Oslo

Personvern- og informasjonssikkerhetsforum

Vi starter klokken 0900

Kjøreregler

- Mange deltagere i dag, skru av lyden underveis og rekk opp hånda eller skriv spørsmål eller kommentarer i chatten.
- Vi vil stoppe noen ganger underveis for å svare på spørsmål.
- 10 minutter pause ca. kl. 10.05

0900	**Velkommen og introduksjon til dagens program** ved Randi Blystad
0905-0920	Introduksjon av nyansatte i ISI og kort om hva de skal jobbe med Siri, Siril, Erling, Lars Martin, Susanne, Edgar, Vidar og Cecilie
0920-0930	Hva skjer på personvernområdet v/Maryke Silalahi Nuth
0930-0940	Hva skjer på informasjonssikkerhetsområdet v/Åsmund Skomedal
0940-0950	Angrepet på Østre Toten kommune og hva gjør Oslo kommune for å unngå å havne i samme situasjon? v/Geir Faremo
0950-1005	Presentasjon av oppdaterte rollekort koordinatorene v/ Atle Halvorsen Hjelkerud og Ivar Aasgaard
1005-1015	Pause til å fylle kaffekoppen
1015-1050	Hva er status med arbeidet etter Schrems II dommen og veileder fra Det europeiske personvernrådet (EDPB) v/Linda Mari Knutsen og Åsmund Skomedal
1050 - 1100	Datoer for neste forum, programgruppe til forum, m.m. v/Maylén Mago Pedersen

Hva skjer på personvernområdet?

Maryke S. Nuth
Fagsjef personvern
maryke.nuth@byr.oslo.kommune.no

Foto: Benjamin Pham

Håndheving av GDPR i EU/EØS 2018-2021

- Ikke tilstrekkelig tekniske og organisatoriske tiltak for å oppnå sikkerhetsnivå som er egnet med hensyn til risikoen
- Ikke tilstrekkelig rettsgrunnlag for behandling av personopplysninger
- Manglende etterlevelse av personvernprinsippene
- Ikke tilstrekkelig ivaretakelse av den registrertes rettigheter (GDPR art. 12, 15 og 17)
- Manglende avviksmelding til tilsynsmyndigheter
- Mangler i databehandleravtale
- Ikke etablert personvernombud

Norske saker publisert av EDPB eller Datatilsynet (des 2020 – mars 2021)

Ikke tilstrekkelig tekniske og organisatoriske tiltak

- Indre Østfold kommune: EUR 20,000
- Telenor AS: irettesettelse (*reprimand*) omfatter også manglende avviksmelding til Datatilsynet

Ikke tilstrekkelig rettsgrunnlag

- Lindstrand Trading AS: EUR 10,000
- Aquateknikk AS: EUR 10,000
- Gveik AS: EUR 7,500
- Grindr LLC: varsel om overtredelsesgebyr på EUR 10 millioner

Manglende etterlevelse av personvernprinsippene og ikke tilstrekkelig rettsgrunnlag

- Ikke navngitt virksomhet: EUR 25,000
- Cyberbook AS: EUR 20,000
- Ikke navngitt virksomhet: EUR 40,000
- Coop Finnmark: EUR 40,000

Hva gjør Oslo kommune (FIN) Q1-Q2 2021?

Veiledere

- Personvern
- Behandlingsgrunnlag
- Innsyn, retting og sletting

Maler

- Overordnet personvernvurdering
- DPIA
- Vurdering av høyrisikonivå ved avvikshåndtering

Vurderinger

- Plassering av behandlingsansvar

Oslo

Informasjonssikkerhet

Aktiviteter i FIN

Åsmund Skomedal
Fagsjef informasjonssikkerhet
asmund.skomedal@byr.oslo.kommune.no

Aktiviteter innen informasjonssikkerhet (I)

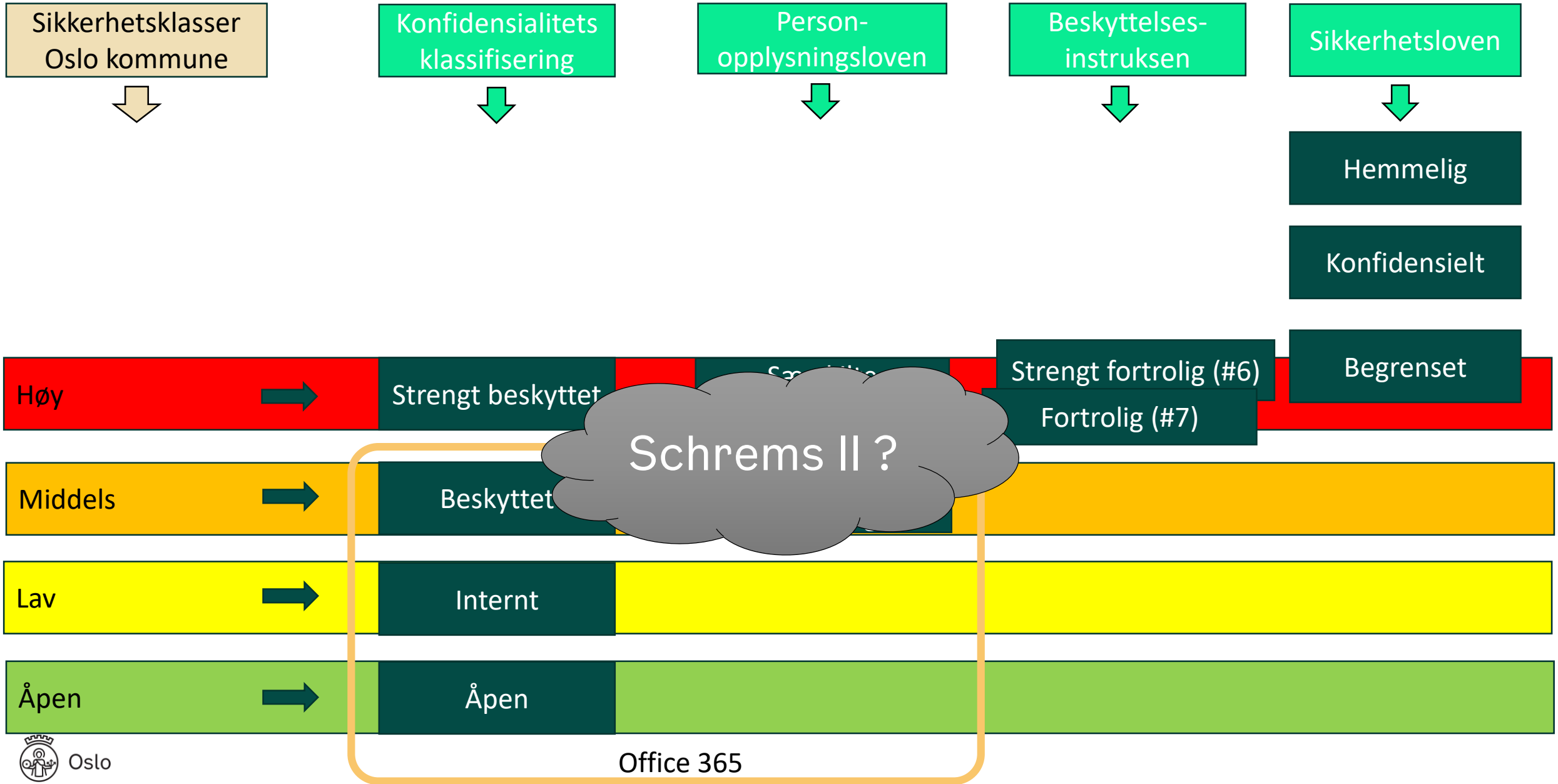
- Oppsummering av Ledelse Gjennomgang og Virksomhetenes Egenerklæring (LG/VE)
  - Normalt i form av et Byrådsnotat
- Oppdatering av Rollekort, mer litt senere
  - Personverkskoordinator (PVK) og Informasjonssikkerhetskoordinator (ISK)
  - Revisjon av øvrige roller
- Skal din virksomhet anskaffe en IT-tjeneste/skytjeneste?
  - Utprøving av verktøy for sikkerhet i anskaffelser pågår i disse dager
  - Fokus er på behovskartlegging og risiko
  - Vi ønsker flere *frivillige* virksomheter i pilotfasen;
    ta kontakt med amin.karroum@byr.oslo.kommune.no

Aktiviteter innen informasjonssikkerhet (II)

- Overordnet styringssystem for informasjonssikkerhet
  - Integrerer også personvern i samme kravsettet (altså elementer fra ISO 27 700)
  - Tre (av tolv) tema nærmer seg ferdig, deretter godkjenningsprosess
  - Tre nye tema er påbegynt

- Klassifisering av informasjon v1.0 foreligger
  - En gradvis innføring
  - Blir en integrert del av Office 365 (først i piloter, deretter i øvrige virksomheter)
  - Planen er å inkludere klassifiseringen i overordnet styringssystem
  - Fire konfidensialitetsklasser; «Åpen» – «Intern» – «Beskyttet» – «Strengt beskyttet»

Konfidensialitetsklasser v1.0 (pr. februar 2021)



Oslo

Nyttige lenker

Styrende dokumenter:

https://felles.intranett.oslo.kommune.no/styrende-dokumenter-avtaler-og-regelverk/informasjonssikkerhet/

Anskaffelsesveileder:
UKE intranett> Kundeportal> Veiledere> Anskaffelsesveileder

Oslo

Angrep på Østre Toten

Hva gjør Oslo kommune sett fra et systemeierperspektiv?

Geir Faremo
Fagsjef IKT byrådsavdeling for Finans
03.03.2021

Foto: Thomas Ekström

Oslo

Agenda

- Tidslinje
- Litt om angrepet på Østre Toten
- Hva gjør Oslo kommune?

Tidslinje

09.01.2021
- Angrep på Østre Toten
- Omtales i media
- Settes høyt på dagsorden

11-12.01.2021
- FIN enes om et håndnotat
- Måten å informere
  - Byråd
  - Kommunaldirektør
- Samarbeid FIN og UKE
- Byråden vurderer å informere videre
  - Hyppige oppdateringer

25.01.2021
- FIN tar initiativ til oppdatering av håndnotat
- Samarbeid FIN og UKE

08.02.2021
- KS Sender ut anbefalinger
- FIN følger opp mot UKE
- FIN vurderer info til alle virksomheter

15.02.2021
- FIN blir bedt om en ny oppdatering av håndnotat
- Samarbeid FIN og UKE

03.03.2021
- Jevnlig oppfølging
- Østre Toten anslår at de trenger 6 mnd før de er i full drift

Østre Toten

- Hva skjedde
  - Alle filer kryptert
  - Backup kryptert eller slettet
  - Store mengder data på avveie
    - Mulig sensitiv persondata
  - Ingen fagsystemer virker
  - Politiske prosesser stoppet opp
- Aktør
  - Økonomisk vinning
  - Profesjonell tilnærming
  - Bruker lang tid på infiltrering
- Konsekvens
  - Ansatte fikk epost 19.01.2021
  - Ny digital infrastruktur etableres
  - Ekstern bistand leid inn
  - Setter ut drift til ekstern leverandør
  - Fagsystemer oppe om 6 måneder
  - Har kostet kommunen 6. millioner til nå
    - Sluttsummen blir langt høyere
- Saken er under etterforskning

Hva gjør Oslo kommune?

- UKE følger opp NSMs anbefalte tiltak
- UKE følger opp leverandører og deres tiltak
- UKE og leverandører har ikke funnet spor etter et tilsvarende angrep mot Oslo kommunes felles IKT-plattform
- UKE har ekstern backup
- Løpende deling av etterretningsinformasjon.

- CSIRT informerte Oslo kommune om trusselen på Workspace
- Det vurderes løpende andre risikoreduserende tiltak
  - Det kan være behov for umiddelbare tiltak som vil berøre tilgjengelighet og funksjonalitet for enkelte brukermiljøer.
- Styrking av sikkerhetsløsningene er et vesentlig element i all videreutvikling og modernisering av Felles IKT-plattform.

Mer om Østre Toten

- Ivar Aasgaards innlegg:
  - Foreningen kommunal informasjonssikkerhet (KiNS)
  - "En kommune sin opplevelse av å være under angrep" - presentasjon av dataangrepet på Østre Toten kommune og situasjonen i kommunen i dag v/ kommunedirektør Ole Magnus Stensrud, Østre Toten kommune, er tilgjengelig frem til 23. mars»
  - https://oslo.workplace.com/groups/informasjonssikkerhetoglKT/permalink/1661757670691119/

Oslo

Rollekort
PKO og ISK

Ivar Aasgaard
Atle H. Hjelkerud

3. mars 2021
Personvern- og
informasjonssikkerhetsforum

Foto: Benjamin Pham

Generelt om rollekort

- Enkle veiledere med fokus på oppgaver, knyttet til ulike rolle, basert på styrende dokumenter.
- Laget for daværende EHA-sektoren (obligatorisk).
- De fleste rollekortene er nå tre år gamle (oppdatering pågår).
- Med mindre rollekortene er gjort obligatoriske i den enkelte sektor, er de frivillige å ta i bruk.
  - Oppgavene i rollekortene kan tilpasses den enkelte virksomhets interne fordeling av roller og ansvar.
- Rollekortene ligger på felles intranett – under «Informasjonssikkerhet og personvern».

Rollekort for informasjonssikkerhetskoordinator (ISK) og personvernkoordinator (PKO)

- Bakgrunn: Krav om å opprette rollene informasjonssikkerhetskoordinator og personvernkoordinator i alle virksomheter (jf. tildelingsbrev 2020).
- Rollekort for ISK eksisterte fra før av – dette er nå revidert.
- Rollekort for PKO er nytt.
- Ikke eget rollekort for den kombinerte rollen PISK.
- Rollekortene er utarbeidet/revidert samtidig, slik at de har lik oppbygging.
- Utkast ble sendt til noen ISKer/PKOer i ulike sektorer for tilbakemeldinger. Rollene må gå seg til – vil bli nødvendig å oppdatere rollekortene senere.
- Fokus på oppgaver – ikke ansvar (ettersom ansvar ikke kan delegeres).

Rollekort for ISK

- Hovedsakelig språklige og strukturelle endringer.
- Personvernbiten er tatt ut – flyttet til eget rollekort.
- Tydeliggjort oppgave med bistand til flere prosesser, herunder anskaffelser.
- Tatt inn eget punkt om at ISK skal være kontaktperson (innen informasjonssikkerhet) overfor overordnet byrådsavdeling, Byrådsavdeling for finans og personvernombudet.
- Nytt punkt med overskrift «Rutiner» dekker tidligere punkter om tilgangsstyring og beredskap.
  - Fysisk sikring/adgangskontroll er ikke lenger eksplisitt nevnt, da det er forskjeller mellom virksomhetene hvem som har utfører dette. «Informasjonssikkerhetsområdet» vil likevel omfatte dette.

Rollekort for PKO

- Bygger på rollekort for ISK.
- Oppgavene er tilpasset til personvernområdet
  - Tydeliggjort rollen ved melding om brudd på personopplysningssikkerheten.
  - Tydeliggjort rollen i forbindelse med eventuelle forhåndsdrøftelser med Datatilsynet.
- PKO skal være kontaktperson utad (både internt i kommunen og overfor Datatilsynet) innen personvernområdet. Tilsvarende for ISK på informasjonssikkerhetsområdet.
  - Det er startet opp nettverksmøter (i regi av FIN) i flere sektorer – og flere er under planlegging. Først og fremst for PKO da rollen er ny og ukjent, men skal også være for ISK.

Pause

Vi starer igjen 1015

Oslo

Schrems II-dommen og veiledning fra Det europeiske personvernrådet (EDPB)

Personvern- og informasjonssikkerhetsforum 3. mars 2021

Linda Mari Knutsen
Spesialrådgiver FIN/ISI

Foto: Thomas Ekström

Oslo

Agenda

- Kort om bakgrunn
- Veiledning fra EDPB
- Nærmere om de enkelte veilederne
- Oppdatering av EUs standardavtaler

Kort om bakgrunn

- Personvernforordning kap. V stiller krav om gyldig overføringsgrunnlag, i tillegg til behandlingsgrunnlag, ved overføring av personopplysninger til tredjeland.

- EU-domstolen konkluderte i Schrems II-dommen med at Privacy Shield-avtalen som overføringsgrunnlag etter art 46 i GDPR er ugyldig.
  - Det betyr at overføring til USA kan forekomme, men det må foreligge et annet overføringsgrunnlag for å sikre nødvendige garantier

- Ved bruk av EUs standardkontrakter som overføringsgrunnlag, må behandlingsansvarlig (ofte kalt dataeksportør) iverksette ytterligere tiltak for å sikre samme beskyttelsesnivå som i EU/EØS.
  - Dommen slo fast at ytterligere tiltak skal etableres ved overføring av personopplysninger til USA

- Hovedpoenget med dommen:
  - Gi dataimportør (ofte leverandør) plikter for å sikre at europeernes personopplysninger blir like godt beskyttet etter overførselen til tredjeland, som de blir i EU/EØS.

Veiledere fra Det europeiske personvernrådet (EDPB)

- 11.11.2020 publiserte EDPB to veiledere som skal hjelpe behandlingsansvarlig med å etablere ytterligere tiltak ved overføring til tredjeland
- Den første veilederen forklarer nærmere reglene om overføring av personopplysninger til tredjeland og hvilke vurderinger som må ligge til grunn før overføringen kan starte
  - Inneholder også vedlegg med eksempler på ytterligere tiltak som kan være tilstrekkelig
- Den andre veilederen viser hvordan man kan gå frem ved vurdering av tredjelands overvåkningslover
  - Dette er et av kravene som må vurderes før overføring til tredjeland kan forekomme

EDPBs veileder om «ytterligere tiltak»

- Veilederen er bygd opp med en stegvis tilnærming, som i stor grad gjenspeiler anbefalingene ISI kom med i september.

1. Oversikt over alle overføringer av personopplysninger med utgangspunkt i behandlingsoversikten til virksomheten

2. Identifisere hvilke overføringsgrunnlag som benyttes ved overføring av personopplysninger til tredjeland (utenfor EU/EØS) etter personvernforordningen kap V.

3. Vurdere om lovgivningen eller praksis i tredjeland vil påvirke beskyttelsesnivået som overføringsgrunnlaget er ment å sikre.
   - Dette innebærer at virksomheten må sjekke om overføringsmekanismen faktisk er effektiv i praksis ved at beskyttelsesnivået i all hovedsak er tilsvarende/likt som EU/EØS.

Forts. EDPBs veileder om «ytterligere tiltak»

4. Virksomhetene må så identifisere og innføre ytterligere tiltak for å sikre tilstrekkelig beskyttelsesnivå.
   - Tiltak kan være av avtalemessig, tekniske og/eller organisatorisk art.
     - Eksempler på tiltak er listet opp i veilederens vedlegg 2.
     - EDPB påpeker at det kan være behov for å implementere ytterligere tiltak for samme overføring, og at det kan være tilfeller hvor ingen tiltak er tilstrekkelig

- Det er viktig å merke seg at dersom man ikke kan finne tilstrekkelig tiltak som ivaretar overføringen av personopplysningene på tilstrekkelig nivå lik EU, **skal ikke behandlingen av personopplysninger forekomme**.
- Dersom man likevel ønsker å overføre dataene må man kontakte Datatilsynet ihht art 46.
- Datatilsynet kan stoppe eller forby overføring hvor den ser at beskyttelsesnivået ikke er tilsvarende GDPR.

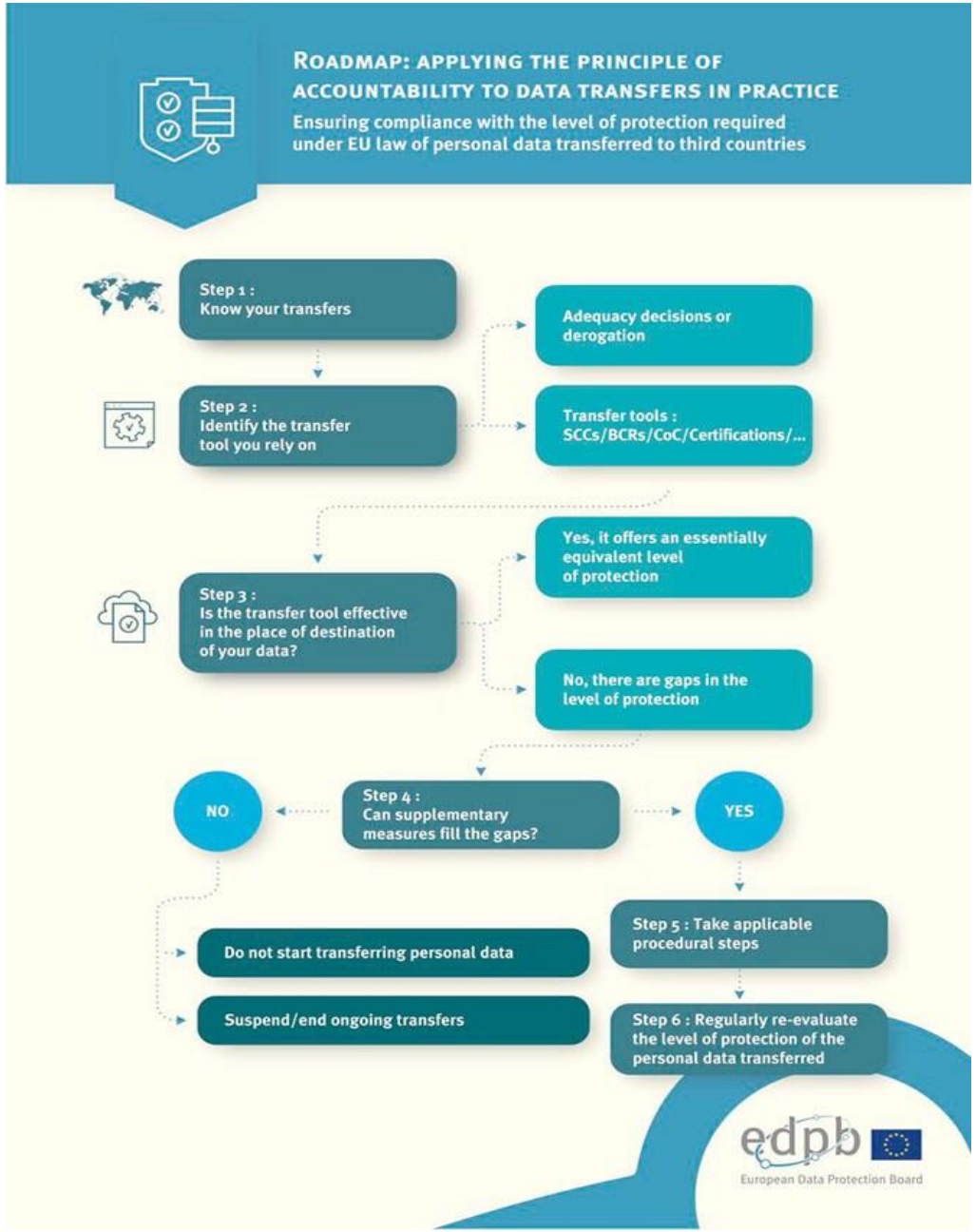
Forts. EDPBs veileder om «ytterligere tiltak»

5. Virksomhetene må videre gjennomføre nødvendige prosessuelle tiltak for å implementere de ytterligere tiltakene.

6. Det siste steget er at virksomhetene jevnlig må sørge for å revurdere beskyttelsesnivået for overføringer av personopplysninger

Veileder om vurdering av beskyttelsesnivået i tredjeland

- Tar for seg hvordan man skal vurdere overvåkningsnivået i et tredjeland og om dette er i tråd med grunnleggende personvernregler i EU/EØS.
- Veilederen oppstiller 4 grunnleggende krav til personvern ved vurdering av behandlingen av personopplysninger i tredjelandet
  - Behandlingen skal baseres på klare, presise og tilgjengelige reguleringer i lov mv.
  - Behandlingen skal være nødvendig og proporsjonal knyttet til de legitime formål som forfølges.
  - Det skal være en uavhengig kontrollmyndighet i landet som fører tilsyn med behandlingen.
  - Den registrerte skal ha effektive midler tilgjengelig for å ivareta sine rettigheter
- Viktig: alle tredjeland som ikke på forhånd er godkjent etter artikkel 45 skal gjennomgå en slik vurdering.
  - Et eksempel her kan være ved overføring av personopplysninger til India.

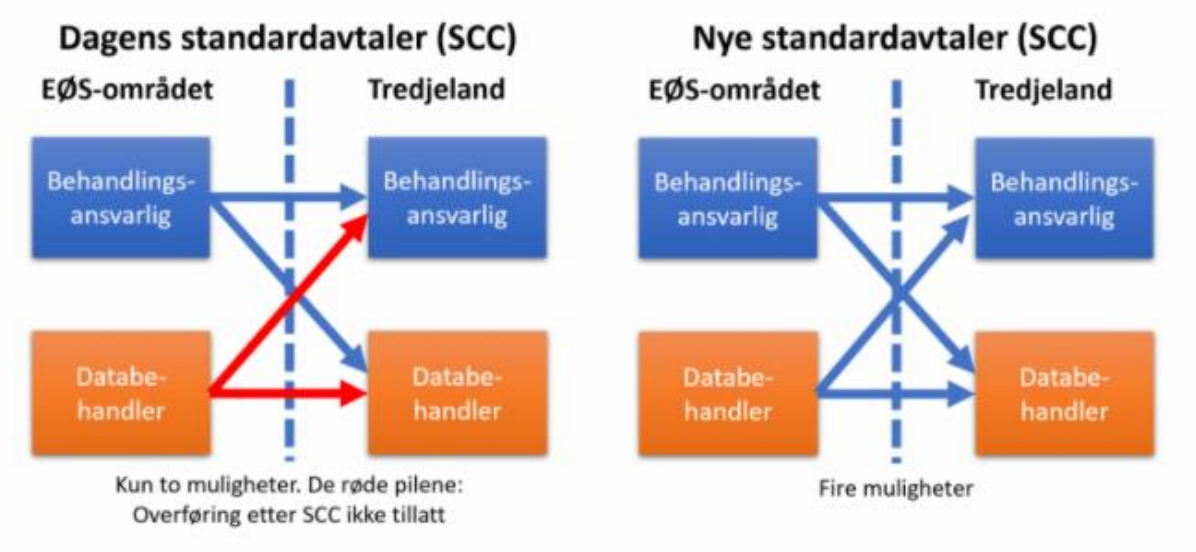

ROADMAP: APPLYING THE PRINCIPLE OF ACCOUNTABILITY TO DATA TRANSFERS IN PRACTICE
Ensuring compliance with the level of protection required under EU law of personal data transferred to third countries
Step 1 : Know your transfers
Step 2 : Identify the transfer tool you rely on
Adequacy decisions or derogation
Transfer tools : SCCs/BCRs/CoC/Certifications/...
Step 3 : Is the transfer tool effective in the place of destination of your data?
Yes, it offers an essentially equivalent level of protection
No, there are gaps in the level of protection
Step 4 : Can supplementary measures fill the gaps?
NO
YES
Do not start transferring personal data
Suspend/end ongoing transfers
Step 5 : Take applicable procedural steps
Step 6 : Regularly re-evaluate the level of protection of the personal data transferred
edpb
European Data Protection Board

Standard contractual clauses (SCC) – forslag til endring av avtaleverket fra EU

- Den vanligste måten å sikre de nødvendige garantiene når en virksomhet overfører personopplysninger til tredjeland, er å bruke EUs standardavtaler (Standard Contractual Clauses).
- EDPB og EUs datatilsyn (EDPS) kom 12. nov med uttalelser til kontraktsbestemmelsene
- I de nye bestemmelsene skal overføringen og behandlingen beskrives nærmere enn tidligere, herunder bl.a. sikkerhetstiltakene.
- Endringene dekker også kravene til databehandleravtale etter personvernforordningens art 28

Forts. forslag til endring av SCC

- Dagens SCC dekker kun overføring mellom behandlingsansvarlig innenfor EU/EØS og enten behandlingsansvarlig i tredjeland eller databehandler i tredjeland.
- Inkludere nå 4 alternative muligheter for overføring:



- Endringene skal vedtas i mars

Oslo

EDPB Rec. 01/2020

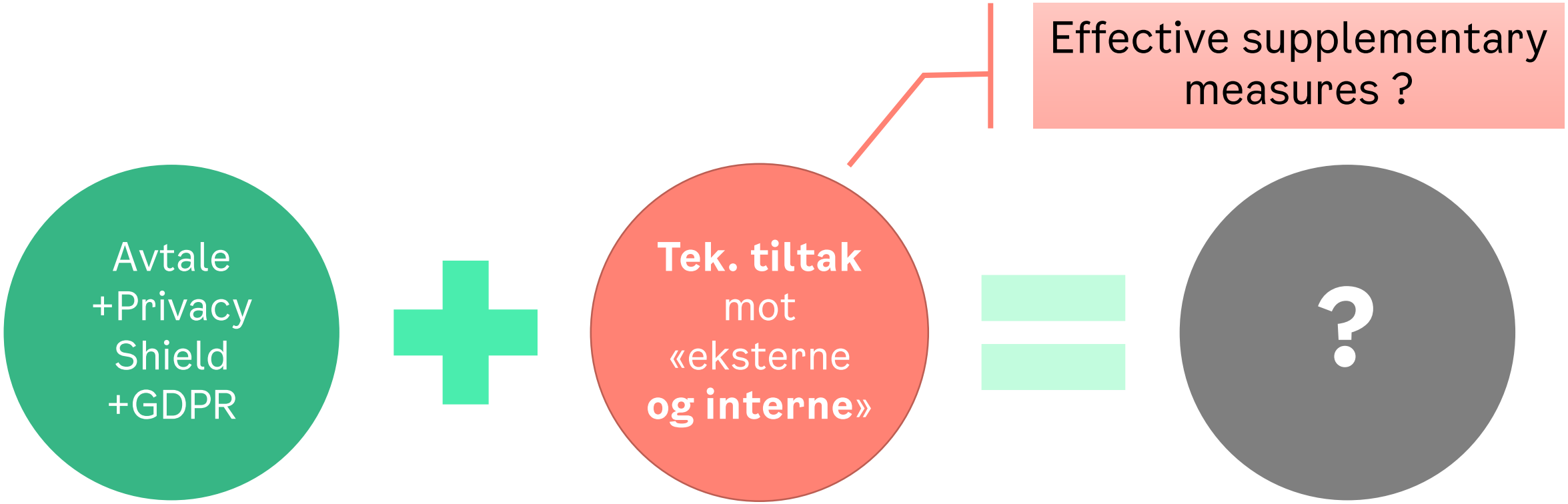
"on **measures** that supplement transfer tools to ensure compliance with the EU level of protection of personal data"

Åsmund Skomedal
Fagsjef informasjonssikkerhet
asmund.skomedal@byr.oslo.kommune.no

Logikken *før* Schrems II dommen

Privacy Shield	EU-US avtale for utveksling av data
GDPR	Artikkel 46, Transfer Tools

Logikken *etter* Schrems II dommen

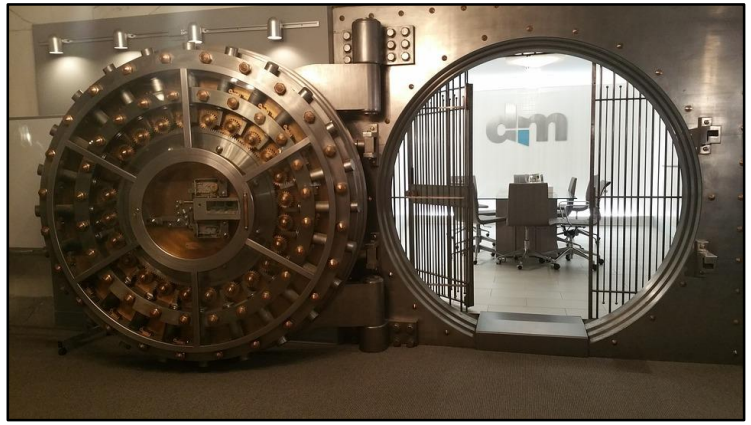


Privacy Shield	EU-US avtalen for utveksling av data
A.46	Artikkel 46, Transfer Tools

Veilederen beskriver tekniske tiltak som *kan* være gode nok, men …

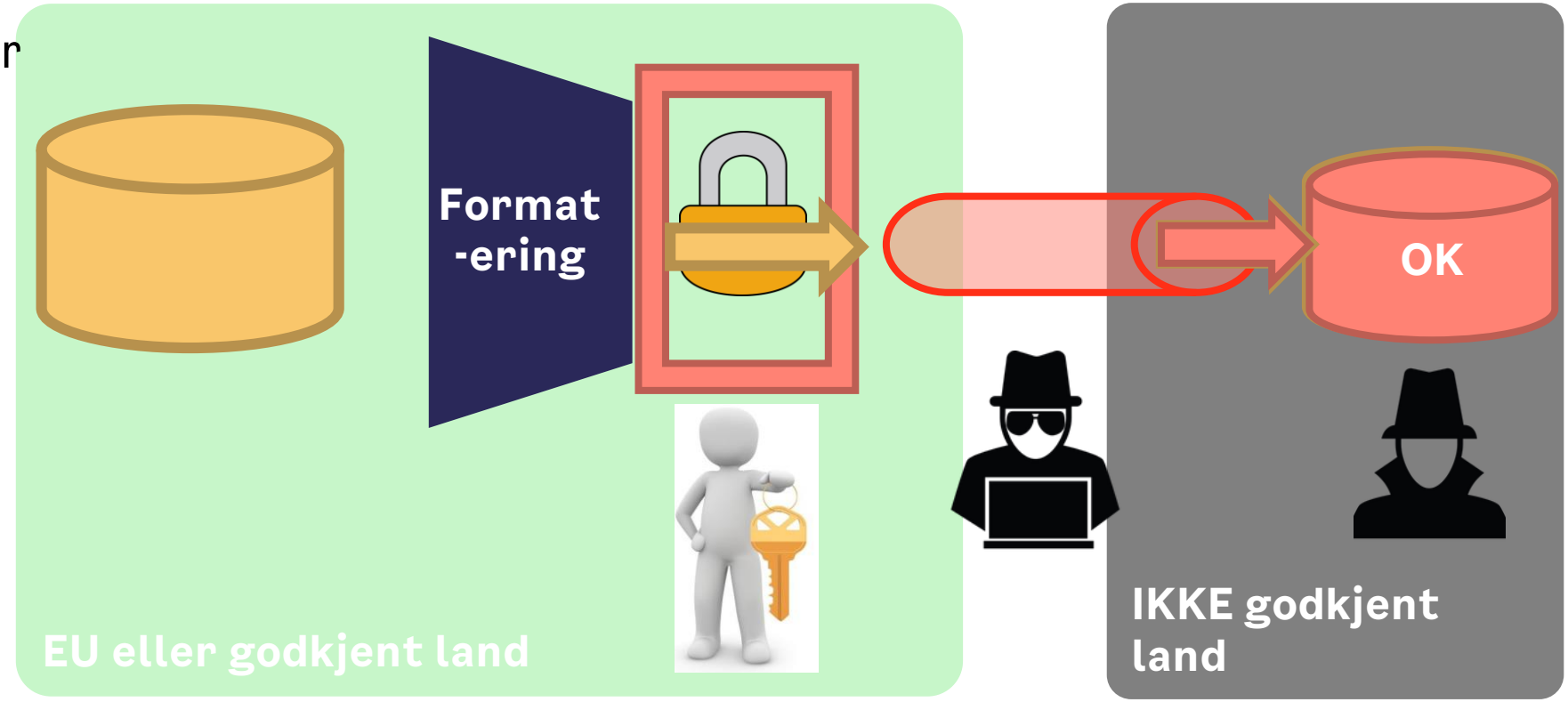
- Betingelsene for at IT-tjenester som leveres fra 3. land har «effektive ytterligere tiltak» kan gjøre dette vanskelige i praksis
- Scenarier for tjenester fra 3. land med tiltak som *potensielt* kan være OK
  1. Datalagring hvor informasjon er **utilgjengelige** i klartekst i 3. landet
  2. Personopplysningene er «**pseudonymisert**» før overføring
  3. Kommunikasjon (transitt) av **krypterte** data
  4. …
  5. …
- Scenario for tjenester fra 3.land som en *ikke* finner noen løsning på
  6. …
  7. …

Et eksempel som kan være «OK» (for å forhindre innsyn via 2. part)



Datalagring (back-up) der en forutsetter:

- sterk kryptering før overføring
- motstandsdyktige algoritmer
- at lagringstiden ivaretas
- implementasjonen er feilfri
- «pålitelig» nøkkelhåndtering
- nøklene forvaltes i «EU»



… then the EDPB considers that the encryption performed provides an effective supplementary measure

For det vi lurer på … så ser en ingen løsning i dag

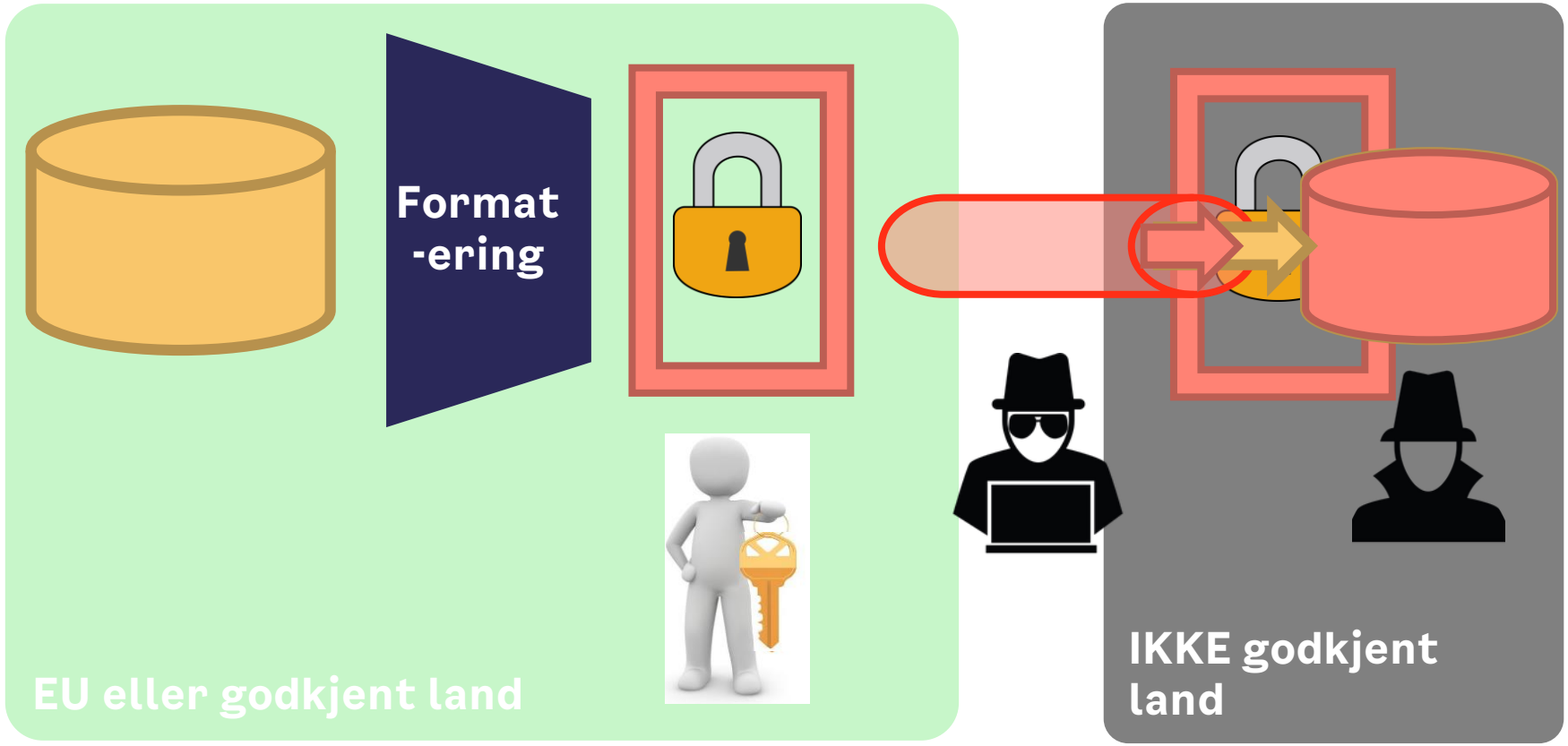
Scenario 6; skytjenester (~Saas)

- som krever databehandling i *klartekst*
- i et ikke godkjent land

og (selv med)

- transportkryptering og
- kryptert lagring

som benyttes hver for seg



Hva betyr dette for kommunen ?

IKT systemer som driftes i Norge og EU (uten 3.lands overføringer) er fortsatt OK

Potensielt store konsekvenser ved bruk av skytjenester, særlig hvor det forekommer overføring og databehandling i USA. Viktigste for dere:

- få oversikt over hvilke tjenester som er berørt
- be om redegjørelse fra leverandørene og
- vurder om dere burde avslutte kontrakt og stoppe behandlingen!
- Datatilsynet; «Det er viktig å **vente** med å inngå **nye avtaler** med tredjelandsleverandører inntil man er helt sikker på at man fullt ut klarer å etterleve alle av EU-domstolens tilleggsvilkår»

- FIN v/ISI sammen med UKE er i dialog med Microsoft for å få redegjørelse om hvilke tiltak de iverksetter for å imøtekomme veiledningen fra EDPB
  - Svar kan gjenbrukes av virksomhetene i andre sammenhenger som er sammenliknbare

- KS og SKATE-virksomheter ser også på om man skal lage veiledninger for hvordan offentlig sektor kan løse disse utfordringene

- EDPB har mottatt kritikk for ikke å ha en risikobasert tilnærming

Nyttige lenker

Veilederen fra EDPB:

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/%C2%A0

Styrende dokumenter:

https://felles.intranett.oslo.kommune.no/styrende-dokumenter-avtaler-og-regelverk/informasjonssikkerhet/

Anskaffelsesveileder:

UKE intranett> Kundeportal> Veiledere> Anskaffelsesveileder

Forum, programgruppe, kompetanse m.m

Maylén Mago Pedersen

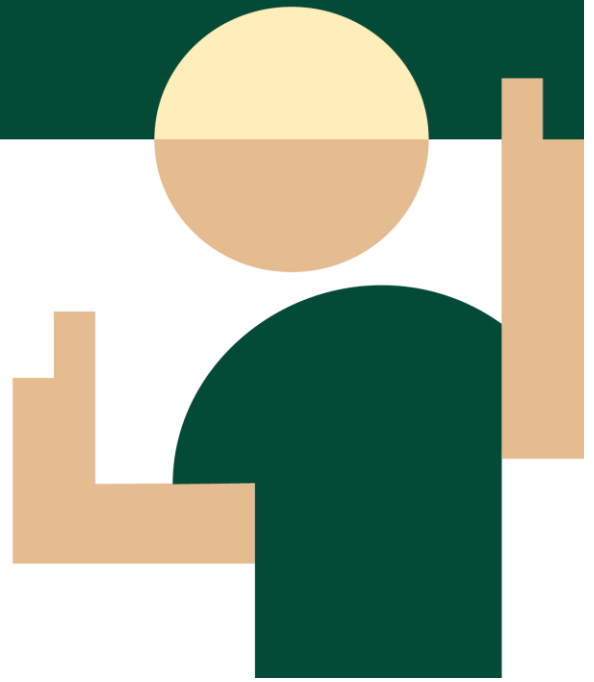
Oslo

Personvern- og informasjonssikkehetsforum

- Mandatet til forumet er oppdatert og ligger på felles intranett
- Vi har en programgruppe til forumet som skal være med å gi innspill og sette sammen det faglige innholdet til forumene slik at vi lager et relevant og engasjerende faglig innhold.
- Programgruppa består av representanter fra virksomhetene i Oslo kommune.
  - For å sikre kontinuitet velges det nye medlemmer hvert år for to år av gangen.

Kommende datoer for forum

14.april
09.juni
1.september
24.november



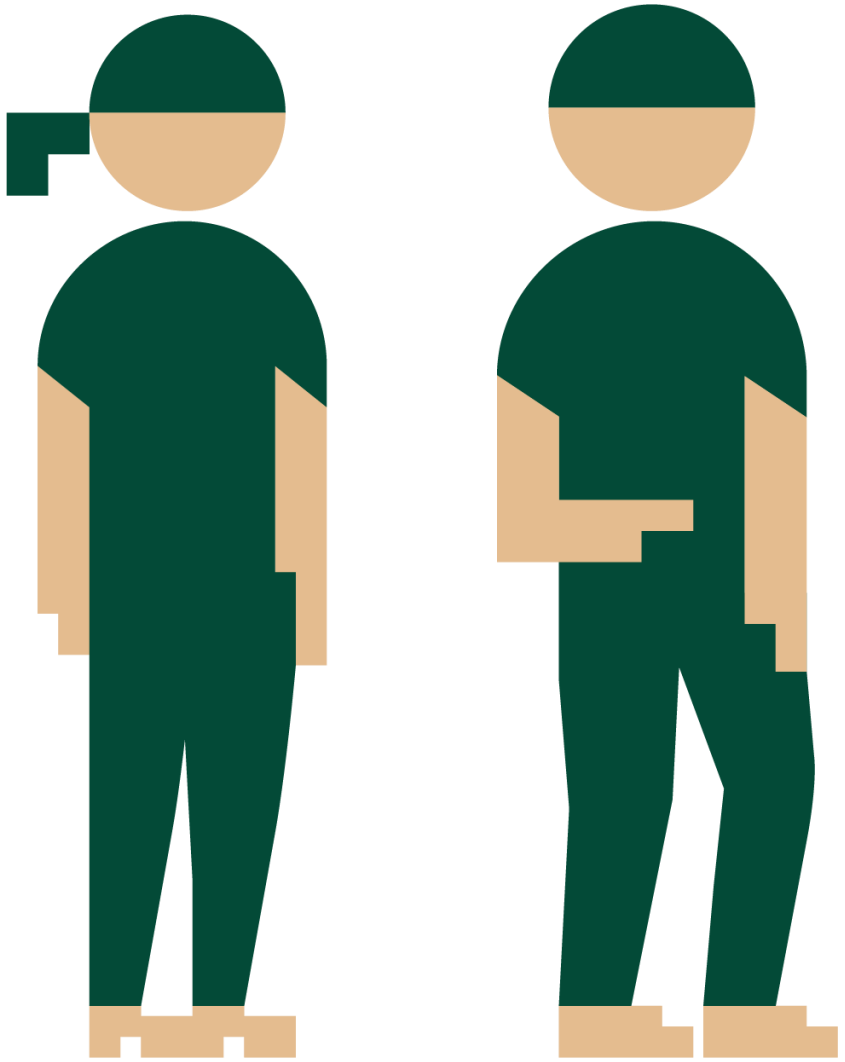
Hvorfor delta i programgruppa?

Programgruppa skal bestå av 3-5 deltakere fra virksomhetene

- Du får være med å sette agendaen på forumene
- Du får et nettverk med andre likesinnede i Oslo kommune

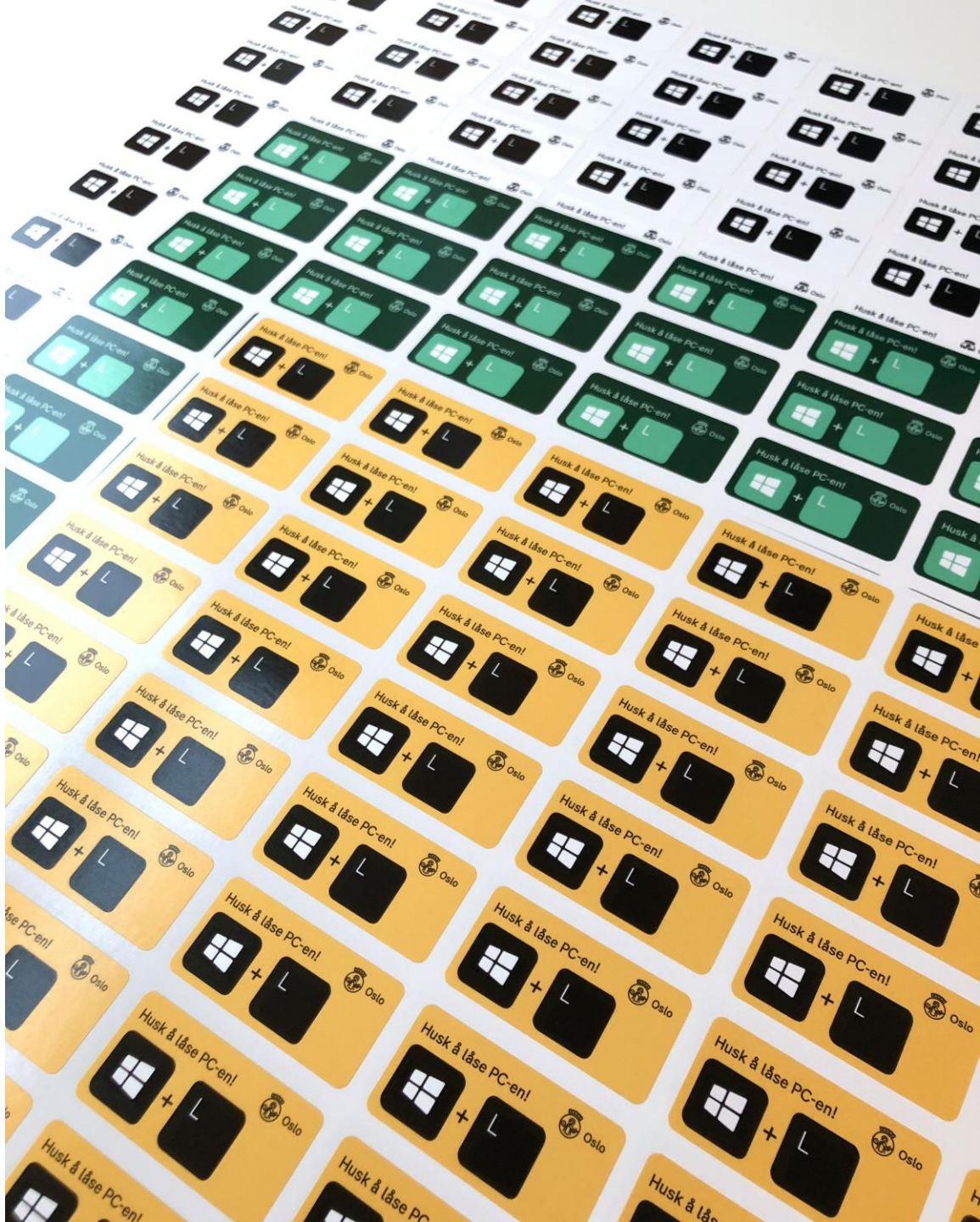
Vi ønsker 2 ny personer inn i gruppa som da sitter i 2 år.

Vil du være med?



Klistremerker

- Vi har oppdatert klistremerkene i henhold til designmanualen
  Oslo kommune logo
  - Tekst «Husk å låse PC-en!»
  - Nye Oslo fargene (gul med sorte taster, hvit med sorte taster og grønn med hvite taster).
- Sendes til alle IKT- brukerstøtter med et skriv i løpet av noen uker



E-læringer

Sikkerhetsmåneden 2021

Tim-universet

Heldagskurs i risikovurderinger

Kompetanseprogram for phishing

Læringsprogram for koordinatorer

Gjenopplive Workplace-gruppe for koordinatorer

Hva skjer på kompetansefronten?