Forum for informasjonssikkerhet og personvern

18.11.2020

Velkommen – vi starter klokken 0900

Oslo

0900-0905	**Velkommen**
0905-0930	Innføring av digitalt tilsyn på Økernhjemmet – en humpete vei til målet ved Linn Skorge fra Sykehjemsetaten
0930-1000	Erfaringer med gjennomføring av DPIA ved Anette Engum, Personvernombud Bærum kommune
1000 - 1005	Pause
1005 -1015	Resultater fra Sikkerhetsmåneden 2020 ved Maylén Mago Pedersen, spesialrådgiver i seksjon for informasjonssikkerhet og IKT.
1015-1055	Hvordan utforme krav til informasjonssikkerhet i en IKT-anskaffelse - demonstrasjon av verktøy ved Amin Ben Karroum, spesialrådgiver i seksjon for informasjonssikkerhet og IKT.
1055-1100	Avslutning

BÆRUM KOMMUNE

Vurdering av personvernkonsekvenser (DPIA) - Erfaringer fra Bærum kommune

Anette Engum, personvernombud

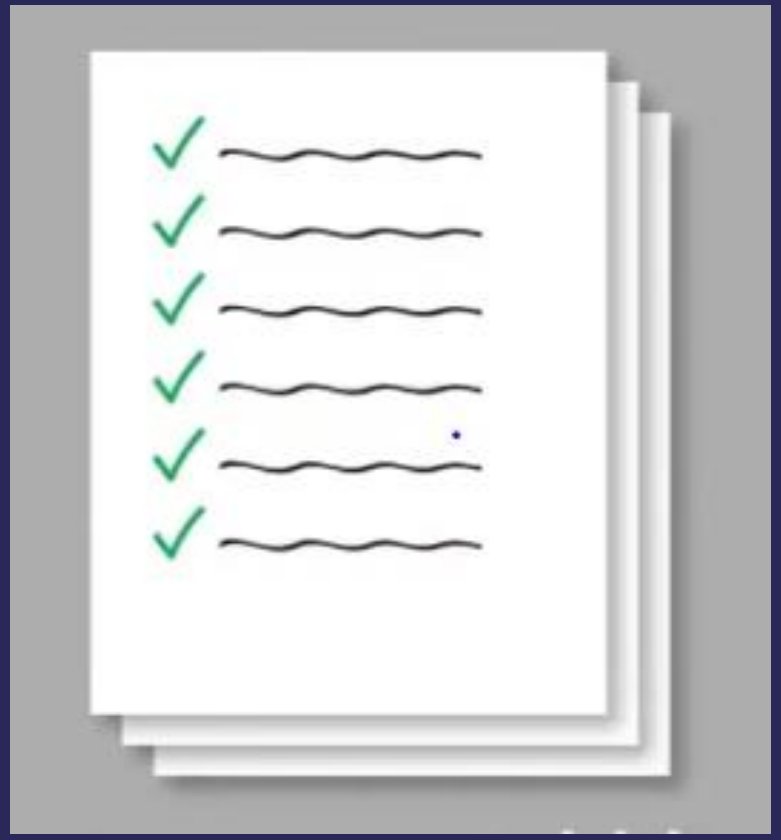
Sammen skaper vi fremtiden

MANGFOLD - RAUSHET - BÆREKRAFT

Vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA)

- *Dersom det er **sannsynlig** at en **type behandling**, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens **art, omfang, formål og sammenhengen den utføres i**, vil medføre en **høy risiko** for fysiske personers **rettigheter og friheter**, **skal** den behandlingsansvarlige **før** behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.»* (Art. 35.1)

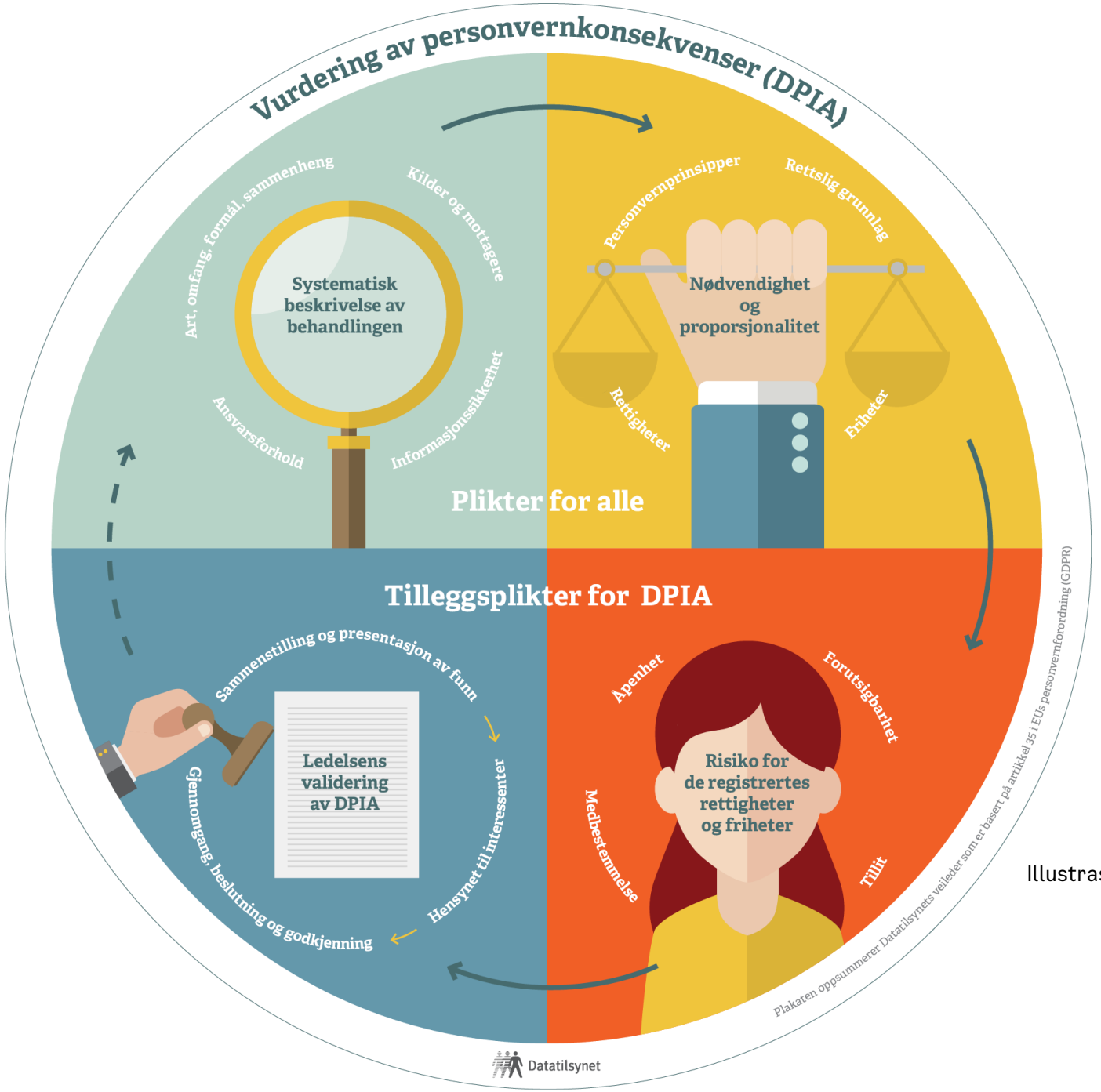
Personvernsjekk



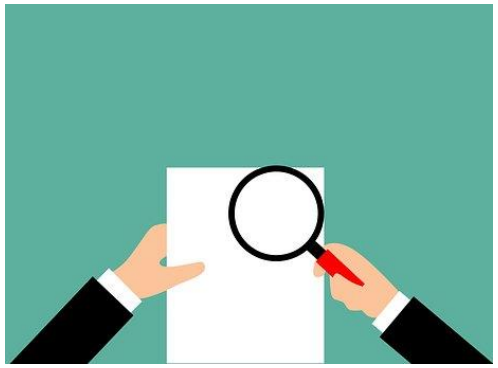
Oslo

Prinsipper for behandling av personopplysninger (personvernforordningen art. 5)

- Lovlighet, rettferdighet og gjennomsiktighet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og fortrolighet
- Ansvarlighet



Illustrasjon fra Datatilsynet.no



Verktøy for mobbekartlegging i skole

- «Behandling av personopplysninger for å evaluere læring, mestring og trivsel i skoler eller barnehager»
- Systematisk monitorering og sårbare registrerte

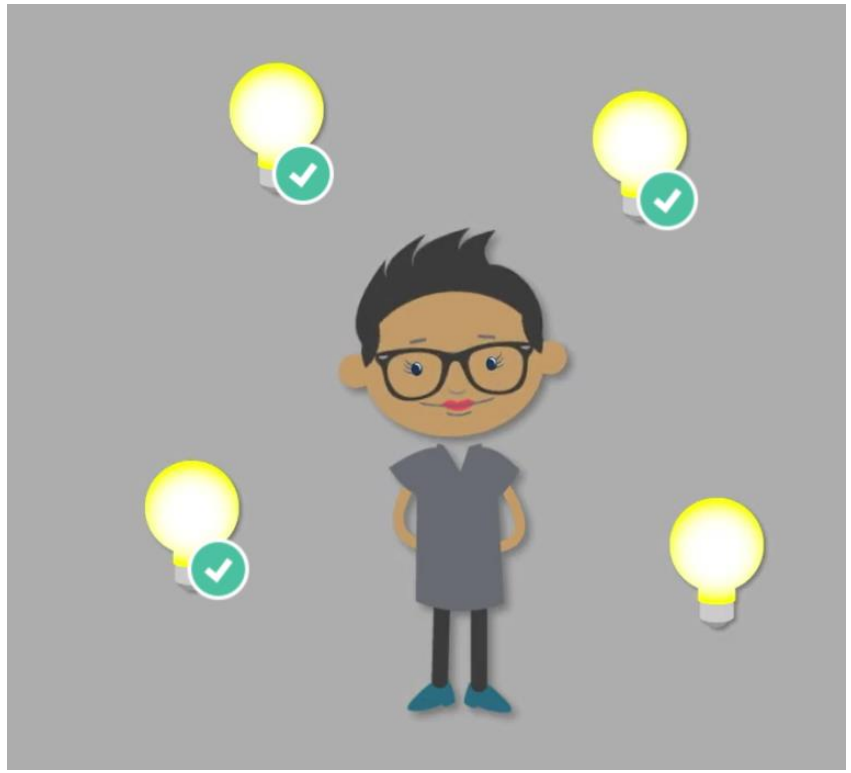
✓ **Krever at det gjennomføres DPIA (art. 35 nr. 4)**

Personvernombudets oppgaver ved DPIA
Art. 39 nr. 1. c)

- på anmodning gi råd om vurderingen av personvernkonsekvenser

- kontrollere gjennomføringen av den

På anmodning gi råd om vurderingen av personvernkonsekvenser…



- Det er den behandlingsansvarlige som har ansvaret for at DPIA gjennomføres (ikke PVO)
- Den behandlingsansvarlige kan be om råd om:
  - det er behov for å utføre en DPIA
  - DPIA skal gjøres internt eller ved hjelp av eksterne
  - hvilke sikkerhetstiltak (tekniske og organisatoriske) som kan minimere risikoen
  - hvorvidt vurderingene har blitt gjennomført på riktig måte, og om konklusjonene er i tråd med regelverket
  - hvilken metode som skal benyttes

Verktøy for DPIA

- Kombinasjon av prosa og excel
- Systematisk beskrivelse (behandlingens formål, grunnlag, art, omfang, kontekst, nødvendighet og proporsjonalitet, ivaretakelse av rettigheter/friheter)
- Konsekvensutredning del I: Identifisere risikoer for den registrertes friheter og rettigheter (scenario/hendelser)
- Konsekvensutredning del II: Tiltak for å redusere risiko
- Rapport med vurdering/konklusjon

Ledelsen vurderer hvorvidt de planlagte tiltakene, restrisikoen og handlingsplan er akseptabel

Kontrollere gjennomføringen…

- Hvilken rolle skal personvernombudet ha i prosessen?

- Være med selv eller gjennomgå rapport?
- Uavhengighet
- Gi råd om vurderingen av personvernkonsekvenser – skal ikke godkjenne
- Hvem skal delta i DPIA?

DPIA i Bærum kommune

- Gjennomfører **initial** vurdering ved alle nye behandlinger av personopplysninger
- Deltakere ved DPIA:
  - Prosjektleder (ved prosjekt)
  - Behandlingsansvarlig repr. (ansvarlig for gjennomføring)
  - Superbruker/ressurs (med inngående kunnskap om behandlingen)
  - Personvernombudet (rådgiver underveis og kontrollerer gjennomføring)
  - Fasilitator
  - Andre deltakere ved behov (eksempelvis IT-sikkerhet, databehandler, andre fagpersoner)
  - De registrerte (eller representanter) dersom det er relevant

Synspunkter fra de registrerte

- Dersom det er relevant (…) innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representanter
- Ulike roller kan ha ulike forventninger om hvordan data blir benyttet
- Hvordan gjøres det i praksis?
- Når involveres de i prosessen?
- Har benyttet bl.a. ungdomsrådet som representant for elevene. Har hatt med både foresatte som jobber i skolene, foresatte som ikke jobber i kommunene, lærere/miljølærere, hovedtillitsvalgte
- Innbyggerutvalg

Oslo

Fra DPIA Verktøy for mobbekartlegging:

«Elev»

«Synes muligheten for innsyn er for begrenset, og bør følges opp med leverandør»

«Det har vært en grundig gjennomgang og fornøyd med at det er ulike representanter med i DPIA»

«Foresatt»

Oslo

Ledelsens validering av DPIA

Ledelsen vurderer hvorvidt de planlagte tiltakene, restrisikoen og handlingsplanen er akseptabel

- Godkjent = Behandling kan starte opp.
- Betinget av forbedringer = Revidert DPIA skal fremlegges på nytt for ledelsen.
- Avvist: Virksomheten beslutter å ikke gjennomføre behandlingen.

Når DPIA er behandlet i ledergruppen mer enn én gang og risikoen fremdeles er høy = forhåndsdrøftelse med Datatilsynet.

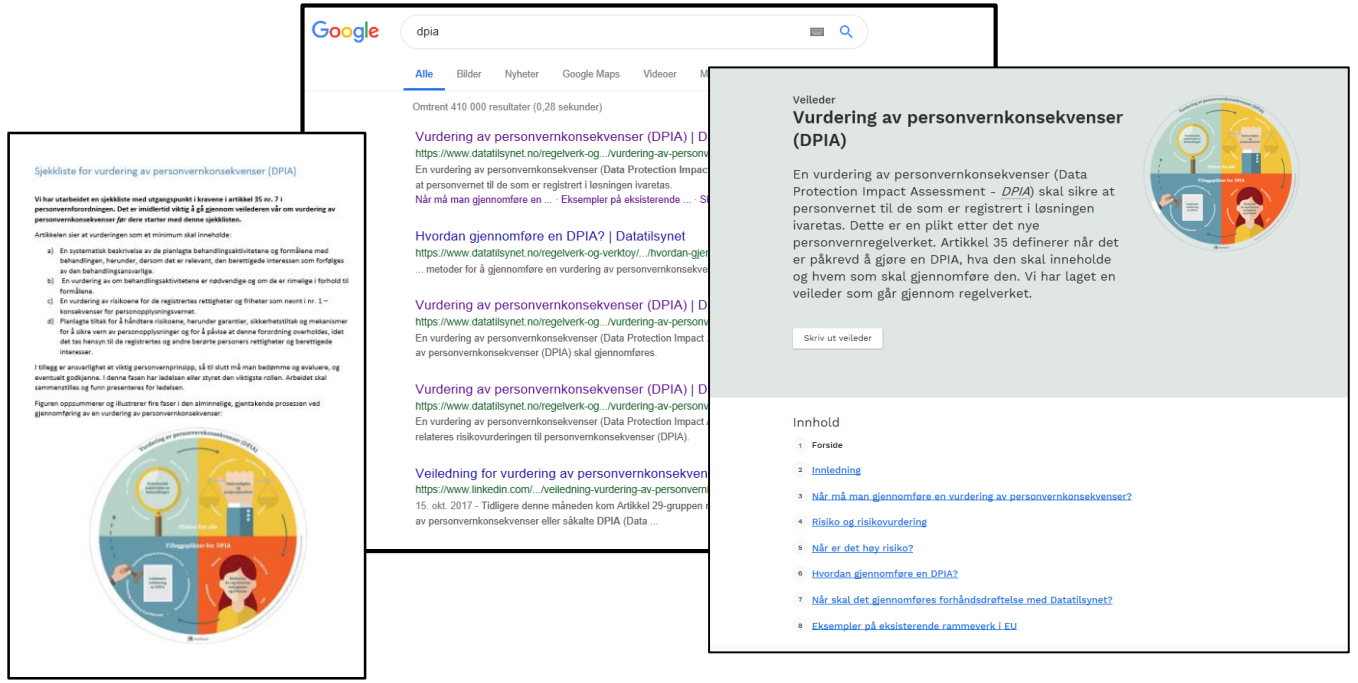
Forhåndsdrøftelse - Datatilsynet

- Dersom man planlegger behandlinger med høy *risiko* for de registrertes rettigheter og friheter og ikke klarer å redusere risikoen, må virksomheten rådføre seg med Datatilsynet før behandlingen starter
- En forhåndsdrøftelse er en skriftlig, formalisert prosess
- Kan resultere i at:
  - Datatilsynet ber om ytterligere informasjon, eksempelvis hvordan opplysningene er tilstrekkelig sikret eller hvordan den ansvarlige har vurdert krav om *innebygd personvern* og personvern som standardinnstilling
  - Datatilsynet gir skriftlige råd
  - Det gis pålegg, advarsler, irettesettelser, gjøres stedlig *tilsyn* eller behandlingen forbys

Erfaringer

- Ressurskrevende, men viktig prosess
- Kan være en utfordring å få med den registrerte/representant
- Avgrensning av formål – hva er det som vurderes, hvem er de registrerte, hva er hjemmelsgrunnlaget
- Omfang: 3-4 møter, 5-7 timer totalt (+/-)
- Får stort sett positive tilbakemeldinger, stort engasjement
- Kompetanseheving av ansatte, bidrar til bedre informasjonssikkerhet på tvers av kommunen, øker bevissthet i organisasjonen
- Kobling til andre virksomhetsprosesser – behandlingsoversikt, ROS, virksomhetsstyring
- Viktig med god forankring!

Tips og triks



- Finn et godt verktøy (Husk at ingen DPIA verktøy er hugget i stein!)
- Ta gjerne utgangspunkt i Datatilsynets veileder og sjekkliste
- Tilpass til din virksomhet!
- Viktig å avgrense analysen – hva er det som vurderes?
- Fordel med risiko- og sårbarhetsanalyse først
- Sluttrapport – synliggjør hva skal ledelsen ta stilling til / restrisikoen

Hva ble resultatet av DPIA for verktøy for mobbekartlegging?

- Kommunalsjefen for skole ble forelagt analysen med restrisiko
- Redusert risiko betinget av både tekniske og organisatorisk tiltak – bl.a. rutiner for gjennomføring, pulter fra hverandre, sette inn forsterket lærer ++
- Kommunalsjefen valgte å avvente å benytte verktøyet inntil alle tiltak er på plass

Pause til klokken 10.10

Forum for informasjonssikkerhet og personvern

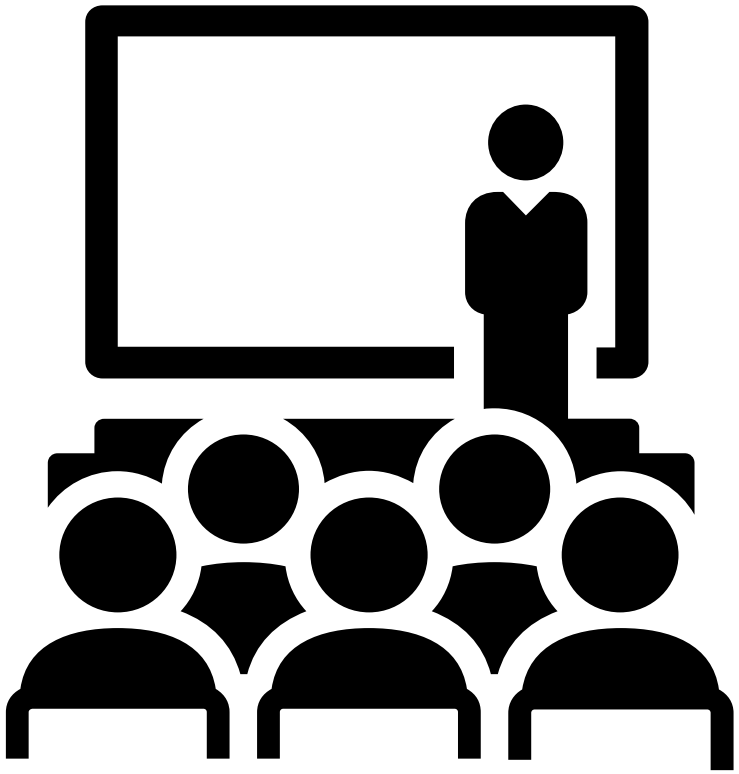
Oslo

Oslo

Resultater fra Sikkerhetsmåneden 2020

Forum 18.11.2020
Maylén Mago Pedersen

Digitale arrangementer



Alle seminarene ble avholdt digitalt, med tilgjengeliggjøring av opptak i ettertid

Vi hadde god deltakelse og høy oppslutning på seminarene.

Antall påmeldte:

- **Åpning av Sikkerhetsmåneden:** 280 påmeldte
- **Tim Talk i Sikkerhetsmåneden:** 240 påmeldte
- **Tim Talk i Sikkerhetsmåneden:** 225 påmeldte
- **Avslutning av Sikkerhetsmåneden:** 272 påmeldte

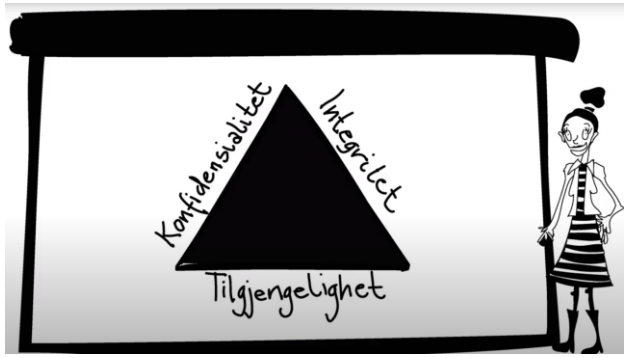
Antall påmeldte i 2019:

152 deltakere
106 deltakere
143 deltakere
80 deltakere

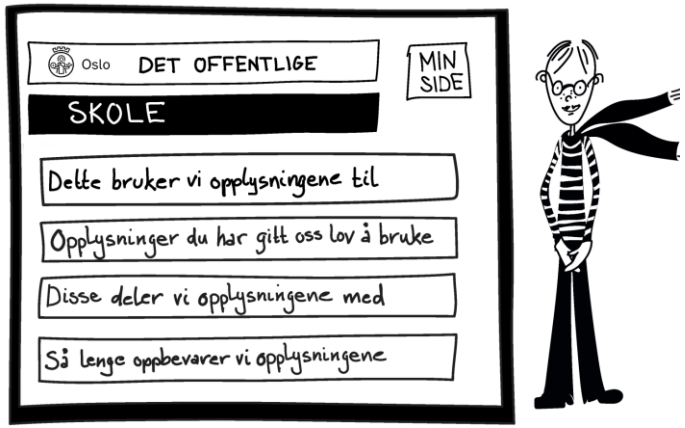
Mange av de som var påmeldt deltok ikke på arrangementene, vi er allikevel fornøyd med å ha økt antallet deltakere og interesse rundt arrangementene.

Vi har alt i alt fått positive tilbakemeldinger på innhold og innledere.

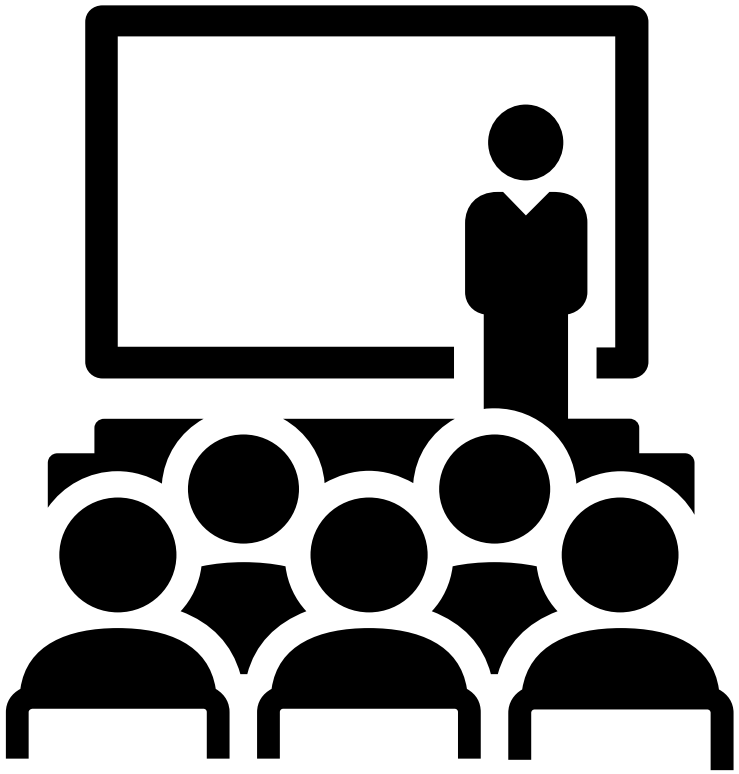
Vi har lansert Tim-film om informasjonssikkerhet og personvern



https://www.youtube.com/watch?v=shKkAoGvTTk



Digitale innføringskurs



Vi tilbød to kurs med alle ansatte som målgruppe. Disse kussene ble holdt på Teams.

Også her hadde vi god deltakelse og høy oppslutning.

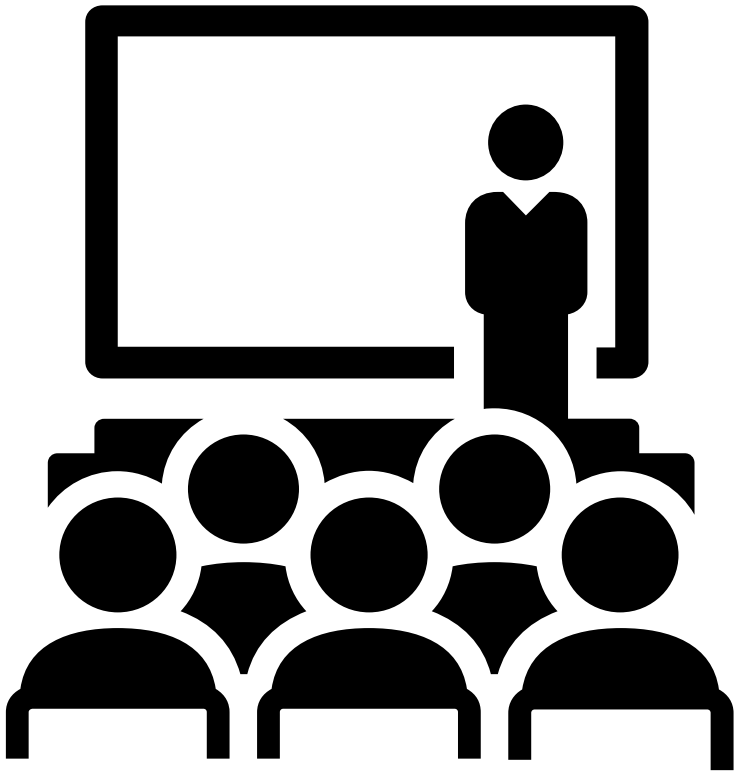
- Innføring i personvern
  - Over 300 påmeldte, ca. 200 som deltok
- Innføring i informasjonssikkerhet
  - 300 påmeldte, ca. 200 som deltok

Også her har vi alt i alt mottatt positive tilbakemeldinger fra deltakerne

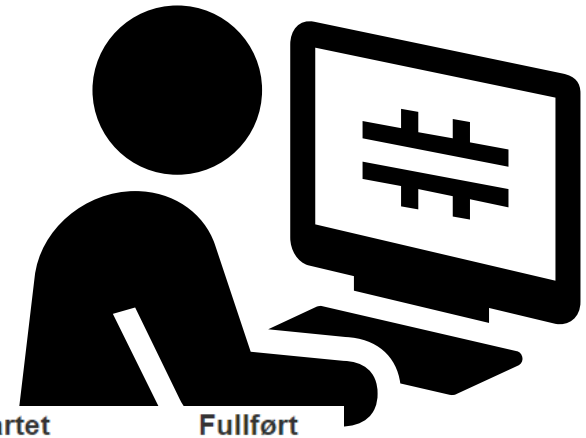
Lederforedrag - Virksomhetene kunne bestille fra oss

Avholdt på Teams med ledere fra virksomhetene

- Et trusselbilde i rask endring – hva betyr det for deg som leder?
  - 5 foredrag
- Personvernregelverkets irrganger – hvordan ha oversikt som leder?
  - 7 foredrag
- 8 virksomheter bestilte foredrag



E-læringer/nanolæringer



- Sendt på epost til 52 136 ansatte
- E-læringer á 2-5 minutter hver tirsdag i oktober

			Startet	Fullført
Velkommen til Sikkerhetsmåneden 2020	13 %	90 %	6740	6034
Beskytt de viktige brukerkontoene dine	12 %	94 %	6448	6081
"Hurra, det er gratis Wi-Fi her!"	13 %	93 %	6759	6311
Enkle tips som hjelper deg å avsløre en svindel	12 %	93 %	6395	5969
Personvernsmyter	12 %	93 %	6092	5690

- Sendte påminnelse 3.november.
- Sendt overordnet statistikk for e-læringene hver uke til postmottakene
  - Virksomheter som har bedt om det får tilsendt detaljert statistikk

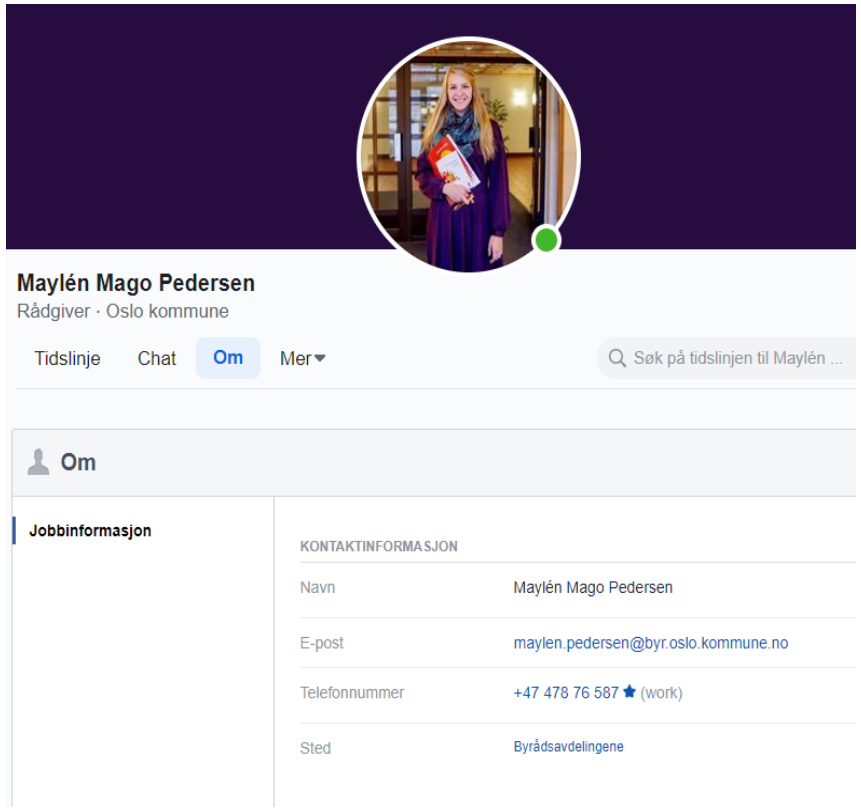
Endring av låseskjermer på Oslo felles i oktober

Workplace

- Økt antall medlemmer som følger gruppen SAM/Informasjonssikkerhet og IKT fra 1003 til 1130 (04.11.2020)
- Innhold
  - Tre poster på Oslo/Alle i Oslo kommune
    - Videoer med byråden for finans
    - Tim-film
  - To poster på Oslo/nyheter i Oslo kommune
    - En bilde/video konkurranse med 28 liker-klikk og 95 kommentarer
    - En quiz med 250 deltakere
  - 19 poster i SAM/Informasjonssikkerhet og IKT
    - Påminnelser om aktiviteter og e-læringer
- Stort engasjement rundt aktivitetene

Spørsmål eller innspill?

- Ta kontakt med oss på e-post: maylen.pedersen@byr.oslo.kommune.no eller send meg en melding på Workplace



Adressere informasjonssikkerhet i IT-anskaffelser

Amin Ben Karroum
Spesialrådgiver informasjonssikkerhet

Byrådsavdeling for finans
Seksjon for informasjonssikkerhet og IKT

Oslo

Agenda

- Når skal informasjonssikkerhet adresseres i en anskaffelse
- Roller og ansvar
- Sammenheng mellom risikovurdering og sikkerhetskrav
- Verktøy til kravspesifisering av IT-løsninger
- Andre relevante verktøy

Hvordan ser en typisk anskaffelse ut?

Avklare behov og forberede konkurransen (behovsfasen)

Gjennomføring av konkurranse

Kontraktsoppfølgning

Avklare roller og ansvar

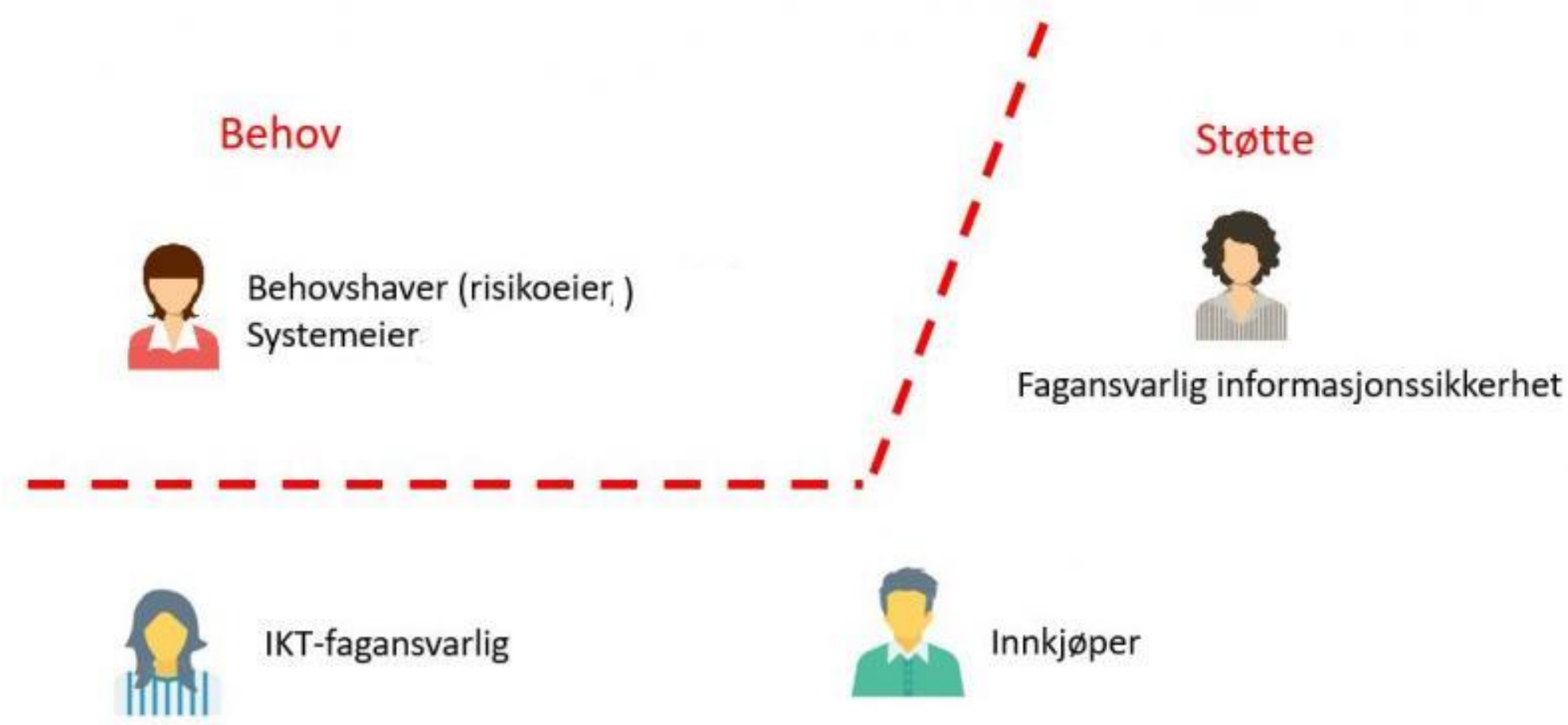
Risikovurdering

Sikkerhetskrav

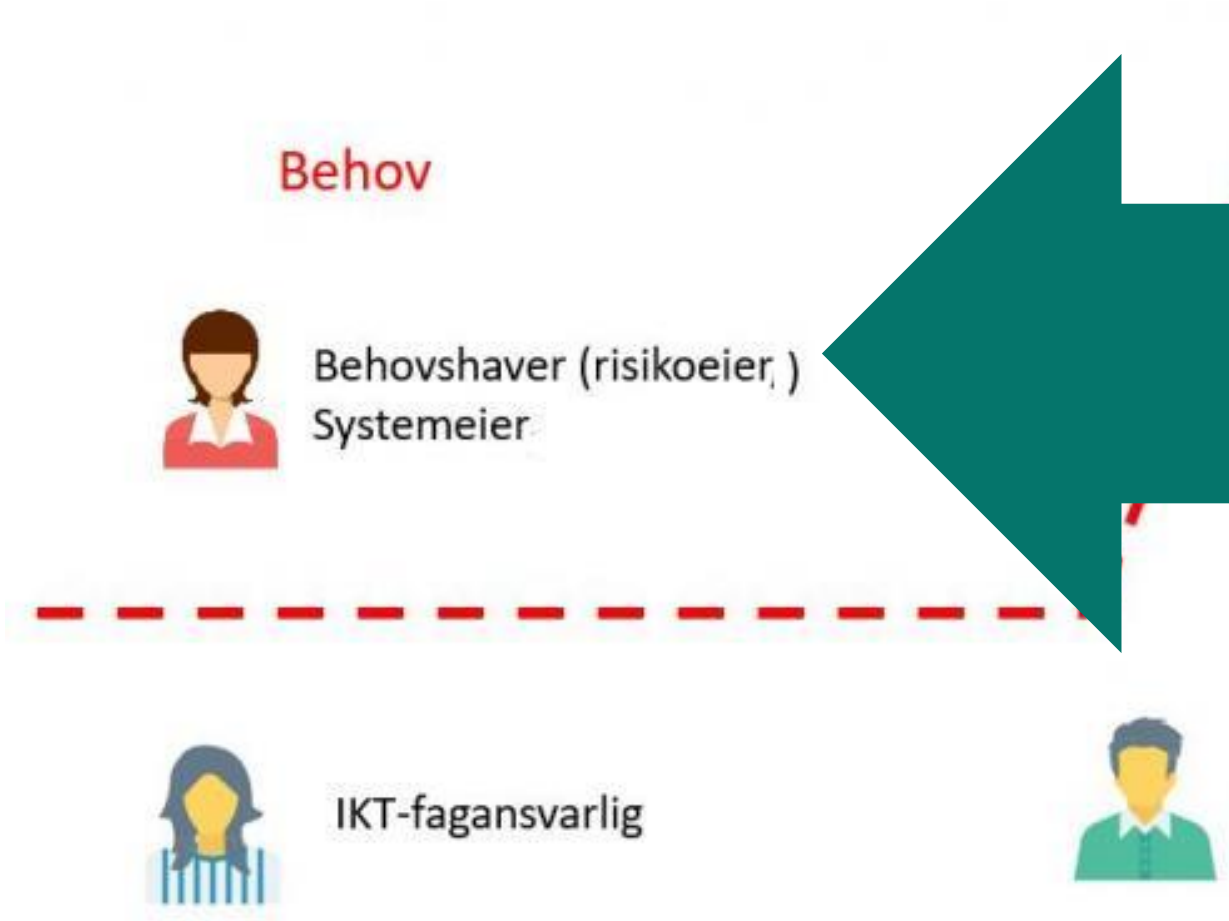
Avklare roller og ansvar

- Hvem har anskaffelseskompetanse?
- Hvem skal spesifisere krav til funksjonalitet?
- Hvem skal spesifisere krav til tekniskarkitektur?
- Hvem skal spesifisere krav til informasjonssikkerhet?
- ....

Avklare roller og ansvar



Avklare roller og ansvar



Ansvarlig for å:

- utrede behov
- ha oversikt over relevant regelverk for tjenesten
- ha oversikt over informasjonen som behandles i tjenesten og i systemet
- Ansvarlig for å styre risiko i arbeidsoppgaven. Dette innebærer å:
- identifisere og vurdere risiko for informasjonssikkerhetsbrudd i tjenesten
- beskrive behovet for sikkerhet i arbeidsoppgaven og systemet
- sørge for riktig beslutning på riktig nivå når det gjelder valg av sikkerhetstiltak
- eskalere håndtering av risiko dersom nødvendig
- informere innkjøper om behov og sikkerhet

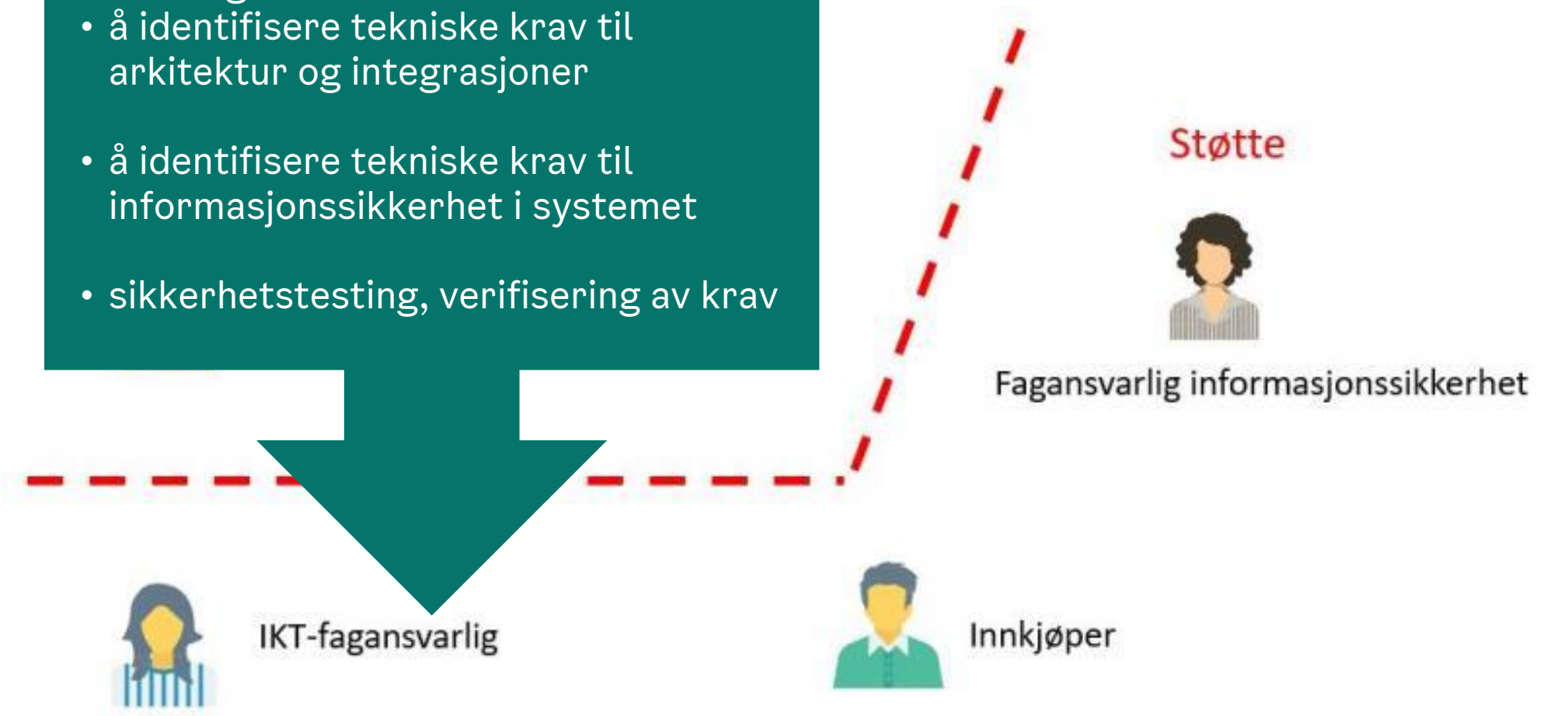
Avklare roller og ansvar

Ansvarlig for å støtte linjeleder i arbeidet med:

- risikovurderinger for tjenesten og tiltenkte systemet
- å beskrive sikkerhetsbehov for systemet

Avklare roller og ansvar

Ansvarlig for:
- å identifisere tekniske krav til arkitektur og integrasjoner
- å identifisere tekniske krav til informasjonssikkerhet i systemet
- sikkerhetstesting, verifisering av krav



Avklare roller og ansvar

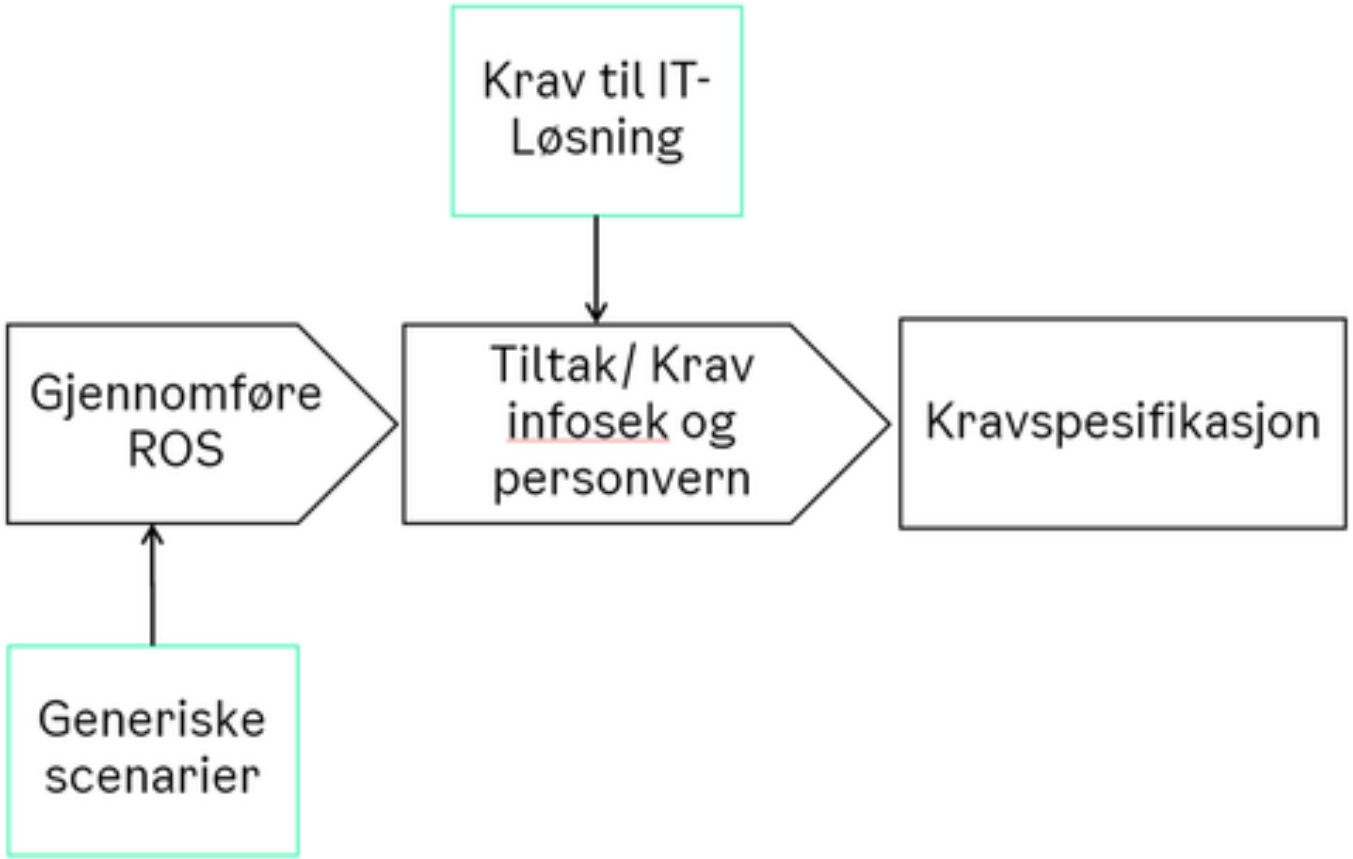
Risikovurdering

- Identifisere relevante risikoscenarier ved bruk av løsningen og tjenesten
- Analysere scenarier og fastslå risikonivå
- Identifisere tiltak for å oppnå akseptabel risiko

Sikkerhetskrav og risikohåndtering

- Omskrive tiltak til krav til løsning og legges ved konkurranseunderlaget
- Inkludere Oslo kommune databehandleravtalen

Verktøy til kravspesifisering av IT-løsninger



DEMO

Skal din virksomhet gjennomføre en anskaffelse?

- Vi ønsker å teste ut verktøyet og eventuelt videreutvikle.
- Vi ber om at 1-2 pilot-prosjekter/anskaffelser som ønsker å teste verktøyet og dele deres erfaringer melder ifra.

Verktøy

- **Verktøy til kravspesifisering av IT-løsninger**: Felles intranett> Informasjonssikkerhet og personvern> Informasjonssikkerhet> Sikkerhets- og personvernskrav til IT-løsninger
- **Rollekort**: Felles intranett> Informasjonssikkerhet og personvern> Informasjonssikkerhet> Styringssystem og Internkontroll> Roller og Ansvar
- **Risikovurderingskurs**: Vurderes å gjennomføres i vinter
- **Verktøy for risikovurdering**: Felles intranett> Informasjonssikkerhet og personvern> Informasjonssikkerhet> Risikostyring
- **Anskaffelsesveileder**: UKE intranett> Kundeportal> Veiledere> Anskaffelsesveileder
- **Veiledning av DFØ/DIGDIR**: Anskaffelser.no> Hva skal du kjøpe> IT

Spørsmål?

Ønsker virksomheten din å delta som pilot? Send epost amin.karroum@byr.oslo.kommune.no

Avslutning

24.november: **Innføring i prinsipper for behandling av personopplysninger**

Målgruppe: alle ansatte
Klokken 11 - 13

08.desember: **Innføring i grunnprinsippene i internkontroll/styringssystem for personvern og informasjonssikkerhet**

Målgruppe: Personvern- og informasjonssikkerhetskoordinatorer og virksomhetsledere
Klokken 12 - 14