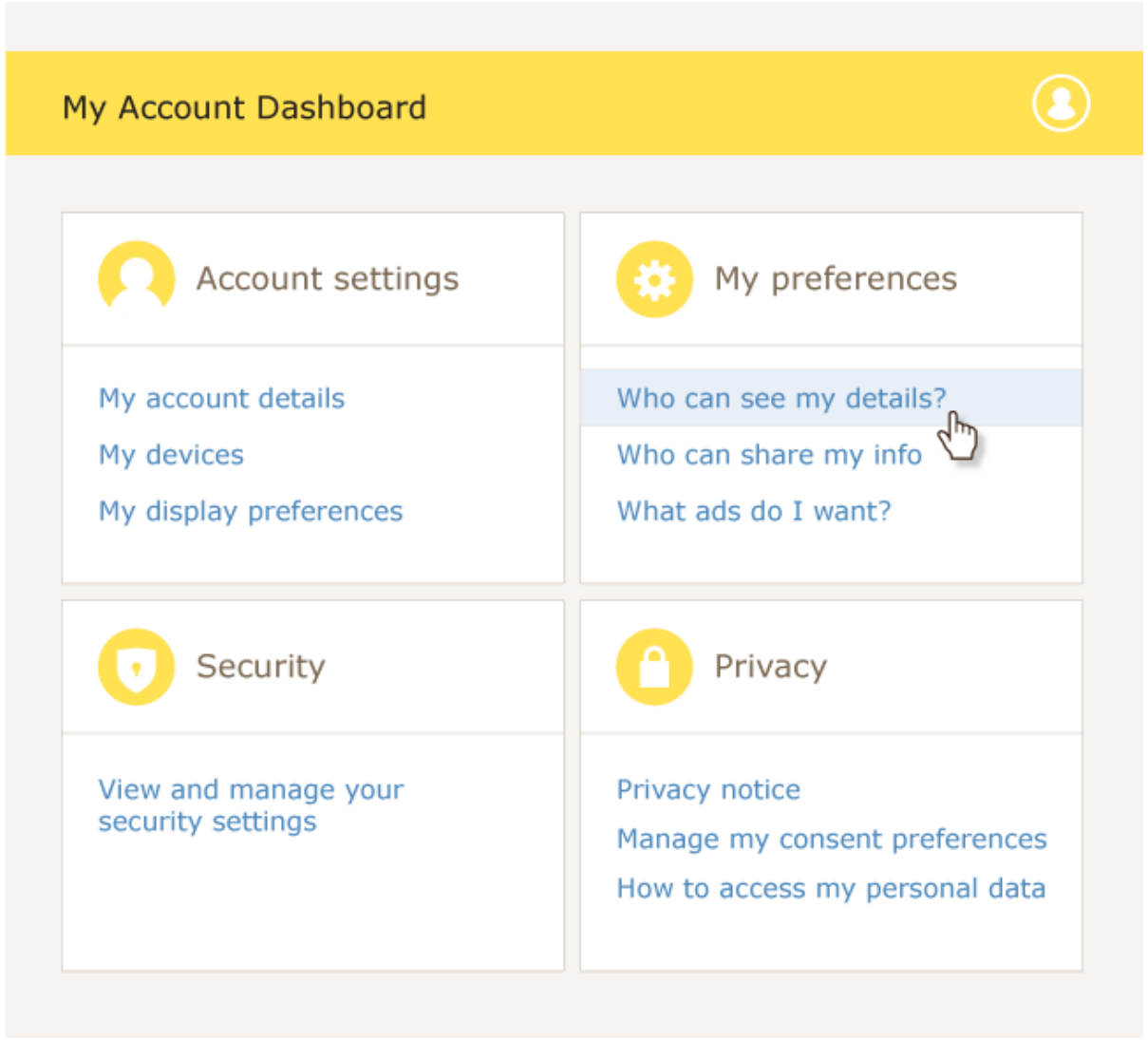
Design

- **Dataorienterte designkrav:**
  - Minimer og begrens *«Select before you collect»,*
  - «gjem og skjul», separer, aggreger,
  - personvern som standard

- **Prosessorienterte designkrav:**
  - informer, kontroller, håndheve, demonstrer

- **Trusselmodellering**
  - analysere komponenter, dataflyt og prosessflyt i programvaren.
  - hvor er det svakheter med hensyn til de krav vi har satt?
  - hvordan kan designet forbedres for å unngå å ikke etterleve krav?

La brukeren selv velge hvilke data hun vil dele

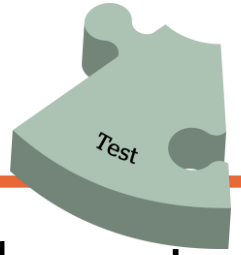


Legg til rette for dataportabilitet

Koding

- **Bruk godkjente verktøy og rammer**
  - Beskriv bruksområde og sikkerhetsfunksjonalitet
- **Ugyldiggjør utrygge funksjoner og moduler**
  - Analyser funksjoner, API, tredjepartsbibliotek og moduler
  - Forby de som er utrygge, oppdater de som er utdaterte eller inneholder kjente sårbarheter,
  - Bruk verktøy for kodeskanning for å sjekke koden, deaktiver unødig sporing, logging og innsamling av personopplysninger
- **Statisk kodeanalyse og kodegjennomgang**
  - Automatiske verktøy, manuell gjennomgang for å fange opp svakheter som kan medføre feil bruk eller lekkasje av personopplysninger, regelmessig gjennomgang

Test



- **Test om personvern og sikkerhetskravene** er implementert og riktig implementert?
  -utarbeid sjekkliste (med sjekklisten fra kravfasen som utgangspunkt)

- **Sikkerhetstesting**
  - testing av programvaren for å avdekke sårbarheter og for å være sikker på at koden ivaretar sikkerhet og personvern på tilstrekkelig måte

- **Gjennomgang av trusselmodell og angrepsflate**
  - programvare kan avvike fra funksjonelle og tekniske spesifikasjoner som er satt under krav- og designfasen
  - trusselmodellen og angrepsflaten må derfor gjennomgås når programvaren er komplett
  - ny gjennomgang av trusselmodell og vurderingen av personvernkonsekvenser

Produksjonssetting

- **Utarbeid plan for hendelseshåndtering**
  -detektere, analysere, rapportere, håndtere og normalisere

- **Sikkerhetsgjennomgang av programvaren**
  -skal baseres på tidligere gjennomganger i utviklingsløpet

- **Godkjenning av produksjonssetting**
  - Sikkerhetsrådgiver og personvernombud verifiserer at definerte sikkerhets- og personvernkrav er implementert og fungerer etter hensikten.
  - Virksomheten må definere hvem som har godkjenningsmyndighet.

- **Arkivering**
  -dokumentasjon av utviklingsløpet

Forvaltning

- **Håndtere hendelser og avvik etter planen**
  - Det skal være avklart hvem som skal kontaktes når, og hvem som er i stand til å bygge, teste og installere oppdateringer
  - Det skal være avklart hvilke prioriteringer som gjelder, samt nøyaktig hvem som skal gjøre hva når avvik skjer.
  - Øve

- **Forvaltning, drift og vedlikehold av programvaren**

  - skal følge etablerte rutiner for hvordan personvern og sikkerhet skal ivaretas over tid

  - styringssystem for personvern og informasjonssikkerhet som omfatte anskaffelse, forvaltning, drift og vedlikehold

  -rutiner for regelmessige testing og revidering, sikkerhetsovervåkning, målinger, forbedring mm.

Kåring av årets produkt med innebygd personvern

Innebygd personvern i praksis – miniseminar og premieutdeling

Vi skal kåre vinnere av fjorårets konkurranse om *innebygd personvern* og i den anledning inviterer vi til et åpent frokostseminar, i tillegg til prisutdeling og presentasjon av finalistene. Kom hvis du er nysgjerrig på hva innebygd personvern er og hvordan det kan brukes i praksis.

Publisert: 12.02.2019

Sted: Kulturhuset, Youngs gate 6, Oslo
Tid: 18. mars, kl 8.30-11.00 (enkel servering og registrering fra kl. 8.30, seminaret starter kl. 9.00)
Arrangementet er gratis og åpent for alle. Det vil også strømmes - lenke legges her i forkant av seminaret.

Innebygd personvern er et krav i personopplysningsloven. Det betyr at personvern skal bygges inn i alle løsninger og i all teknologi der personopplysninger blir behandlet. For å løfte frem eksempler på hvordan det kan og bør jobbes med, rent praktisk, utlyste vi høsten 2018 en konkurranse og nå skal vinnerene kåres.

Nytt av året er at vi også deler ut en studentpris.

Les mer om konkurransen

Program

Detaljene i programmet er ikke helt på plass, men det blir en innledning om innebygd personvern, presentasjon av finalistene og prisutdeling.

I tillegg vil vi få to fagpresentasjoner; et om sikkerhetskoding og et om sikkerhetstesting ved programvareutvikling med innebygd personvern.

1. Koding understreker hvor viktig det er at utviklere bruker godkjente verktøy og rammer, at utrygge funksjoner og moduler bør ugyldiggjøres, og at statisk kodeanalyse og kodegjennomgang bør gjennomføres regelmessig.

2. Test innebærer en anbefaling om å teste om personvernkrav og sikkerhetskrav er riktig implementert, en beskrivelse av hva slags sikkerhetstester som bør gjennomføres, og en forklaring på hvor viktig det er å gjennomgå trusselmodell og angrepsflate.

Dette vil dere få høre mer om på seminaret.

Vi hadde en tilsvarende konkurranse i fjor, da var det Direktoratet for e-helse som vant med sin Kjernejournal.

Takk for oppmerksomheten!

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no

@datatilsynet