



# Forum for informasjonssikkerhet og personvern

Onsdag 1. mars

Kl. 09:00 – 11:00



# Program

|                      |                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>09:00 - 09:05</b> | <b>Velkommen og introduksjon til dagens program</b>                                                                                                                     |
| <b>09:05 - 09:15</b> | <b>Hva skjer på personvernområdet?</b><br>Maryke Silalahi Nuth                                                                                                          |
| <b>09:15 - 09:25</b> | <b>Hva skjer på informasjonssikkerhetsområdet?</b><br>Åsmund Skomedal                                                                                                   |
| <b>09:25 - 09:50</b> | <b>Security Champions</b><br>Martin Albert-Hall fra Origo                                                                                                               |
| <b>09:50 - 10:00</b> | <b>Pause til å fylle kaffekoppen</b>                                                                                                                                    |
| <b>10:00 - 10:30</b> | <b>Dugnad i Gamle Oslo</b><br>Et eksempel på hvordan få oversikt over behandlinger av personopplysninger<br>Ida Marie Larsen og Tommy Haugen Svela fra Bydel Gamle Oslo |
| <b>10:30 - 10:55</b> | <b>Åpen mikrofon – erfaringsdeling i forumet</b>                                                                                                                        |
| <b>10:55 - 11:00</b> | <b>Avslutning</b>                                                                                                                                                       |





Oslo

# Hva skjer på personvernområdet?

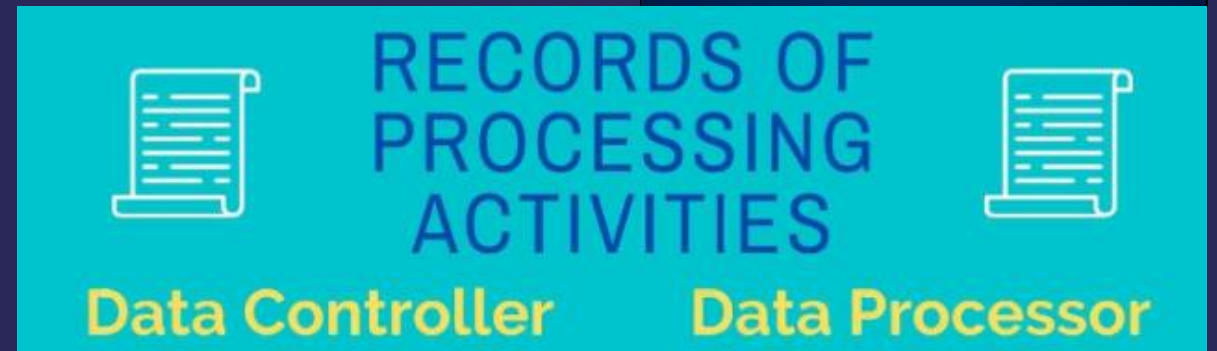
Maryke S. Nuth  
Fagsjef personvern  
[maryke.nuth@byr.oslo.kommune.no](mailto:maryke.nuth@byr.oslo.kommune.no)

*Forum for informasjonssikkerhet og personvern  
01. mars 2023*



# Behandlingsoversikten i Oslo kommune

- › Fra prosjekt til forvaltning mars 2023
- › Flere utviklingsfaser – også i forvaltning
- › Virksomhetenes bruk av løsningen



# Tilbakeblikk personvernåret 2022 i EU

## Eye-catching fines

Ireland's Data Protection Commission **issued** the second- and third-largest GDPR fines to date: 405 million and 265 million euros **against** Instagram and Meta, respectively. In the U.S., Epic Games will pay \$275 million to **settle** children's privacy violations with the U.S. Federal Trade Commission. The FTC also fined Twitter \$150 million for **using** account security data for targeted advertising in violation of a 2011 consent decree.

## GDPR Strengthening Its Influence Across the Globe

EU-based privacy pros place even more emphasis on **GDPR compliance**, with more than 60% saying it is their number one job, compared to just 16% in the U.S.

In 2021, the number of companies that achieved GDPR compliance increased by 7% compared to 2020, the **IAPP** recent study states. 47% of respondents claimed to be wholly or very compliant with GDPR. Therefore, organizations are expected to use GDPR to gain greater adoption in 2022-2025 due to its jurisdictional neutrality. Strict penalties for non-compliance push companies to continuously improve their cyber policies aimed at information security and data protection.

## Flowing forward: EU-US Data Privacy Framework took shape

The EU and the U.S. finally agreed to a fresh data transfer regime this year. The **proposed** EU-U.S. Data Privacy Framework could be finalized sometime during summer 2023, which will mark three years since the invalidation of its predecessor — the EU-U.S. Privacy Shield.

The DPF addresses concerns over U.S. foreign intelligence and EU consumer redress. However, the proposal faces a **looming** Court of Justice of the European Union challenge over whether the EU and the U.S. hit on the shortcomings outlined in the previous deal's invalidation. And what if the EU-U.S. agreement can't rise to CJEU standards? Journalist Luca Bertuzzi **painted** a picture of potential EU data localization, with EU policymakers "progressively" examining "stricter limitations to trans-Atlantic data flows."



# Tilbakeblikk personvernåret 2022 i Norge

- Schrems II
- Bruk av apper og SoMe
- Gjenbruk av data til forskning
- Rapport fra personvernkommissjonen
- Bruk av kunstig intelligens:  
ansiktsgjenkjenning



# Har du spørsmål? Ta kontakt med din sektorkontakt i FIN/ISI team personvern

|               | BLK              | NOE | KIF | FIN        | BYU | MOS | OVK              | AIS            | HEI | BYD              |
|---------------|------------------|-----|-----|------------|-----|-----|------------------|----------------|-----|------------------|
| Sektorkontakt | Siri P. Johansen |     |     | Brit Røthe |     |     | Linda M. Knutsen | Siril Jonassen |     | Linda M. Knutsen |

Generelle henvendelser sendes til fagsjef for personvern Maryke S. Nuth



# Informasjonssikkerhet - hva skjer

Oslo 01.02.2023

Åsmund Skomedal,  
informasjonssikkerhetssjef  
**[asmund.skomedal@byr.oslo.kommune.no](mailto:asmund.skomedal@byr.oslo.kommune.no)**



Foto: Amara Husic



# Trusselrapporter – Q1 2023

## E-tjenesten – «Fokus»

### NSM – «Risiko 2023» [13. februar]

- ♦ De største selskapene og anleggene er kompliserte å angripe. Angrepsforsøkene vil derfor i økende grad gå mot **underleverandører**
- ♦ Fremmede aktører investerer og kjøper seg inn i norske virksomheter og eiendom for å få sensitiv informasjon og skaffe seg strategisk viktig teknologi.
- ♦ Målrettede påvirkningsoperasjoner med spredning av desinformasjon
  - På sikt kan desinformasjon svekke tilliten vi har til hverandre, til statlige institusjoner, og dermed også **skade vår politiske stabilitet** i Norge.

### PST – «nasjonal trusselvurdering 2023» [13. februar]

- ♦ Nettverksoperasjoner vil utgjøre en stor del av russisk og kinesisk etterretningsaktivitet i Norge. De digitale trusselaktørene utvikler stadig mer avanserte metoder og virkemidler for å få tilgang til sensitiv informasjon.



# EU nyheter – Q1 2023



## Nytt Direktiv – «NIS2 Direktivet»

- ♦ ... the proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) was presented by the Commission on 16 December 2020.
- ♦ The Directive was published ... in December 2022 and will enter into force on **16 January 2023**. Member states will have 21 months from the entry into force of the directive in which to incorporate the provisions into their national law (actual date: **18 October 2024**).
- ♦ Hovedmål
  - God beredskap
  - Samarbeid og informasjonsutveksling
  - Tiltak og sikkerhetskultur i vitale sektorer (energi, transport, vann, bank & fin. helse og digital infrastruktur)

# Hendelser i desember

- ▶ Smishing i Oslo-området ca 9. desember
  - Phishing via SMS med betalingskrav for parkering
  - Korrekt navn og adresse på eier og bilens reg. nr
  - Impliserte indirekte **Innkrevningsetaten** i kommunen
  - Strakstiltak: informere eksternt (web)
  - Omfang: antagelig ikke veldig stort (?)
- ▶ Flaske innsynsforespørsler (noen tusen?)
  - Strakstiltak internt i kommunen
    - informert om ikke å saksbehandle
    - «avsender» informert at sakene ikke behandles
  - Forespørslene ble vasket ut av WebSak i januar
  - DigiDir har lagt in «live test» for avsender



# Utvikling på sikkerhetsområdet

Tekniske sårbarheter  
1999: **894** nye  
2022: ca **25 000** nye

Et *målbilde* for  
sikkerhetsarbeidet

Kunstig  
intelligens

Angrep på  
leverandørkjeder

Løsepengevirus

Kommersialisering  
av skadevare

Tyveri av  
personopplysninger

Hacktivisme

Sosial manipulering

GDPR LG/VE

ISI  
etabl.

Koordinator  
ISK/PISK

Krav til  
styrings-  
system

Grunnleggende sikring (UKE m.fl.)



2010

2012

2014

2016

2018

2020

2022

2024



# Styringsrammeverket er verktøyet for sikkerhetsstyring

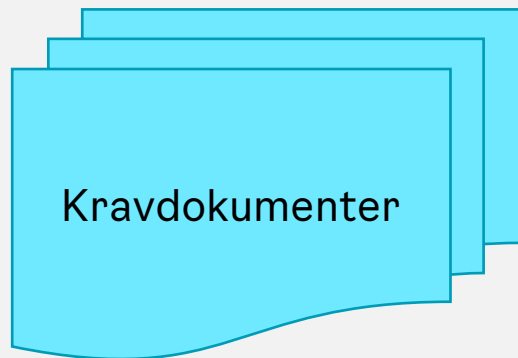
- ▶ Sette oppgaver i system slik at vi vet at vi
  - Beskytter de riktige tingene
  - Beskytter dem fra de riktige truslene
  - Beskytter dem tilstrekkelig, - ikke for mye og ikke for lite
- ▶ Styrer/leder for å unngå/motstå uønskede hendelser og håndterer dem når det skjer
- ▶ Iverksette systematiske sikkerhetstiltak for å
  - Forebygge
  - Oppdage
  - Håndtere
  - Gjenopprette
- ▶ Sette opp aktivitetene i et årshjul for å sikre kontinuerlig forbedring



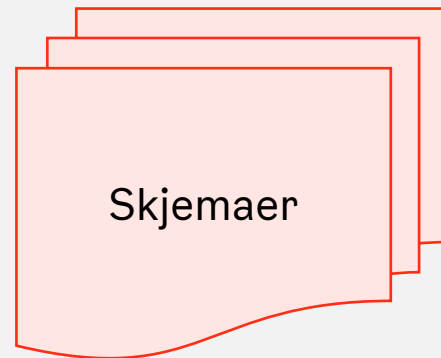
Det handler om å gjøre de riktige tingene, ikke bare om å ha de riktige dokumentene

# Hva inneholder OSIS?

Krav – til HVA som skal gjøres



Verktøykasse



Opplæring



Nettverk

**Let's be careful out there!**



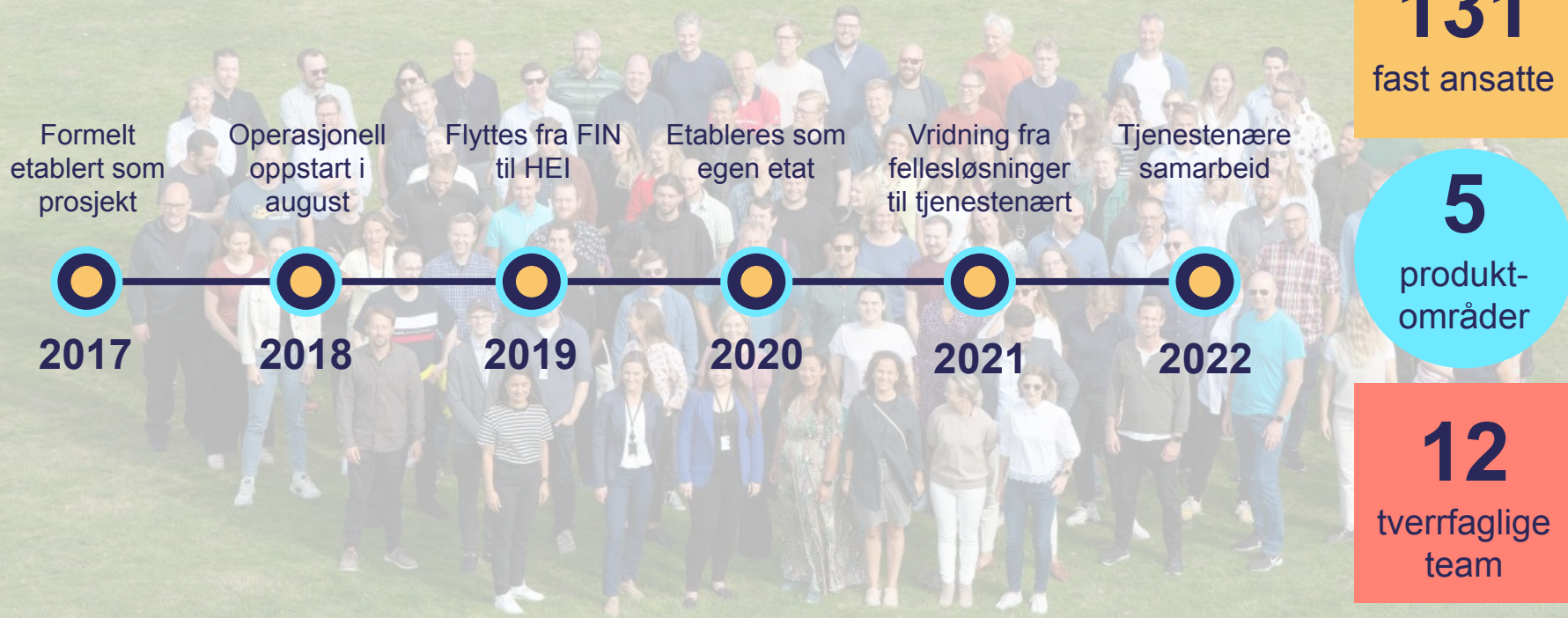


# Etablering av Security Champion i Origo

Bakgrunn - Hensikt - Prosess - Erfaringer

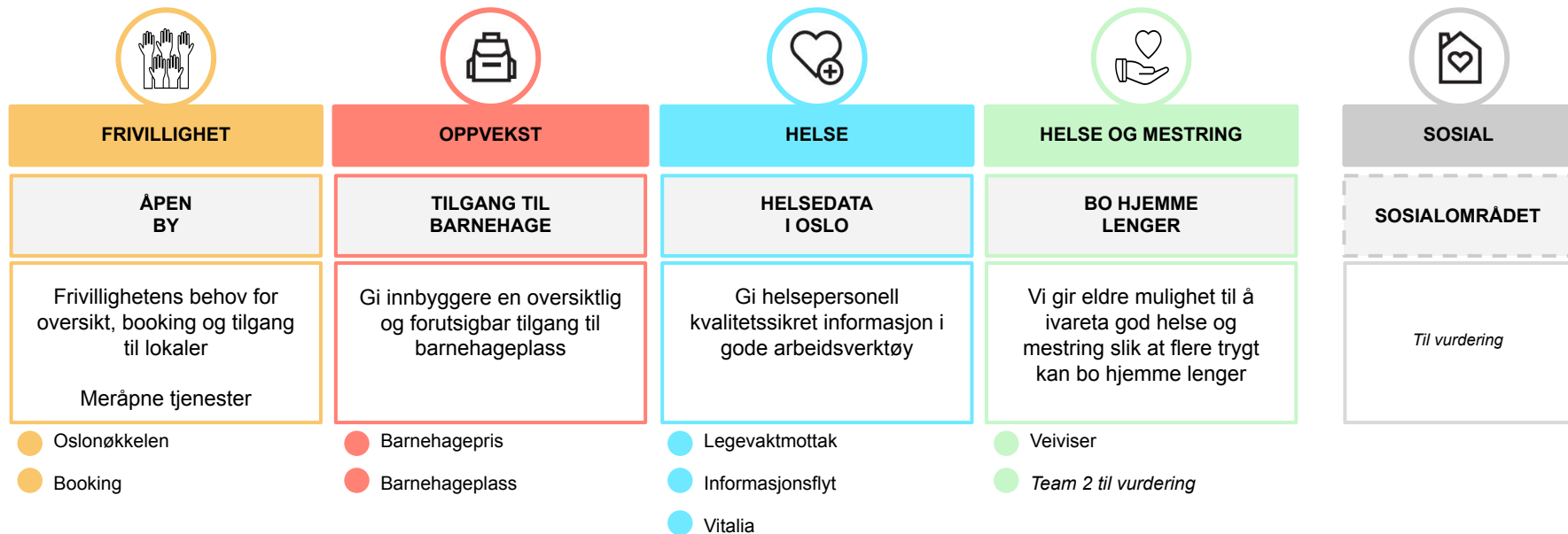


# Oslo Origo - kommunens interne kompetansemiljø for digital transformasjon





# Origos tjenestenære målbilde



## UTVIKLINGSOPPLEVELSER

- Dataspeilet
- Kjøremiljø

## SELVSTENDIGE TEAM

- Skjema
- Min side / designsystem



Oslo

# Team i Origo

Autonome team

Diversitet i teknologi

Egenutviklet vs åpen kildekode vs hyllevare

Diversitet i verdier som skal sikres

Utviklet komponent inngår i et større system



Oslo



# Infosec i Origo

4 faste, 2 konsulenter

Organisert sammen med 6 tekjurister

Noe av det vi jobber med:

- Sikkerhet i produktutvikling
- Risikovurderinger
- Sikkerhetstesting
- Bevisstgjøring og kulturbygging
- Styring, kontroll og etterlevelse



Oslo



# Hensikt - sikkerhet i team

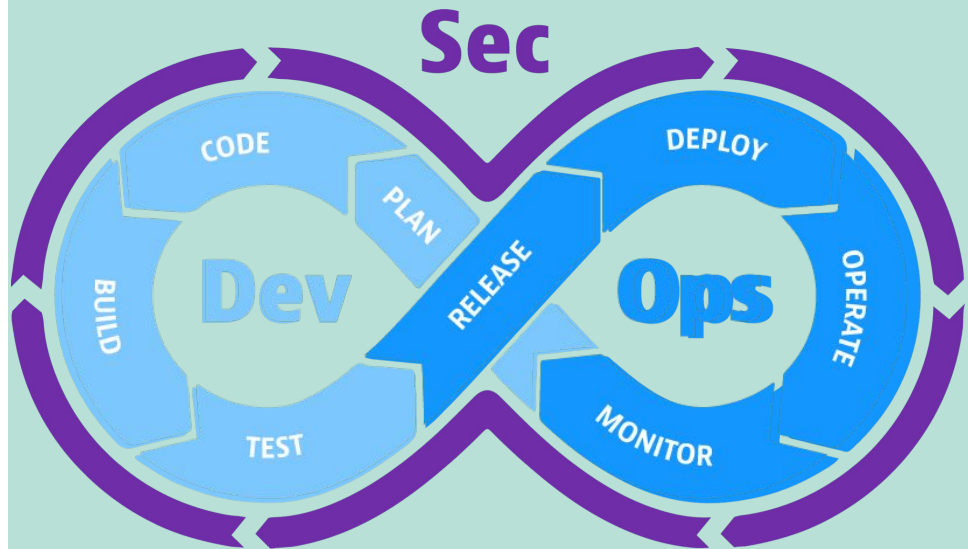
Fokusere sikkerhetsarbeidet relevant for team

Gi team trygghet i infosec-arbeidet

Understøtter DevOps prinsippet

Skalerbar (og kostnadseffektiv) løsning

Hindre ansvarspulverisering





# Security champion

Et etablert konsept i moderne utvikling

Ikke sikkerhetsekspert, men en motivert person i teamet

Med ekstra fokus på informasjonssikkerhet

Bidrar i teamets daglige sikkerhets-arbeid

Vet når ekspertkompetanse må innhentes



Oslo

# Alternativ

~~Alternativ 1:~~

~~Dedikert infosec person i teamet~~

~~Alternativ 2:~~

~~Asynkron sikkerhetstesting av infosec team  
før release~~

**Alternativ 3:**

**Etablere Security Champion**



Oslo

# ~~Planen~~ Fasiten

- Nov 21  Informere ledergruppen
- Apr 22  Informere POL/PL/TL
- Mai 22  Arbeidsgruppe etablert
- Mai 22  Innsiktsarbeid
- Mai 22  Konseptutredning (2 møter)
- Juni 22  Beslutning i ledergruppe
- Aug-Okt 22  Rekrutterings-"turné"
- Okt 22  Allmøte
- Nov 22  Kick-off



Oslo



# “Konseptbeskrivelse”

Hva er Security Champion i Origo

Rollebeskrivelse (oppgaver)

Ressursbehov (forventet tidsbruk)

Hva lærer man som Security Champion

Hvem kan bli Security Champion



Oslo

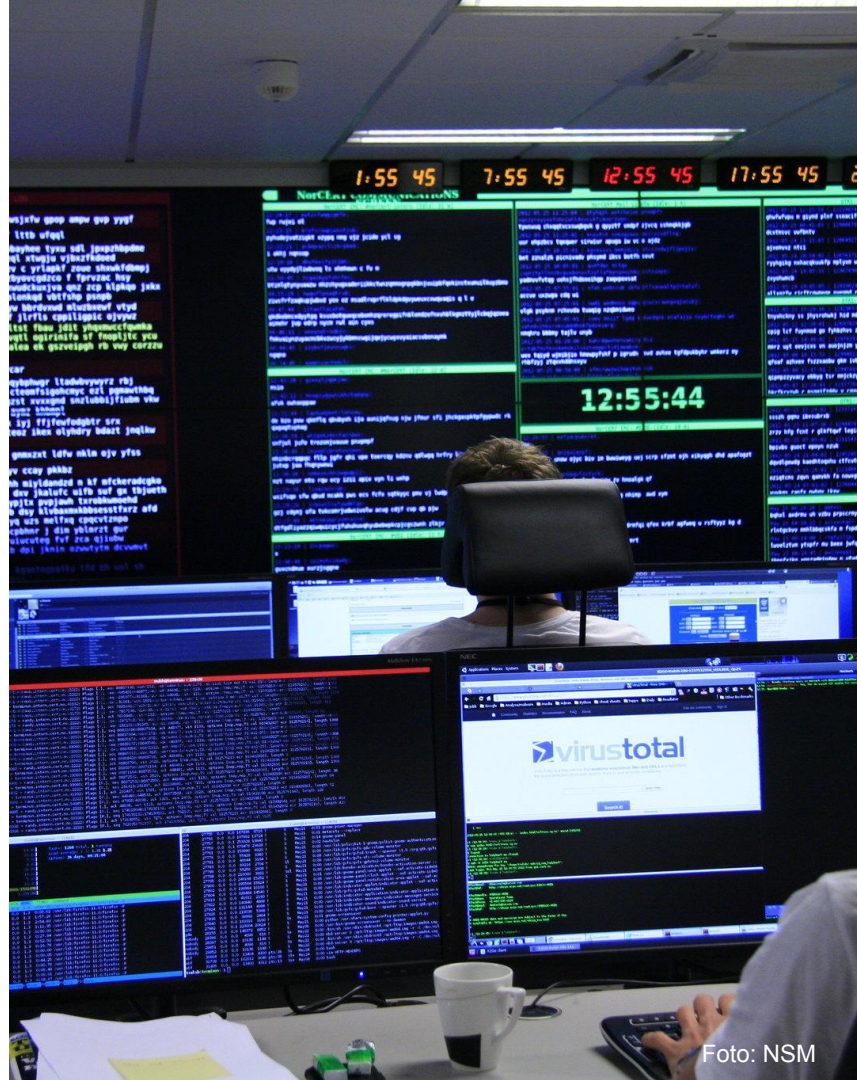


Foto: NSM



# Suksesskriterier

Støtte fra ledelsen (inkl POL, PL, TL)

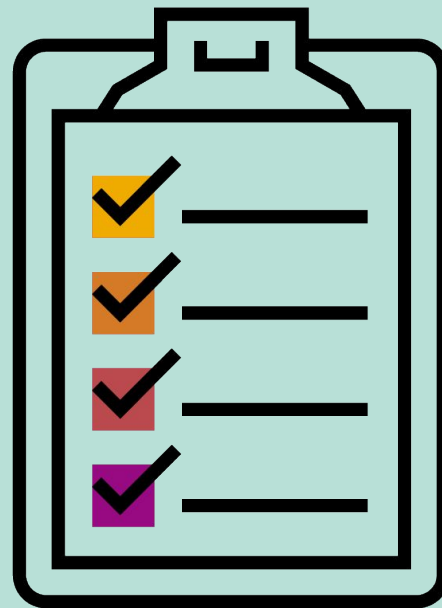
Security Champion kan prioritere tid til rollen

Tilstrekkelig midler til aktiviteter med gruppen

Tydelig ansvarlig for oppfølging av gruppen

Frivillig å gå inn i rollen

Ikke tro at Security Champion alene er  
løsningen på informasjonssikkerhet

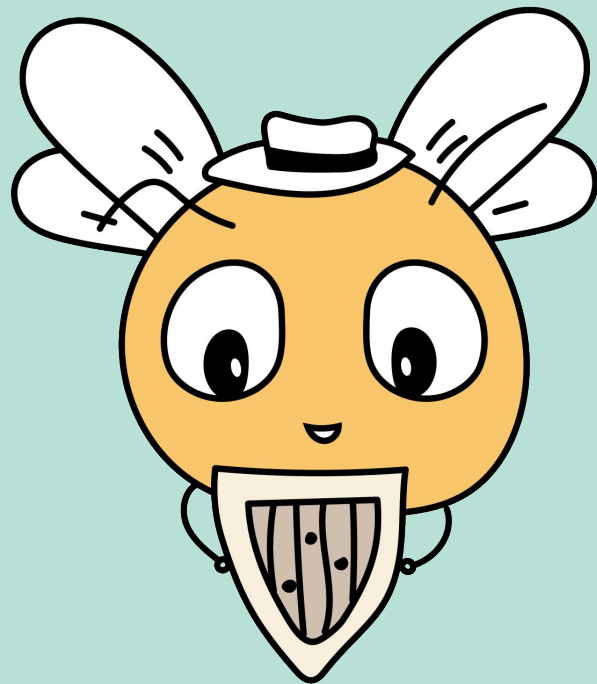


# Erfaringer nov-mars

10 av 12 team har nå en champion

Egen logo er gøy! (takkt til Mira!)

Merch, stæsj bra for å skape en identitet



Oslo



# Erfaringer nov-mars

Håndtering av OpenSSL sårbarhet

Implementering av hemmelighets-  
skanning



Oslo



Foto: Kode24 v/Mattis vaaland

# Erfaringer nov-mars

3 meetups med erfaringsutveksling

1 workshop om sikring av skyplattform

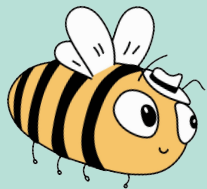
1 utflukt til Kripos og NC3



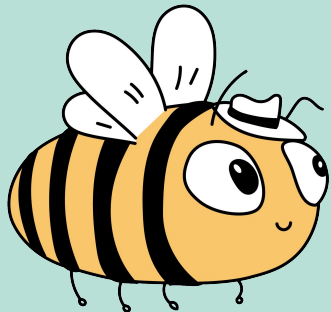
Oslo



Foto: Origo v/Håkon Lexberg



**Bzzzzz - spørsmål?**



Oslo





# "Dugnad" i Gamle Oslo

Forum for personvern og informasjonssikkerhet

01.03.2023



# Hei!



**Tommy Haugen Svela**  
Fagleder IKT



**Ida Marie Larsen**  
Personvern- og informasjonssikkerhetskoordinator

# Hvor skal vi starte?

- Omfattende kartlegging
- Behov: rydde i eget hus, kontroll og oversikt selv, lovpålagt å ha en behandlingsoversikt
- Excel, Kartotek – systemoversikt, innovativ og oppfinnsom bydel

# Behandlingsoversikt



# Gode erfaringer

- Personvern og IT =  sant
- Godt å være to
- Større kompetanse og oversikt sammen



# Hvordan forbedre og lykkes?

## Forankring, samarbeid og deling

---

- Eieforhold og forankring
- Veikart
- Bruke LG «ledelsens gjennomgang» og VE «virksomhetsleders egenerklæring» aktivt i virksomhetsstyringen
- Etterlevelse og sikre kontinuitet
- Tverrfaglig samarbeid



Sharing is caring



Steal with pride



Oslo

# Åpen mikrofon – har du erfaringer eller problemstillinger du vil dele i forumet i dag?

- ▶ Ta ordet 
- ▶ Skriv inn i ordskyen 
- ▶ Bruk chatten 



# Hva er det som rører seg hos dere for tiden?



Samtykke  
Deling av personopplysninger  
**DPIA (4)**

**Vurdering av  
personvernkonsekvenser (3)**  
**Behandlingsoversikten (8)**

Behandlinger  
Utvikle/anskaffe gode løsninger som ivaretar  
personvern  
GPDR-utfordringer  
Samtykke

**Kameraovervåking (2)**

Brukerroller

Revisjon

Deling av data/informasjon  
Egnete kanaler for deling

digitalisering  
rekruttering ISK  
Transfer Impact Assessment  
Økt bevissthet  
Øvelser  
Policy  
Ressurser

**ROS (4)**

Risikostyring  
Systemoversikt og ansvar

**Systemadministrasjon (3)**

Systemforvalterrollen internt  
**Tilgangsstyring (3)**  
Risikobildet

# Avslutning

- ▶ Årets forum – du kan melde deg på nå!
  - Se her: <https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/kompetanse/forum-for-informasjonssikkerhet-og-personvern/>
- ▶ Vi søker nye medlemmer til programgruppa til forum.
  - Bli med! <https://forms.office.com/e/FB4035fKsV>
- ▶ Møte i uke 12 med koordinatorene om Sikkerhetsmånedens
  - Følg med i din innboks

## Forum 2023

~~01. mars~~

19. april

7. juni

6. september

29. november

