Oslo

Forum for informasjonssikkerhet og personvern

Onsdag 24. november

Tema: Verktøy

Sendingen starter kl 09:00

Program

09:00 - 09:05	**Velkommen og introduksjon til dagens program**
09:05 - 09:15	**Hva skjer på personvernområdet?** Maryke Silalahi Nuth
09:15 - 09:25	**Hva skjer på informasjonssikkerhetsområdet?** Åsmund Skomedal
09:25 - 09:50	**Nye maler for personvernvurderinger og DPIA** Maryke Silalahi Nuth
09:50 – 10:00	Pause til å fylle kaffekoppen
10:00 - 10:25	**Selvbetjeningsløsning for informasjonssikkerhet og personvern på intranett** Ida Marie Larsen i bydel Gamle Oslo
10:25 - 10:50	**Personvernhåndbok** Hana Temsamani i bydel Søndre Nordstrand
10:50 - 11:00	**Andre verktøy og avslutning** Cecilie Bergh

Oslo

Hva skjer på personvernområdet?

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

Personvern- og informasjonssikkerhetsforum 24. november 2021

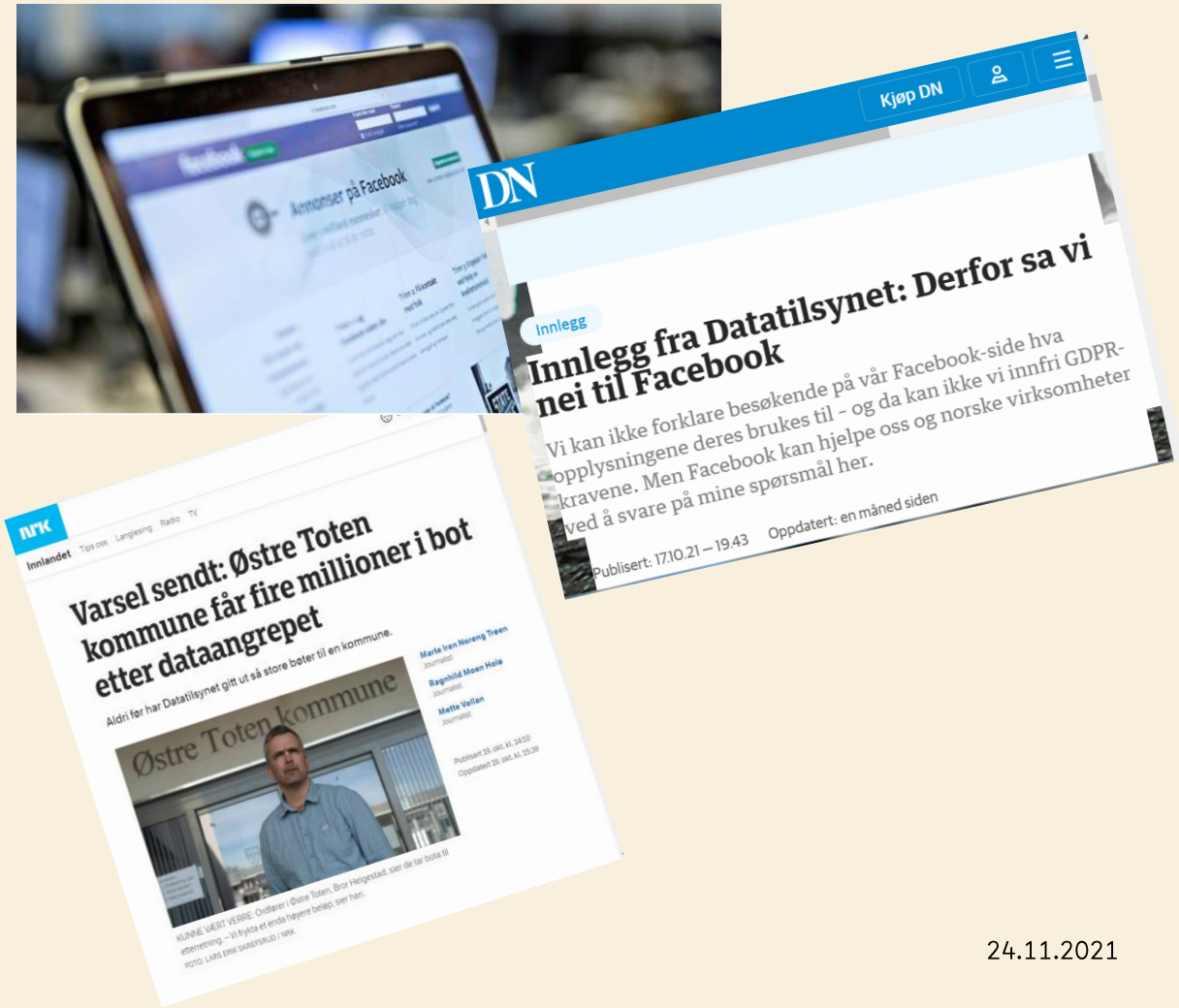
Foto: Ben Garratt

Oslo

Hva skjer utenfor Oslo kommune Q4 2021

- Datatilsynets vurdering av Facebook
  - BLK starter vurdering av Oslo kommunes Facebook-side «Oslo.kommune»

- Datatilsynets varsel om overtredelsesgebyr til Østre Toten kommune
  - Grunnleggende mangler ved kommunens personopplysnings- og informasjonssikkerhetssystemer



Henvendelser i Oslo kommune Q4 2021

- Kameraovervåking
  - Økt bevissthet om strenge krav for bruk
- Avvikshåndtering
  - Oppfølging av personvernombudets rapport 2020
  - Melding til Datatilsynet
    - Utfylling av melding – vær varsom!
- Schrems II oppfølging
  - UKE vurderer svar fra Microsoft
  - Spørsmålsliste til leverandører er publisert på intranett – kan gjenbrukes

FIN/ISI tiltak

- Vurderinger
- Faglig rådgivning (bistand DPIA)
- Dialog og sektormøter
- Informasjon

FIN/ISI team personvern – leveranser

Veiledere

(publisert 30. juni 2021)

- Avvikshåndtering
- Innsyn i personopplysninger
- Behandlingsgrunnlag (Ny)

Maler med veileder

(publisert 1 okt. 2021 ifbm. Sikkerhetsmåneden)

- Innledende vurdering av personvern (IVP)
- Vurdering av personvern ved ikke høyrisiko (OVP/IHVP)
- DPIA

Vurderinger

(ferdigstilt 19. nov 2021)

- Fulltekstpublisering av dokumenter med personopplysninger

Pågående arbeid (2021-2022)

Vurdering av behandlingsansvar

- Vil påvirke rolle, ansvar og oppgaver

Personvernerklæringer

- Deles i tre nivåer: Oslo kommune, virksomhet/etat og system/tjeneste
- Behov for veileder

Behandlingsoversikt (protokoll)

- UKE er prosjekteier, FIN/ISI har faglig ansvar
- Involvering av sektorer

Maler for personvernvurderinger med veileder

1

Start med innledende vurdering av personvernet til den registrerte

Vurdering av om risikoen for den registrerte er **lav/middels** eller **høy**

A

Personvernkonsekvens-vurdering ved lav/middels risiko (PLM)

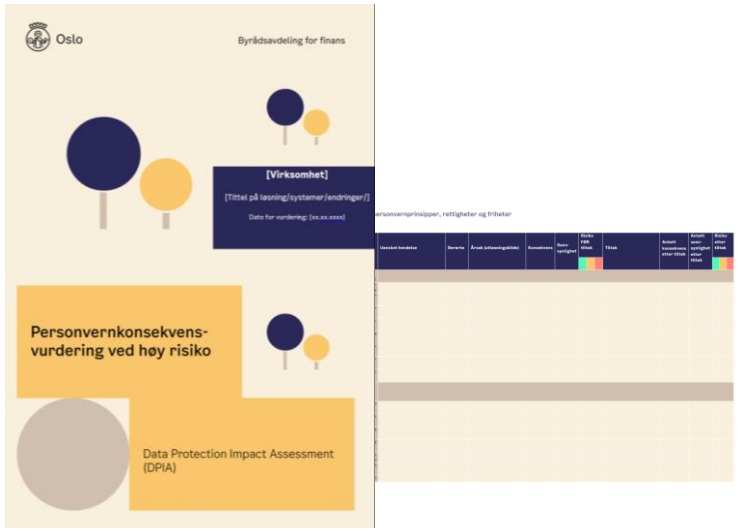
ELLER B

A

B

Personvernkonsekvens-vurdering ved høy risiko

(DPIA – Data Protection Impact Assessment)



Oslo

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

	BLK	FIN	NOE	BYU	MOS	KIF	OVK	AIS	HEI	BYD
Sektorkontakt	Siri P. Johansen			Christina M. Grønli			Linda M. Knutsen	Siril Jonassen		Linda M. Knutsen

Generelle henvendelser sendes til fagsjef for personvern Maryke S. Nuth

Oslo

Informasjonssikkerhet

En kort oppdatering

24. november 2021

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

Skytjenesteveileder - for IaaS & PaaS

Publiseres i nærmeste framtid på intranett

- Formålet er å bidra til å sikre at det ikke tas i bruk infrastruktur eller plattform i skyen *som medfører uakseptabel* ***risiko*** for kommunens virksomhet når det gjelder informasjonssikkerhet og personvern
- Veilederen fokuserer på de særskilte vurderingene som må gjøres for skytjenester
  - Avtalefleksibilitet
  - Ansvarsforhold
  - Risikobildet
- Informasjon kommer på WorkPlace og

  publiseres på: Oslo | Felles intranett for Oslo kommune

Hovedside | Informasjonssikkerhet og personvern | Informasjonssikkerhet | Verktøy og maler | Skytjenester

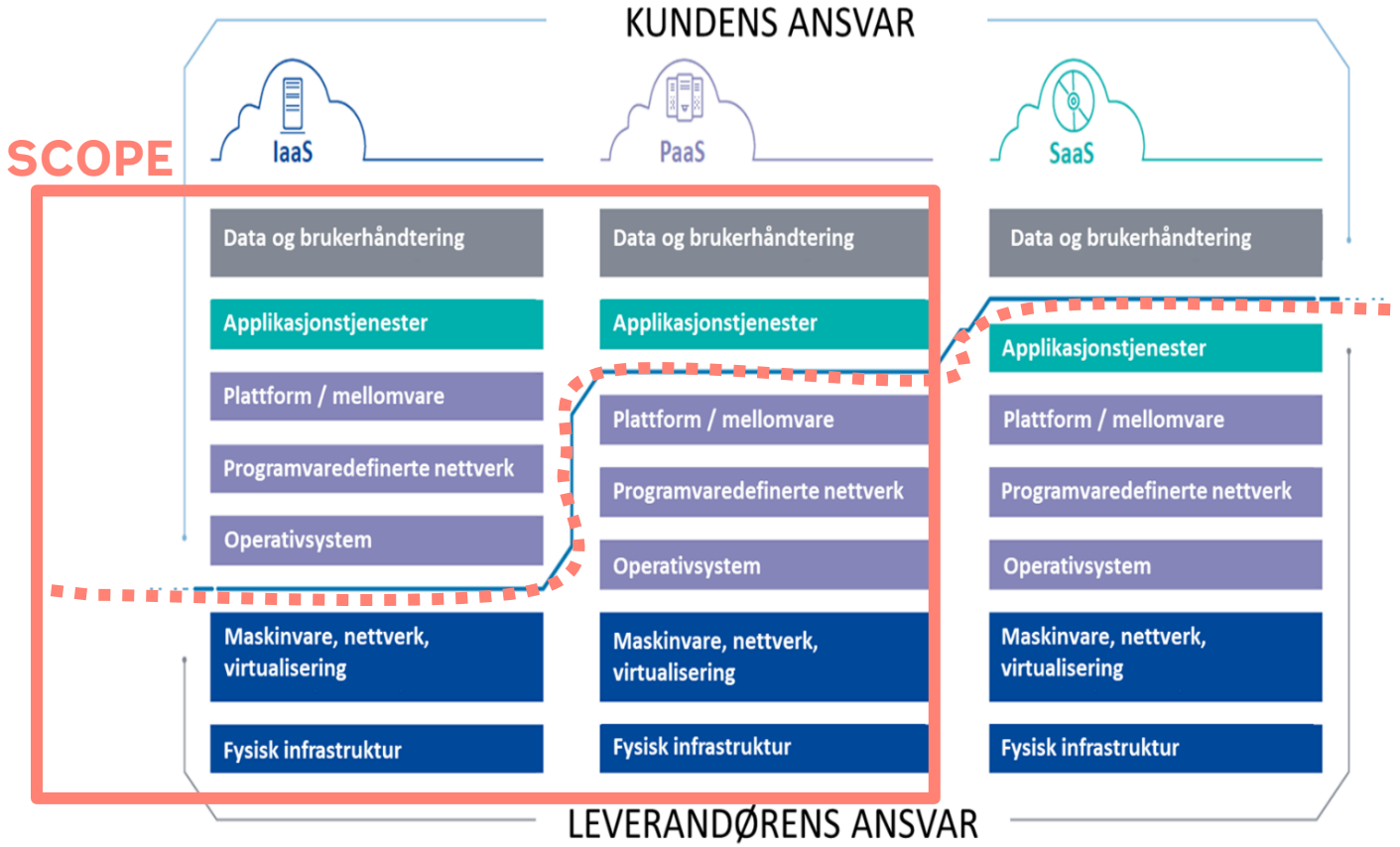
Om veilederen (i)

Merk: denne versjonen dekker ikke SaaS tjenester

Målgrupper:

ledere og medarbeidere som er systemeiere eller er involvert i arbeidet med

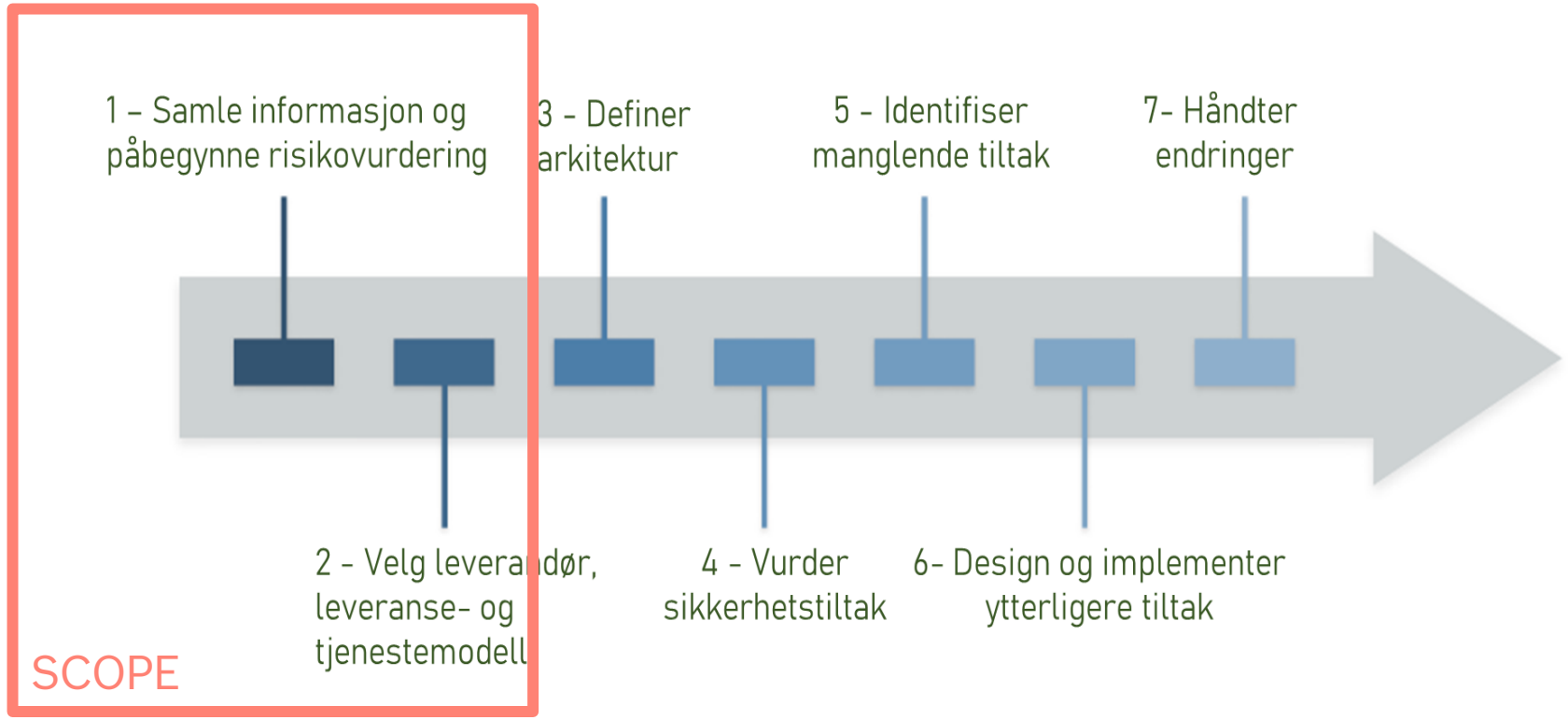
- etablering,
- utvikling,
- forvaltning og drift av skytjenester



Information Security Forums rapport «Using Cloud Services Securely»)

Om veilederen (ii)

- Primært om oppgaver som bør eller må utføres i **vurderingsprosessen** rundt etablering av infrastruktur og plattform i sky
- Dette er ikke en teknisk veileder



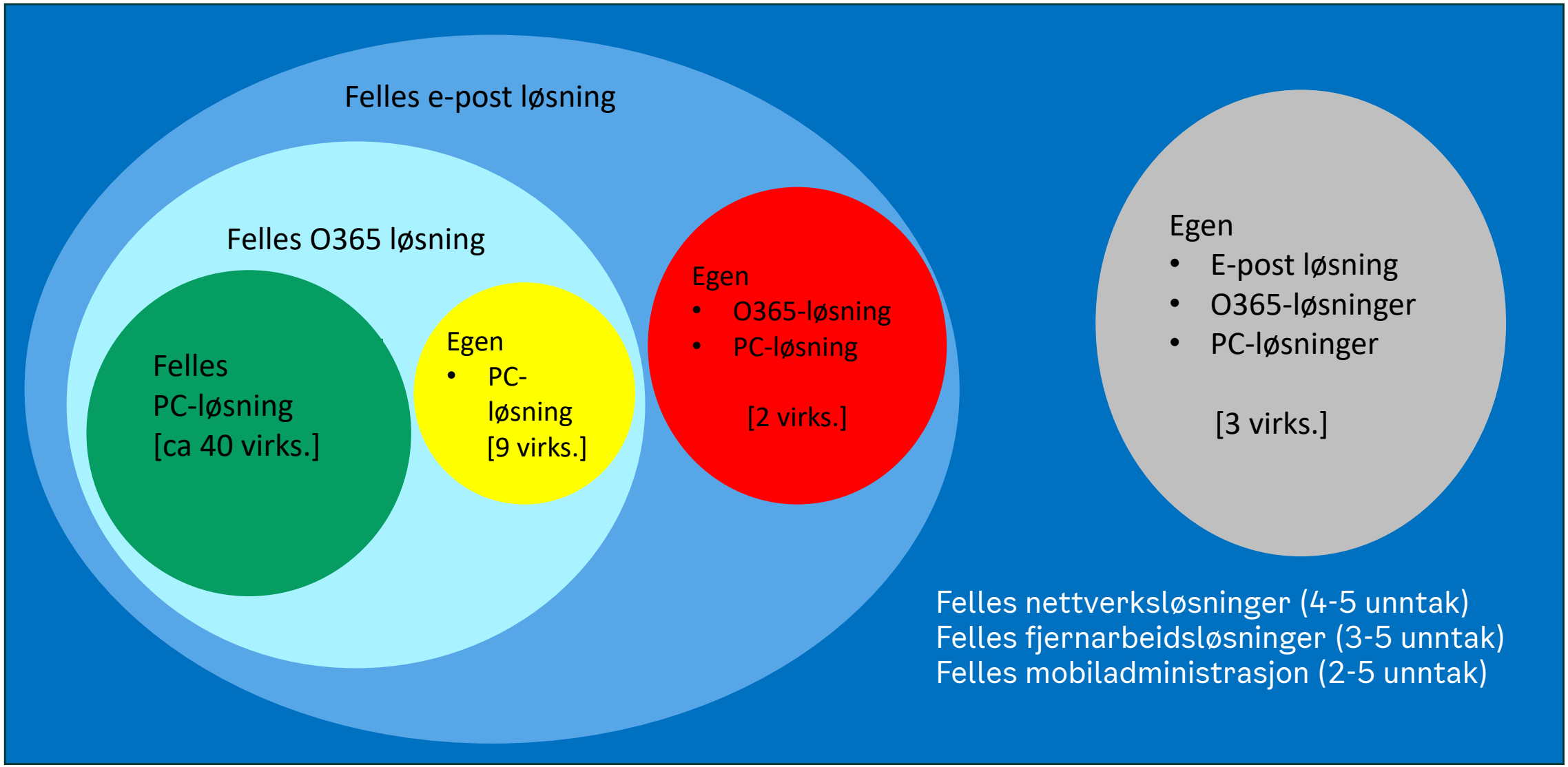
Sikkerhet i felles IKT-plattform

Office 365 bidrar med felles komponenter

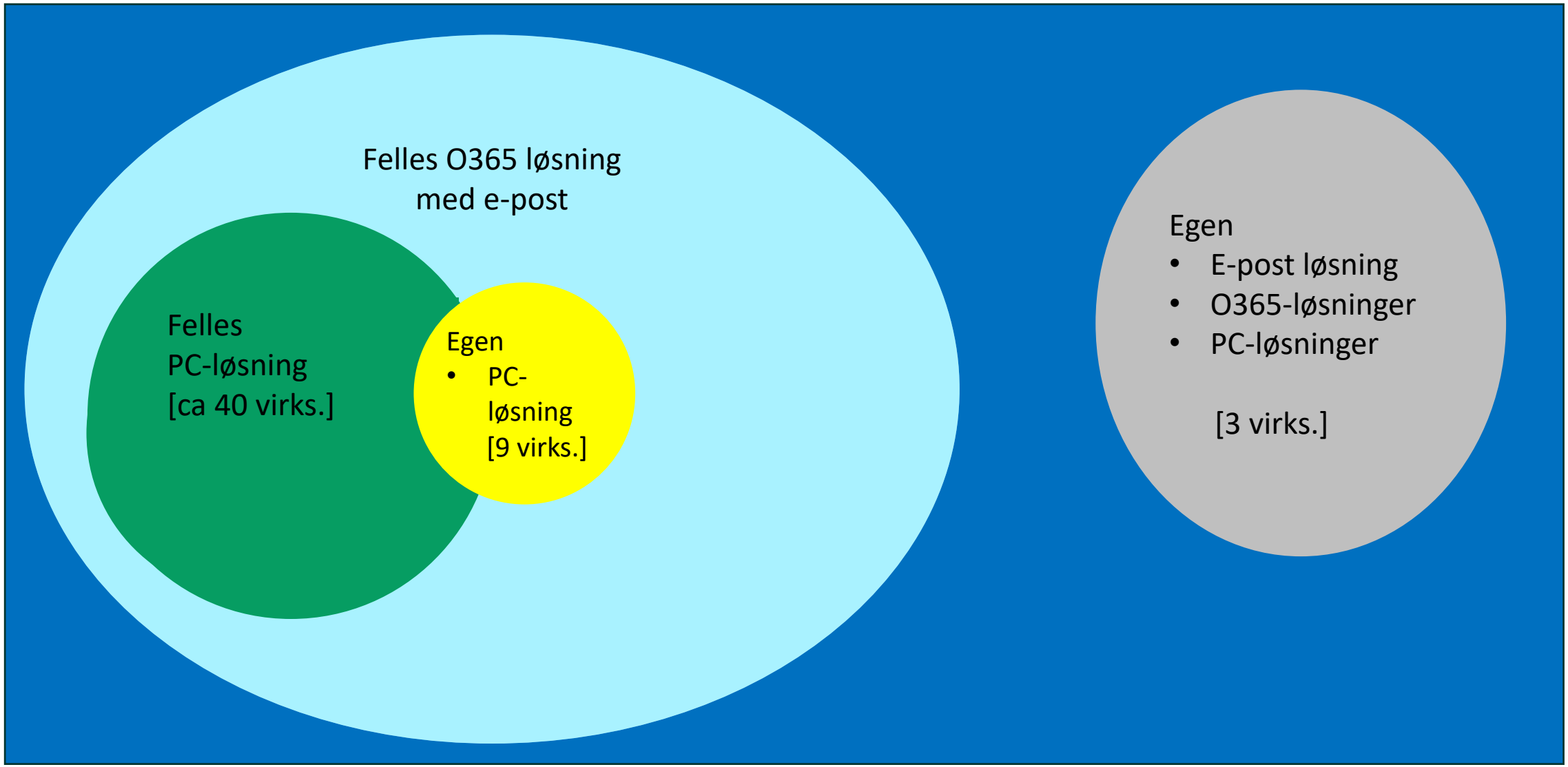
Noen viktige tiltak i Office hever sikkerheten betydelig:

- Pålogging med 2-faktor autentisering
  - Mobil (SMS og/eller «app»)
  - Andre metoder utredes
- Enhetlig sikkerhetsnivå på klientene
  - Administrert og innrullet PC (=>ikke Office365 fra privat PC)
  - Innrullet mobil
- Katalogtjeneste for sentral lagring av brukerrettigheter

Sikkerhet i felles IKT-plattform (november 2020)



Sikkerhet i felles IKT-plattform (februar 2022)



Sikkerhet i felles IKT-plattform – langsiktig målbilde

Gjenbruk av sikkerhetsløsninger fra Office 365

- Én felles løsning for PC administrasjon for «alle» virksomheter
- 2-faktor autentisering for «alle» ansatte
- Én felles katalogtjeneste for sentral lagring av brukerrettigheter
- Gjenbruk av autentisering og brukerrettigheter for andre tjenester
- Ett felles (IGA) verktøy for administrasjon av brukerrettigheter (erstatter PRK)

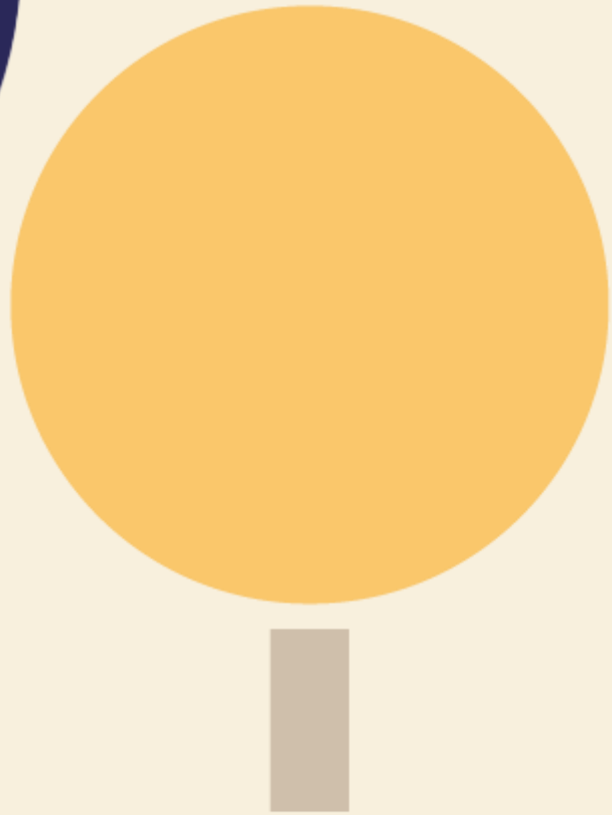
Foto: irpp.org, Creativ

Oslo

Personvernvurderinger ved behandling av personopplysninger

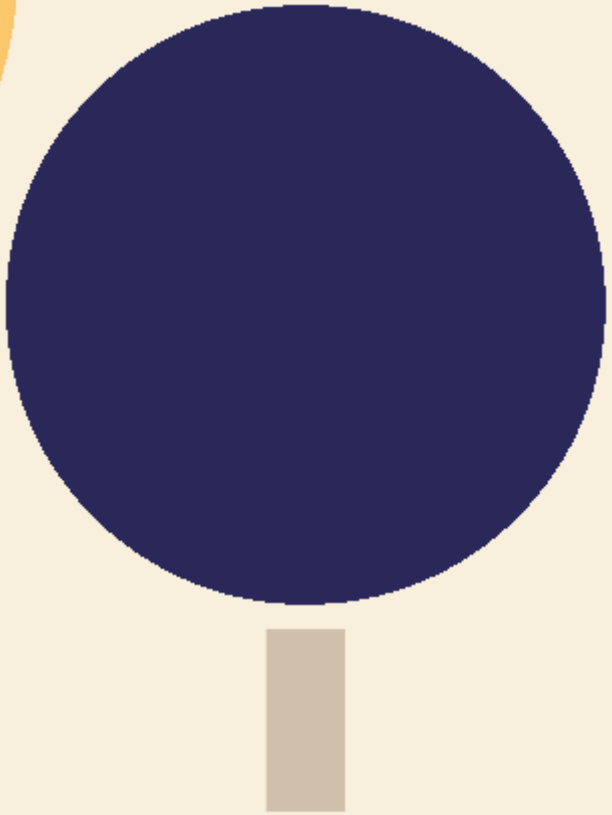
Maryke S. Nuth
Fagsjef personvern
maryke.nuth@byr.oslo.kommune.no

Personvern- og informasjonssikkerhetsforum
24. november 2021



Oslo

Prosess for personvernvurderinger



1

Start med innledende vurdering av personvernet til den registrerte

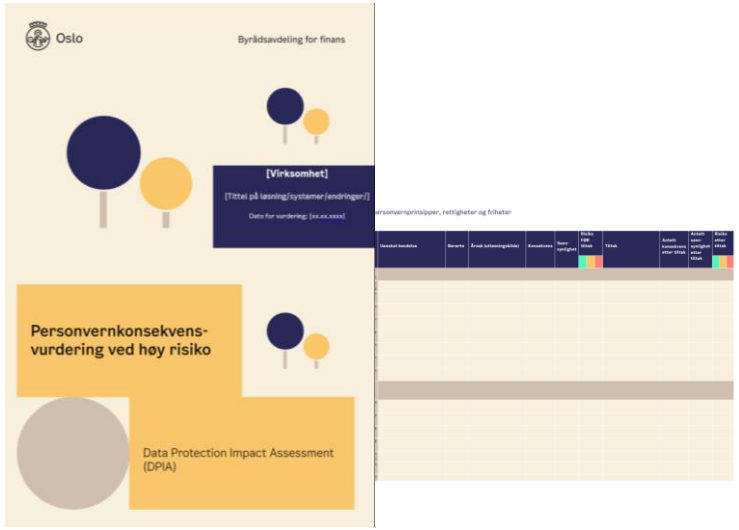
Vurdering av om risikoen for den registrerte er **lav/middels** eller **høy**

A Personvernkonsekvens-vurdering ved lav/middels risiko (PLM)

A ELLER B

B Personvernkonsekvens-vurdering ved høy risiko

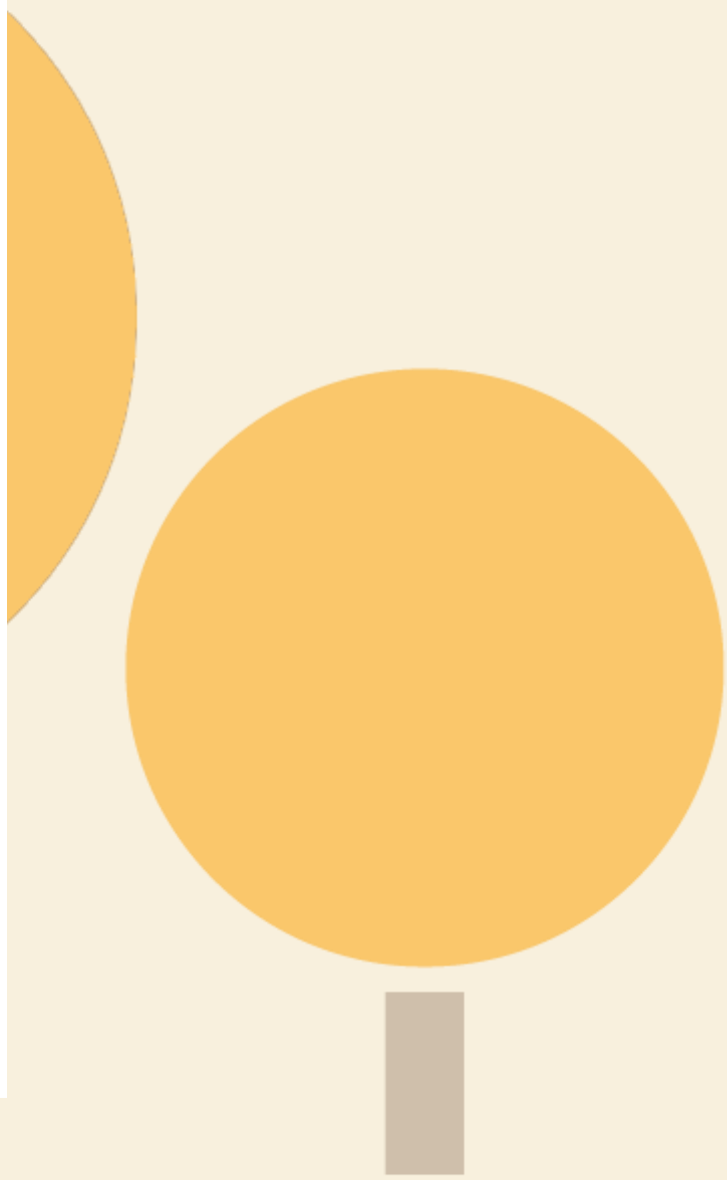
(DPIA – Data Protection Impact Assessment)



Oslo

Oslo

Mål og hensyn bak malene



En helhetlig tilnærming for personvern

Personvernvurderinger | Personvernerklæring | Behandlingsoversikt | Avvik

PLANLEGGE

INNHOLD FRA IP/PLM/DPIA

UTFØRE/ VIRKELIG-GJØRE

INNHOLD FRA IP/PLM/DPIA

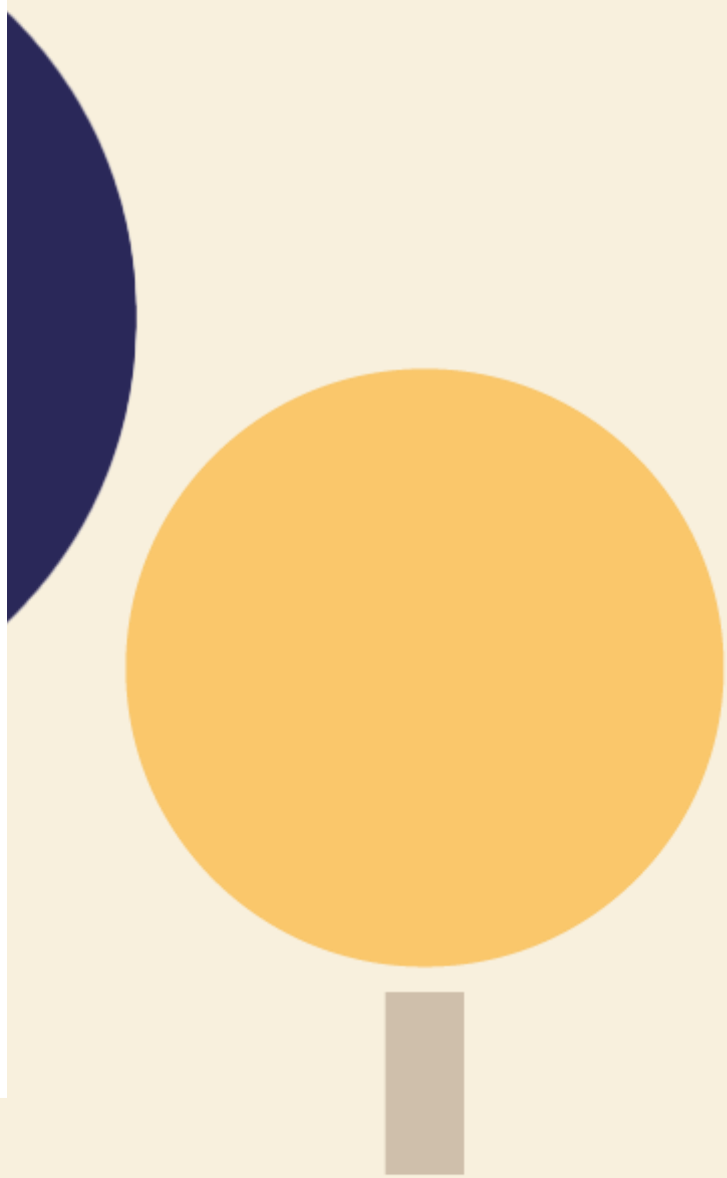
KONTROLLERE

INNHOLD FRA IP/PLM/DPIA

KORRIGERE

Oslo

Sammenheng mellom malene



Fellesdeler

IP	PLM	DPIA
FELLESDELER		
1. Grunnleggende informasjon om tjeneste/løsning/system og roller	1. Grunnleggende informasjon om tjeneste/løsning/system og roller	1. Grunnleggende informasjon om tjeneste/ løsning/system og roller (utvidet)
2. Grunnleggende informasjon om de registrerte	2. Grunnleggende informasjon om de registrerte	2. Grunnleggende informasjon om de registrerte
3. Grunnleggende informasjon om personopplysninger	3. Grunnleggende informasjon om personopplysninger	3. Grunnleggende informasjon om personopplysninger
	4. Behandlingens art, omfang og kontekst	4. Behandlingens art, omfang og kontekst (utvidet)
	4.A. Beskrivelse av behandlingen	4.A. Beskrivelse av behandlingen
4. Grunnleggende informasjon om planlagt behandling	4.B. Behandlingens art	4.B. Behandlingens art (utvidet)
	4.C. Behandlingens omfang	4.C. Behandlingens omfang (utvidet)
	4.D. Behandlingens kontekst	4.D. Behandlingens kontekst (utvidet)
	4.E. Overføring til utlandet	4.E. Overføring til utlandet (utvidet)
5. Grunnleggende informasjon om formål	5. Behandlingens formål 5.A. Formål for førstegangsbehandling	5. Behandlingens formål og begrunnelse 5.A. Formål for førstegangsbehandling (utvidet)
	5.B. Formål ved viderebehandling	5.B. Formål ved viderebehandling (utvidet)
		5.C. Begrunnelse for formålet

Særdeler

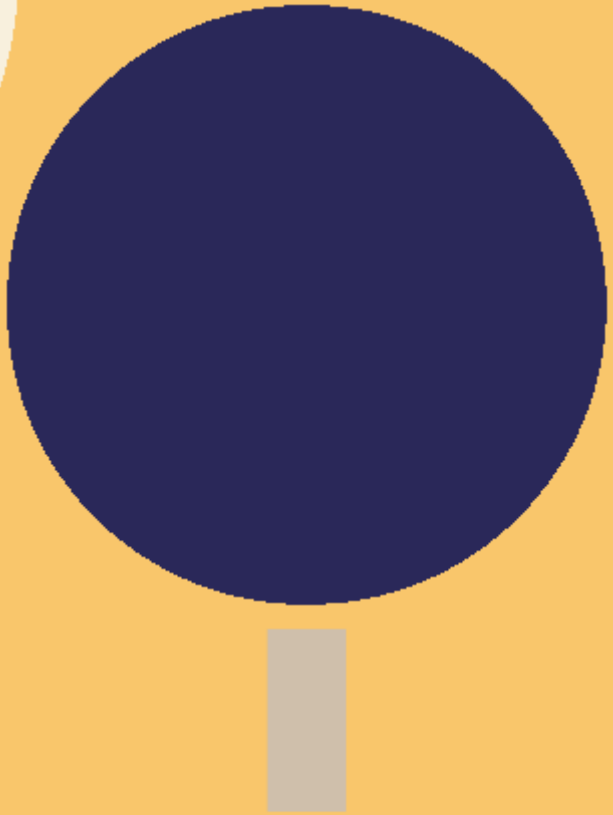
IP	PLM	DPIA
SÆRDELER		
6. Særlig plikter og unntak etter GDPR art. 35	6. Behandlingens lovlighet	6. Behandlingens lovlighet (utvidet)
	6.A. Behandlingsgrunnlag	6.A. Behandlingsgrunnlag
	6.B. Samtykke	6.B. Samtykke
7. Grunnleggende informasjon om behov for DPIA	7. Behandlingens nødvendighet og proporsjonalitet 7.A. Nødvendighetsvurdering	7. Behandlingens nødvendighet og proporsjonalitet 7.A. Nødvendighetsvurdering (utvidet)
	7.B. Proporsjonalitetsvurdering	7.B. Proporsjonalitetsvurdering (utvidet)
	7.C. Ivaretakelse av personvernprinsippene	7.C. Ivaretakelse av personvernprinsippene (utvidet)
	7.D. Ivaretakelse av de registrertes rettigheter	7.D. Ivaretakelse av de registrertes rettigheter (utvidet)
	7.E. Ivaretakelse av de registrertes friheter	7.E. Ivaretakelse av de registrertes friheter (utvidet)
	7.F. Databehandlere	7.F. Databehandlere
		7.G. Samlet vurdering
8. Konklusjon	8. Risiko og tiltak 8.A. Personopplysningssikkerhetsrisiko	8. Risiko og tiltak 8.A. Personopplysningssikkerhetsrisiko (utvidet)
	8.B. Annen personvernrisiko	8.B. Personvernprinsipprisiko
		8.C. Rettighetsrisiko
		8.D. Frihetsrisiko
		8.E. Oppsummering av restrisiko

Fellesdeler: involvering og godkjenning

IP	PLM	DPIA
FELLESDELER		
9. Involvering og godkjenning	9. Involvering, risikoaksept og godkjenning	9. Involvering, risikoaksept og godkjenning. 9 A. Involvering (utvidet)
		9 B. Risikoaksept (utvidet)
		9 C. Godkjenning

Oslo

Innhold



IP

Innhold

	7. Grunnleggende informasjon om behov for DPIA	Ja/Nei
1.	Behandling av: • særlige kategorier personopplysninger (GDPR art. 9) • personopplysninger om straffbare forhold/dommer (GDPR art. 10) • andre personopplysninger av følsom karakter for den registrerte	Velg et element.
2.	Behandling av personopplysninger i «stor skala» (antall registrerte i tall eller andel, volumet av data, lagringstid eller geografisk omfang).	Velg et element.
3.	Behandling av personopplysningene på nye måter som kan oppfattes som inngripende for personvernet eller ikke forutsigbart for den registrerte.	Velg et element.
4.	Behandlingen vil føre til beslutninger eller tiltak med betydelig innvirkning på enkeltpersoner eller de registrerte selv f.eks. vedtak, tjenestenekt osv.	Velg et element.
5.	Behandlingen vil innebære at de registrerte kontaktes på måter som de kan finne inngripende.	Velg et element.
6.	Evaluering eller scoring/profilering i stor skala f. eks. for å forutsi den registrertes antatte evner eller egenskaper.	Velg et element.
7.	Automatiserte beslutningsprosesser med rettslige eller lignende vesentlige konsekvenser for den registrerte.	Velg et element.
8.	Systematisk overvåkning eller sporing av en persons geografiske posisjon eller atferd, f.eks. på internett.	Velg et element.
9.	Matching eller sammenstilling av data fra flere kilder, dvs. at det kombineres, sammenlignes eller avstemmes personopplysninger fra flere kilder.	Velg et element.
10.	Opplysninger om sårbare registrerte personer eller ubalanse i styrkeforhold.	Velg et element.
11.	Innovativ bruk av eksisterende teknologi eller organisatoriske løsninger, eller bruk av nye teknologiske eller nye organisatoriske løsninger (herunder bruk av biometriske og/eller genetiske opplysninger).	Velg et element.
12.	Behandlingsansvarlig henter inn personopplysningene fra andre enn den registrerte selv, og den registrerte har derfor ikke mulighet til å vite at opplysningene blir behandlet.	Velg et element.
13.	Bruk av personopplysninger om barn til informasjons- eller markedsføringsformål (eventuelt basert på automatisert utvalg), eller dersom virksomheten planlegger å tilby nettjenester direkte til barn.	Velg et element.
14.	Behandling av personopplysninger i land utenfor EU/EØS (tredjeland) som ikke er godkjent av EU-kommisjonen.	Velg et element.

IP

6. Særlig plikter og unntak etter GDPR art. 35

Det skal gjennomføres DPIA etter GDPR art. 35 nr. 3 i følgende tilfeller:

a) En systematisk og omfattende vurdering av personlige aspekter av de registrerte som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for de registrerte eller på lignende måte i betydelig grad påvirker den registrerte
b) Behandling i stor skala av særlige kategorier personopplysninger (GDPR art. 9 nr. 1) eller av personopplysninger om straffedommer og lovovertredelser (GDPR art. 10)
c) En systematisk overvåking i stor skala av et offentlig tilgjengelig område

Kan den planlagte behandlingen anses som et av tilfellene nevnt ovenfor?	☐ Ja, spesifiser hvilket tilfelle a, b eller c Velg et element. ☐ Nei

Det skal *ikke* være nødvendig å gjennomføre DPIA etter GDPR art. 35 nr. 10 dersom:

- behandlingen er i henhold til GDPR art. 6 nr. 1 bokstav c) eller e) har et rettslig grunnlag i loven som virksomhetene er underlagt, og
- nevnte lov regulerer den eller de aktuelle spesifikke behandlingsaktivitetene, og
- det allerede er utført en vurdering av personvernkonsekvenser som en del av en generell personvernvurdering i forbindelse med vedtakelse av loven.

Kan den planlagte behandlingen anses som dekket av unntaket som nevnt ovenfor?	☐ Ja ☐ Nei

Konklusjon

Oppsummering av funn:	☐ Det foreligger ikke høy risiko ☐ Det foreligger høy risiko
Beskriv funn som tilsier høy risiko:	1. 2. 3.
Foreligger det plikt til eller unntak fra å gjennomføre DPIA etter GDPR art. 35?	☐ Plikt til å gjennomføre DPIA ☐ Unntak fra å gjennomføre DPIA
Hvilken personvernvurdering må gjennomføres?	☐ PLM ☐ DPIA

PLM og DPIA

4. Grunnleggende informasjon om planlagt behandling	PLM	DPIA
	4.A. Beskrivelse av behandlingen	4.A. Beskrivelse av behandlingen
	4.B. Behandlingens art	4.B. Behandlingens art (utvidet)
	4.C. Behandlingens omfang	4.C. Behandlingens omfang (utvidet)
	4.D. Behandlingens kontekst	4.D. Behandlingens kontekst (utvidet)
	4.E. Overføring til utlandet	4.E. Overføring til utlandet (utvidet)

5. Grunnleggende informasjon om formål	PLM	DPIA
	5. Behandlingens formål 5.A. Formål for førstegangsbehandling	5. Behandlingens formål og begrunnelse 5.A. Formål for førstegangsbehandling (utvidet)
	5.B. Formål ved viderebehandling	5.B. Formål ved viderebehandling (utvidet)
		5.C. Begrunnelse for formålet

PLM og DPIA

6. Behandlingens lovlighet	PLM	DPIA
	6. Behandlingens lovlighet	**6. Behandlingens lovlighet (utvidet)**
	6.A. Behandlingsgrunnlag	6.A. Behandlingsgrunnlag
	6.B. Samtykke	6.B. Samtykke

7. Behandlingens nødvendighet og proporsjonalitet	PLM	DPIA
	7.A. Nødvendighetsvurdering	7.A. Nødvendighetsvurdering (utvidet)
	7.B. Proporsjonalitetsvurdering	7.B. Proporsjonalitetsvurdering (utvidet)
	7.C. Ivaretakelse av personvernprinsippene	7.C. Ivaretakelse av personvernprinsippene (utvidet)
	7.D. Ivaretakelse av de registrertes rettigheter	7.D. Ivaretakelse av de registrertes rettigheter (utvidet)
	7.E. Ivaretakelse av de registrertes friheter	7.E. Ivaretakelse av de registrertes friheter (utvidet)
	7.F. Databehandlere	7.F. Databehandlere
		7.G. Samlet vurdering

PLM og DPIA

8. Risiko og tiltak	PLM	DPIA
	8.A. Personopplysningssikkerhetsrisiko	8.A. Personopplysningssikkerhetsrisiko (utvidet)
	8.B. Annen personvernrisiko	8.B. Personvernprinsipprisiko
		8.C. Rettighetsrisiko
		8.D. Frihetsrisiko
		8.E. Oppsummering av restrisiko

Oppdage og forebygge

Vedlegg X

DPIA risikoanalyse: personvernprinsipper, rettigheter og friheter

ID	Områder	Uønsket hendelse	Berørte	Årsak (utløsningskilde)	Konsekvens	Sann-synlighet	Risiko FØR tiltak	Tiltak	Antatt konsekvens etter tiltak	Antatt sann-synlighet etter tiltak	Risiko etter tiltak
	Risiko knyttet til Personvernprinsippene:										
	Lovlighet herunder behandlingsgrunnlag										
	Rettferdighet										
	Åpenhet og forutsigbarhet										
	Formålsbegrensninger										
	Dataminimering										
	Riktighet										
	Lagringsbegrensninger										
	Ansvarlighet										
	Risiko knyttet til den registrertes rettigheter										
	Informasjon										
	Innsyn										
	Sletting										
	Retting										
	Begrensning av behandling (hvis relevant)										
	Dataportabilitet (hvis relevant)										
	Innsigelse (hvis relevant)										
	Profilering/automatiserte avgjørelser (hvis relevant)										
	Risiko knyttet til den registrertes friheter										
	Privatliv, familieliv, hjem og kommunikasjon										
	Likebehandling										
	Ytringsfrihet										
	Tanke-, tros- og religionsfrihet										

Pause

Vi starter igjen ca. kl. 10:10

Oslo

Personvernhåndbok

Personvernsarbeid i Bydel Søndre Nordstrand

Personvernkoordinator
Hana Temsamani

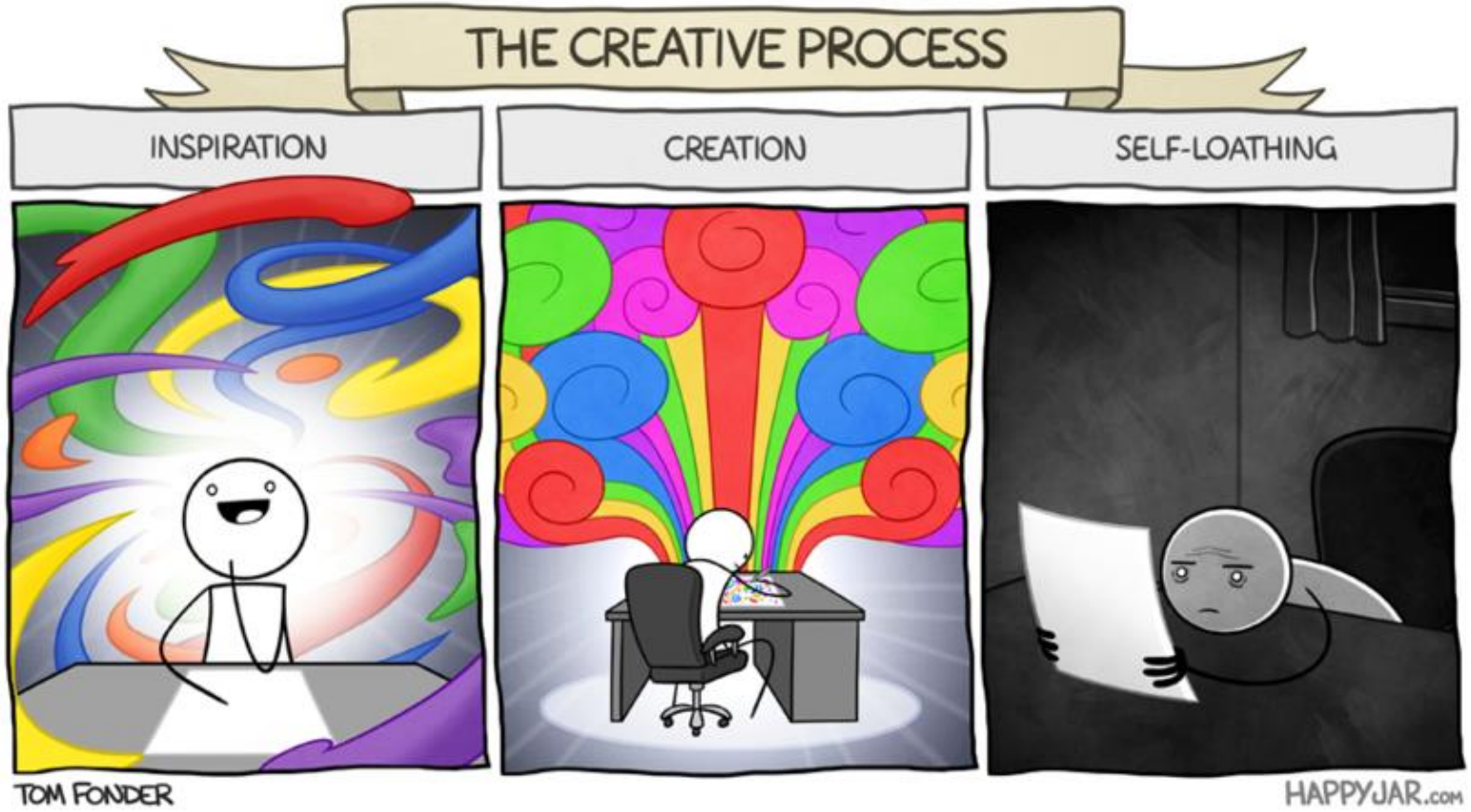
Rammen for presentasjonen

- Formål
- Prosess
- Resultatet
- Utbytte
- Veien videre

Formål med å utarbeide en håndbok

- **Personvern skal være en integrert del av arbeidet som utføres i bydelen**
  - Både for ledere og ansatte
- **Mye uklarheter rundt personvern**
  - Hva er lov og ikke lov?
  - Definisjoner
- **Hvordan det skal jobbes med i praksis**
  - Personvern kommer «i veien» for alt annet arbeid som må utføres
- **Uttrykk for at det er utydelige løsninger på etterlevelse av personvern**
  - Mye e-postbruk
- **Avviksmeldinger på personvernområdet**
  - EQS

Prosessen rundt utformingen av håndboken



Prosessen rundt utformingen av håndboken

- **Henvendelser til personvernkoordinator og jurist avdekker et behov for en kortfattet og oppklarende «oppslagsverk»**
  - Håndbok fremfor rutiner/veiledere
- **Sendt ut på høring i enhet juridisk og internkontroll, personvernombud og i nettverket for PK og ISK**
- **Innføring og ikke ment til å være et omfattende og fullstendig opplæringsmateriale**
  - Introduksjon som systematiserer personvernområdet

Resultatet

Personvernhåndbok i Bydel Søndre Nordstrand

Utbytte

- **Flere henvendelser til personvernkoordinator**
  - Med spørsmål som berører avvik og hvordan disse skal løses i praksis, eksempelvis kryptering
- **Flere avviksmeldinger på personvern og informasjonssikkerhet i EQS**
  - Økning av meldinger til Datatilsynet
- **Større grad av integrasjon av personvernarbeidet i bydelen**
  - Enhetsledere som setter personvern i sine strategi- og målplaner
  - Anskaffelser
  - Raskere ut med løsninger

Veien videre

- **Utarbeide veiledere til samtlige enheter/avdelinger som tilleggsdokumenter til håndboken**
  - Mer målrettet opp mot deres virke
  - Øke graden av integrasjon mellom arbeidsoppgavene som utføres og personvern
- **Håndboken er dynamisk**
  - Innholdet i håndboken er ikke statisk og må derfor oppdateres jevnlig

- Personvernhåndboken: https://bsn.intranett.oslo.kommune.no/administrative-tjenester-og-ikt/juridisk-og-internkontroll/personvern-og-informasjonssikkerhet/for-ansatte/opplaring/

Takk for oppmerksomheten!

Oslo

Selvbetjeningsløsning om informasjonssikkerhet og personvern

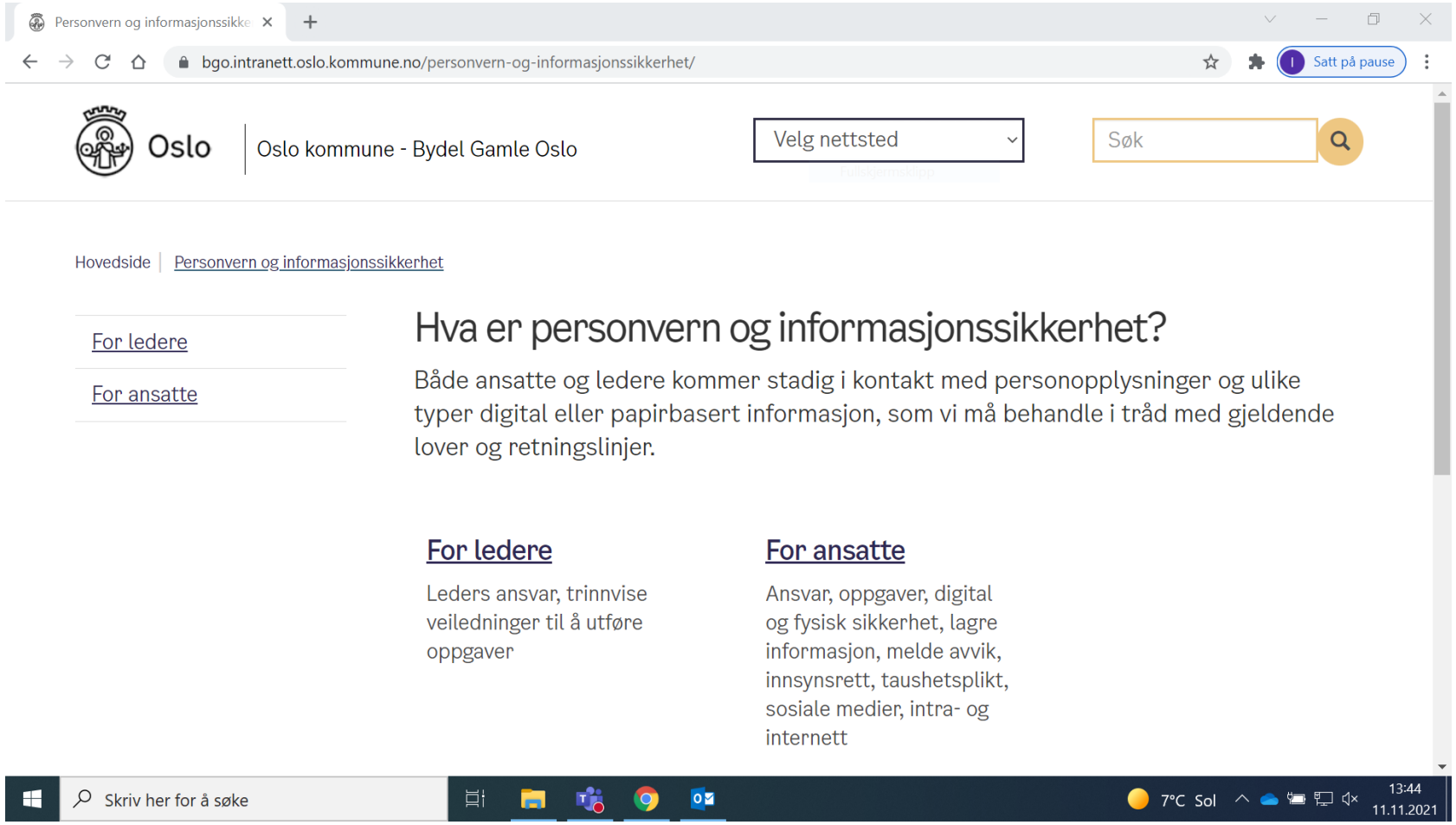
Bydel Gamle Oslo

Ida Marie Larsen

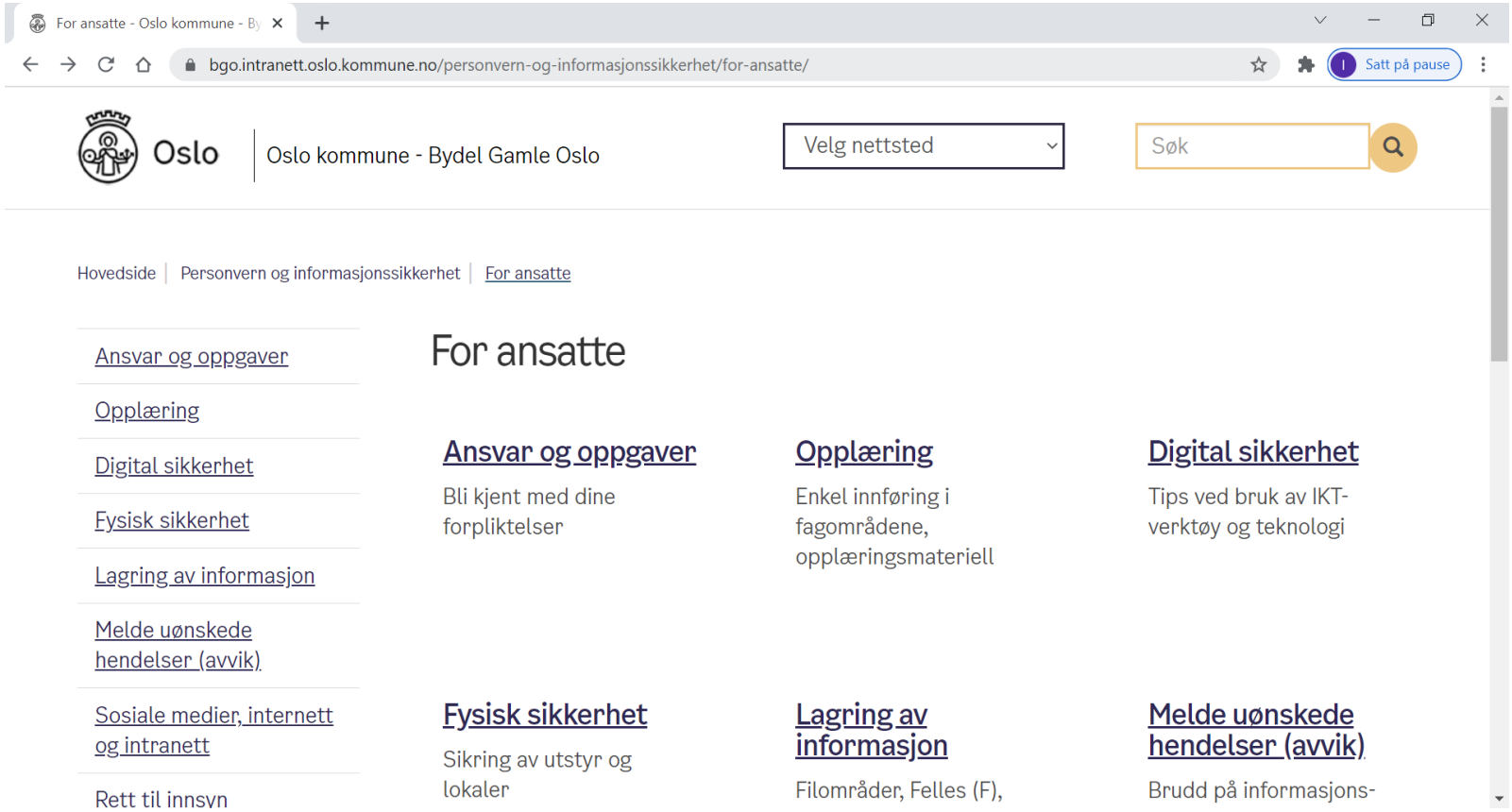
Hva jeg skal snakke om

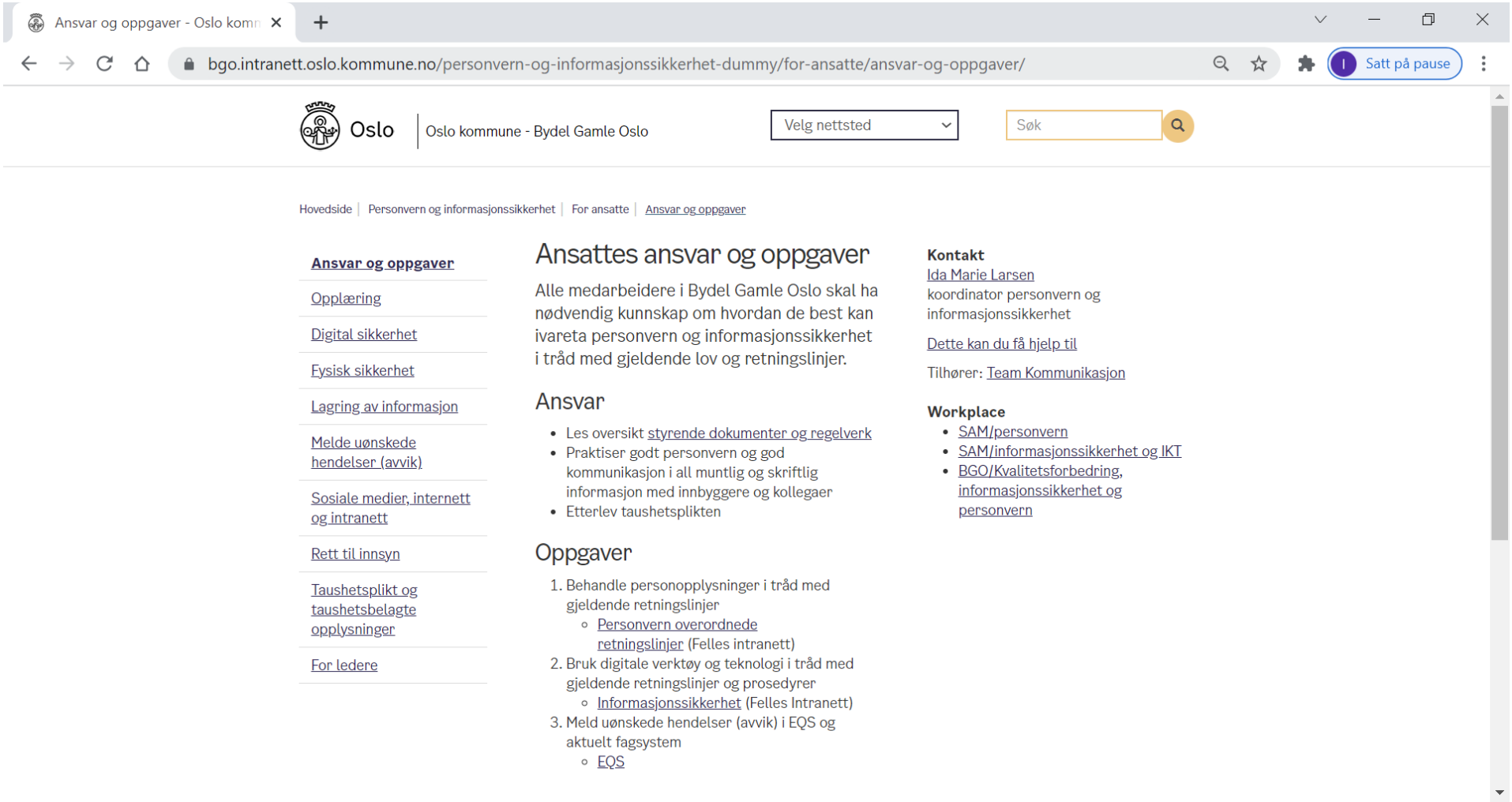
- Hva er en selvbetjeningsløsning?
- Hvorfor har vi laget en slik løsning?
- Hvordan har vi laget den?
- Filmsnutt

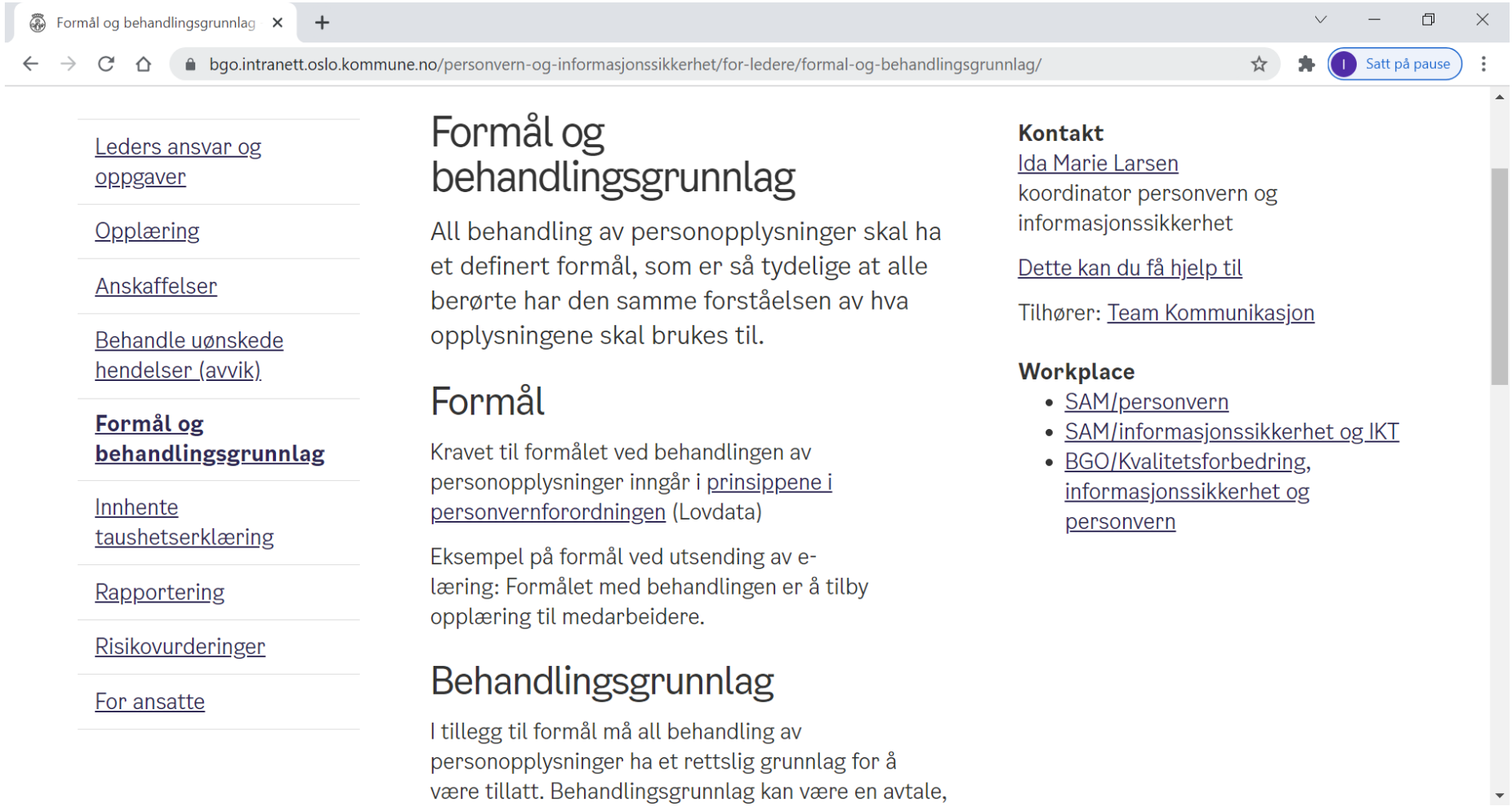
Hva er en selvbetjeningsløsning?



Hvorfor?


For ansatte - Oslo kommune - By
bgo.intranett.oslo.kommune.no/personvern-og-informasjonssikkerhet/for-ansatte/
Satt på pause
Oslo
Oslo kommune - Bydel Gamle Oslo
Velg nettsted
Søk
Hovedside | Personvern og informasjonssikkerhet | For ansatte
Ansvar og oppgaver
Opplæring
Digital sikkerhet
Fysisk sikkerhet
Lagring av informasjon
Melde uønskede hendelser (avvik)
Sosiale medier, internett og intranett
Rett til innsyn
For ansatte
Ansvar og oppgaver
Bli kjent med dine forpliktelser
Opplæring
Enkel innføring i fagområdene, opplæringsmateriell
Digital sikkerhet
Tips ved bruk av IKT-verktøy og teknologi
Fysisk sikkerhet
Sikring av utstyr og lokaler
Lagring av informasjon
Filområder, Felles (F),
Melde uønskede hendelser (avvik)
Brudd på informasjons-


Ansvar og oppgaver - Oslo komm
bgo.intranett.oslo.kommune.no/personvern-og-informasjonssikkerhet-dummy/for-ansatte/ansvar-og-oppgaver/
Satt på pause
Oslo
Oslo kommune - Bydel Gamle Oslo
Velg nettsted
Søk
Hovedside | Personvern og informasjonssikkerhet | For ansatte | Ansvar og oppgaver
Ansvar og oppgaver
Opplæring
Digital sikkerhet
Fysisk sikkerhet
Lagring av informasjon
Melde uønskede hendelser (avvik)
Sosiale medier, internett og intranett
Rett til innsyn
Taushetsplikt og taushetsbelagte opplysninger
For ledere
Ansattes ansvar og oppgaver
Alle medarbeidere i Bydel Gamle Oslo skal ha nødvendig kunnskap om hvordan de best kan ivareta personvern og informasjonssikkerhet i tråd med gjeldende lov og retningslinjer.
Ansvar
Les oversikt styrende dokumenter og regelverk
Praktiser godt personvern og god kommunikasjon i all muntlig og skriftlig informasjon med innbyggere og kollegaer
Etterlev taushetsplikten
Oppgaver
1. Behandle personopplysninger i tråd med gjeldende retningslinjer
   - Personvern overordnede retningslinjer (Felles intranett)
2. Bruk digitale verktøy og teknologi i tråd med gjeldende retningslinjer og prosedyrer
   - Informasjonssikkerhet (Felles Intranett)
3. Meld uønskede hendelser (avvik) i EQS og aktuelt fagsystem
   - EQS
Kontakt
Ida Marie Larsen
koordinator personvern og informasjonssikkerhet
Dette kan du få hjelp til
Tilhører: Team Kommunikasjon
Workplace
SAM/personvern
SAM/informasjonssikkerhet og IKT
BGO/Kvalitetsforbedring, informasjonssikkerhet og personvern


Formål og behandlingsgrunnlag
bgo.intranett.oslo.kommune.no/personvern-og-informasjonssikkerhet/for-ledere/formal-og-behandlingsgrunnlag/
Satt på pause
Leders ansvar og oppgaver
Opplæring
Anskaffelser
Behandle uønskede hendelser (avvik)
Formål og behandlingsgrunnlag
Innhente taushetserklæring
Rapportering
Risikovurderinger
For ansatte
Formål og behandlingsgrunnlag
All behandling av personopplysninger skal ha et definert formål, som er så tydelige at alle berørte har den samme forståelsen av hva opplysningene skal brukes til.
Formål
Kravet til formålet ved behandlingen av personopplysninger inngår i prinsippene i personvernforordningen (Lovdata)
Eksempel på formål ved utsending av e-læring: Formålet med behandlingen er å tilby opplæring til medarbeidere.
Behandlingsgrunnlag
I tillegg til formål må all behandling av personopplysninger ha et rettslig grunnlag for å være tillatt. Behandlingsgrunnlag kan være en avtale,
Kontakt
Ida Marie Larsen
koordinator personvern og informasjonssikkerhet
Dette kan du få hjelp til
Tilhører: Team Kommunikasjon
Workplace
SAM/personvern
SAM/informasjonssikkerhet og IKT
BGO/Kvalitetsforbedring, informasjonssikkerhet og personvern

Hvordan?

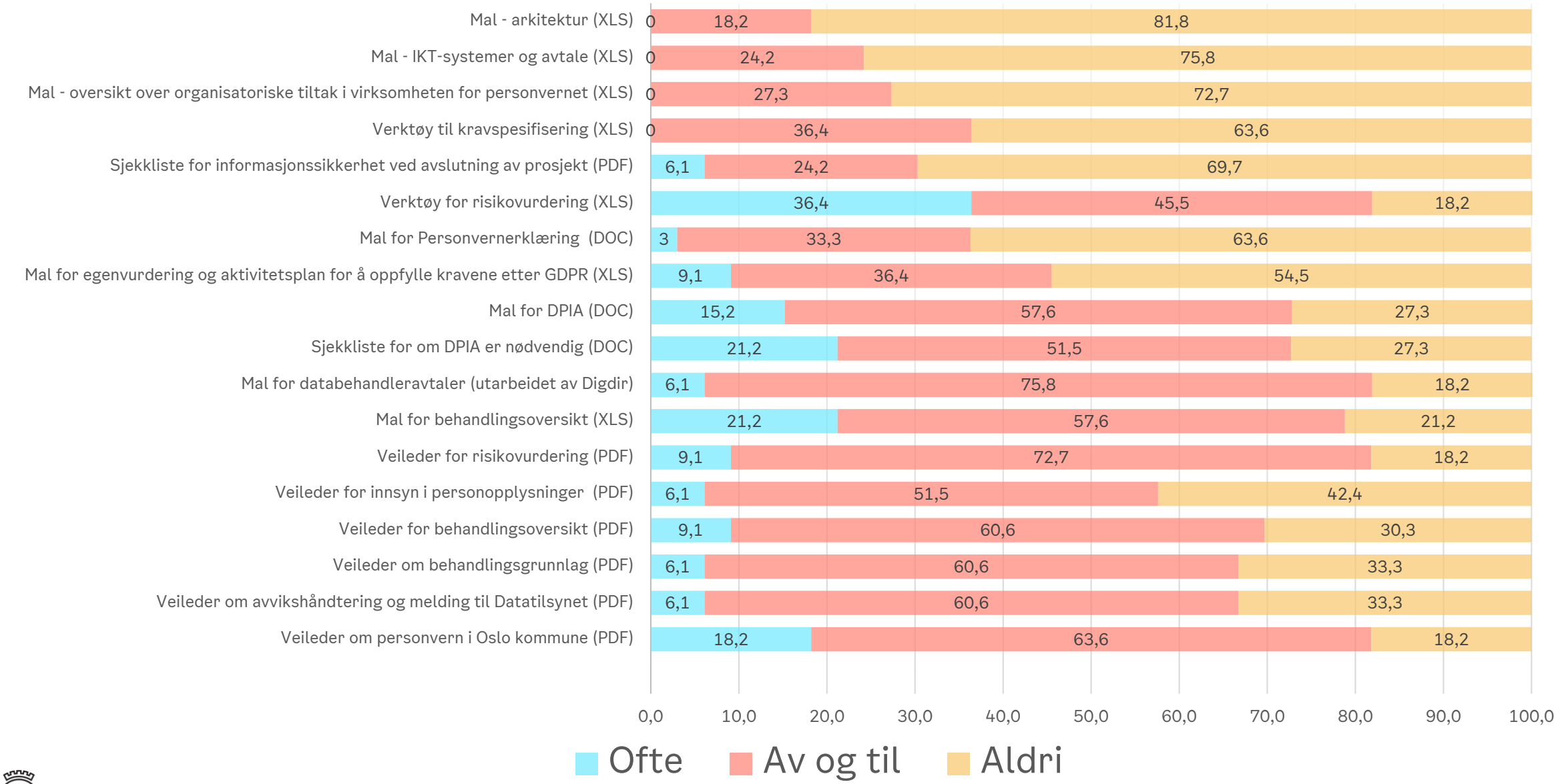
- Prosjekt
- Samarbeid på tvers av fag
- Definert fremdriftsplan med avsatt tid

#deling #testing #referanser

Snurr film!
https://oslo.workplace.com/groups/informasjonssikkerhetogpersonvernkooridnatorer/permalink/1189012061577555/

Flere verktøy...

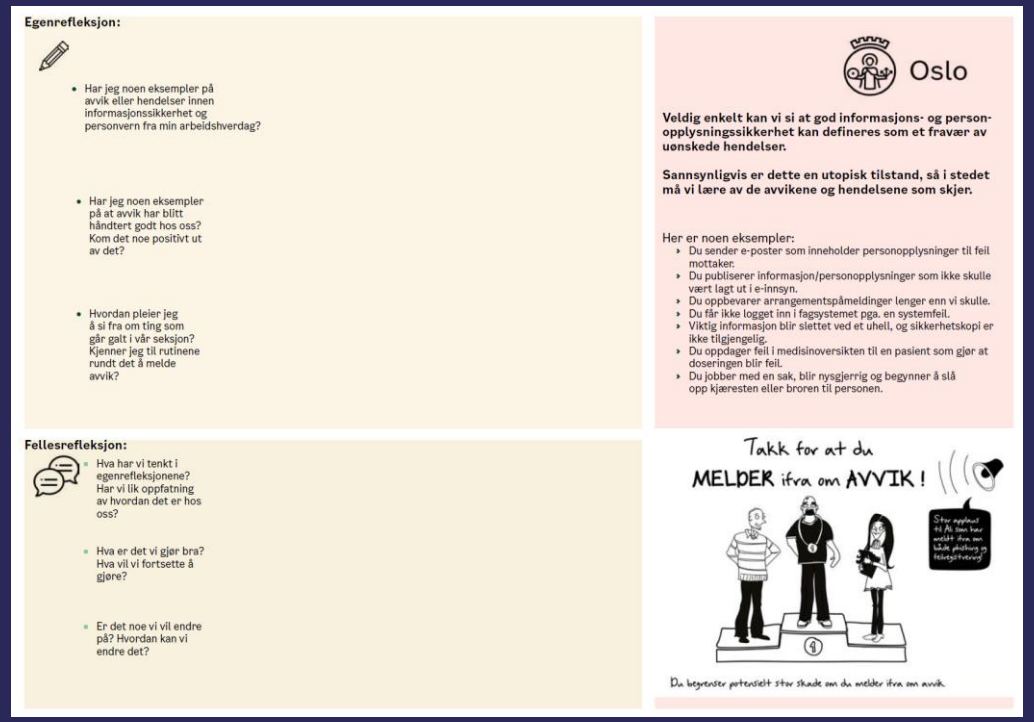
BRUK AV VERKTØY



Samtalekort – verktøy for grupper + Veileder om brudd på personopplysningssikkerheten

«Lider kommunen av en fryktkultur hvor man ikke melder avvik av redsel for å bli straffet eller er det noe annet?»

Personvernombudet i Oslo kommune



Ligger på Felles intranett:
https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/personvern/veiledninger-og-maler/avvikshandtering-og-melding-til-datatilsynet/

Ligger på Felles intranett:
https://felles.intranett.oslo.kommune.no/category.php?categoryID=90772

Aktiviteter framover

- Kurset i personvernvurderinger 1. desember er **fullt**, men følg med for nye datoer.
- Flere læringsaktiviteter kommer neste år.

Datoer for forum i 2022:

- 26. januar
- 2. mars
- 8. juni
- 7. september
- 30. november

E-læringer 2022:

Siste tirsdag hver måned!

Avslutning

- Det blir sendt ut en evaluering etter dette forumet
- Kom gjerne med forslag til temaer for neste år!

God jul!