

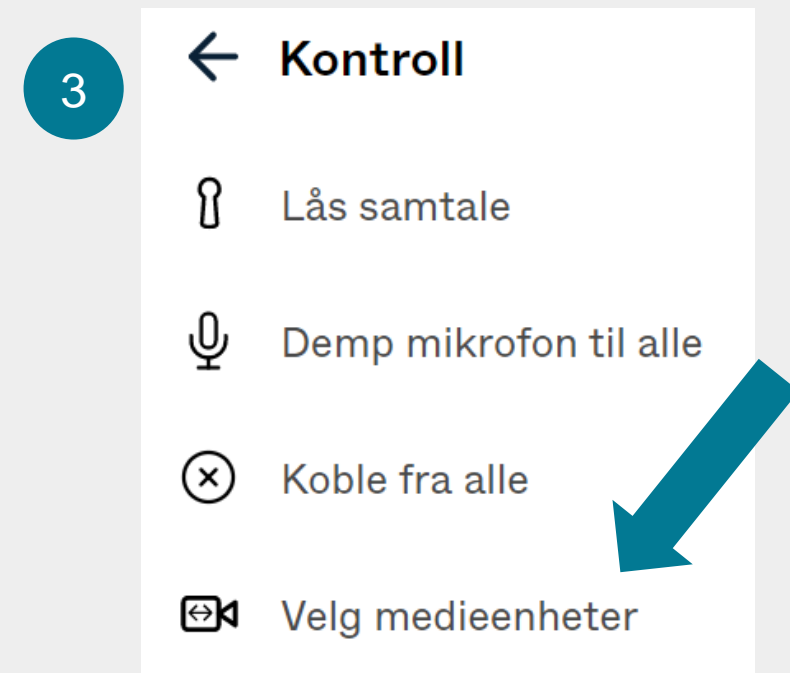
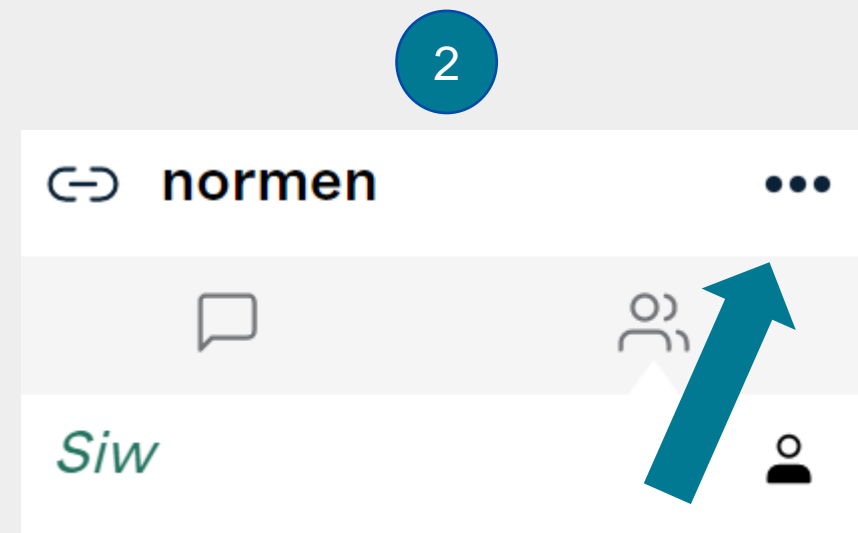
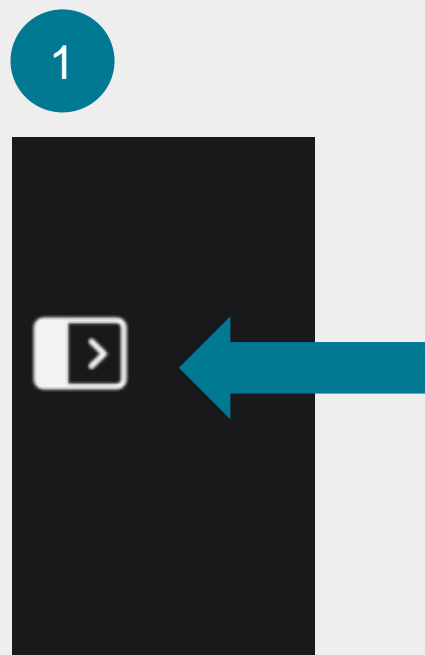


# **INNSPILLSWEBINAR: Veiledningsmaterieell – internkontroll og risikostyring**

Siw Tynes Johnsen  
Sekretariatet for Normen  
23.06.21

# Kjøreregeler

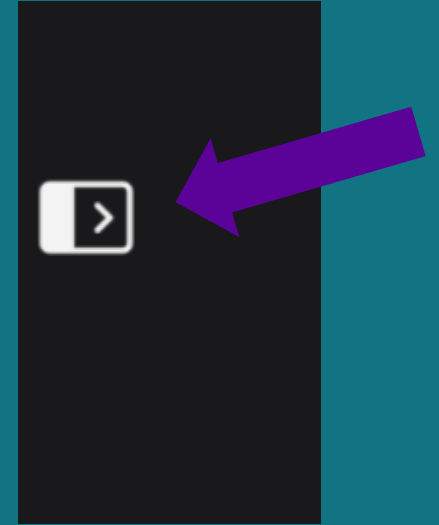
- Møteleder styrer ordet
- Sett mikrofonen på «mute» når du ikke snakker
- Det foretas ikke opptak av dette webinarret
- Presentasjonen legges ut på [normen.no](https://normen.no)
  
- Problemer med lyden?



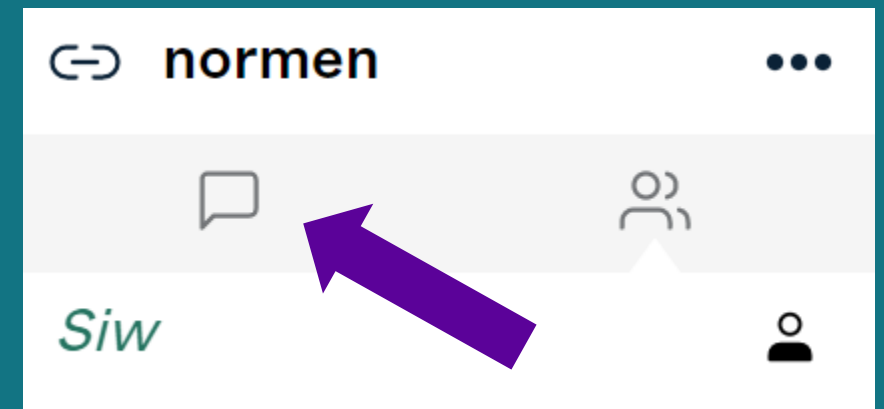
# Spørsmål og kommentarer underveis

- Bruk chatfunksjonen når som helst under webinaret til spørsmål eller kommentarer
- Vi svarer på spørsmål enten i plenum og/eller i chat
- Hvis du har spørsmål som ikke blir besvart under webinaret eller innspill du ønsker å komme med i etterkant, send oss en epost til [sikkerhetsnormen@ehelse.no](mailto:sikkerhetsnormen@ehelse.no)

1



2



# Agenda

- Introduksjon til veiledningspakken internkontroll og risikostyring
- Diskusjon og innspill
- Veien videre for veiledningspakken



# En liten forsmak på diskusjonstemaene ...

- Opplevs det hensiktsmessig å dele opp veiledningsmateriellet i to veiledere med tema internkontroll og risikostyring?
- Hvordan fungerer rekkefølgen i innholdsfortegnelsene?
- Er det temaer som mangler i innholdsfortegnelsene som bør med?
- Er det temaer som bør strykes eller løftes ut i andre veiledningsprodukter (egne faktaark eller lignende)?
- Bør personvernkonsekvensvurdering (DPIA) være en del av risikostyringsveilederen eller være et eget faktaark?





Introduksjon til veiledningspakken internkontroll  
og risikostyring

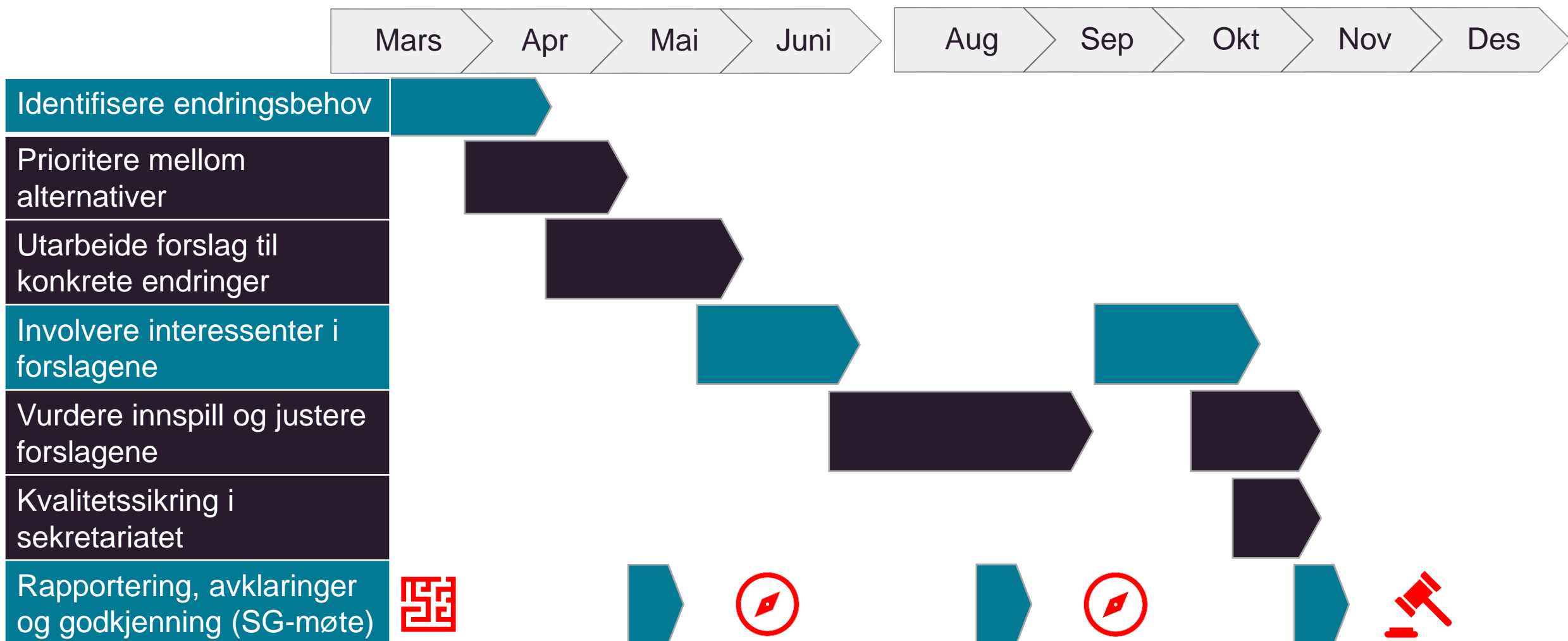
# Oppdatering av veiledningsmaterieill: Internkontroll og risikostyring

- Faktaark 01 Ansvar og organisering
- Faktaark 02 Styringsystem for informasjonssikkerhet og personvern
- Faktaark 04 Kartlegge og klassifisere systemer
- Faktaark 05 Fastsette nivå for akseptabel risiko
- Faktaark 07 Risikovurdering
- Faktaark 08 Avviksbehandling
- Faktaark 09 Opplæring av ledere og medarbeidere
- Faktaark 27 Retningslinjer for daglig informasjonssikkerhet
- Faktaark (nytt) om personvernkonsekvensvurdering (DPIA)
- Veileder for små helsevirksomheter
- Mal for internkontroll legekantor
- Mal for internkontroll psyk, fysio, manuell, og kiropraktor
- Mal for internkontroll tannhelsetjeneste
- Mal for internkontroll apotek

Temaer som  
inngår i  
arbeidspakken



# Plan for arbeidet med veiledningsmateriellet





# Kort om gjennomførte aktiviteter

- Innspill fra Normens styringsgruppe og andre aktører i sektoren
- Innspillseminar for nytt faktaark DPIA ble gjennomført 5. mai
  - Innspill om utfordringer, behov og eksempler/maler fra sektoren
- Referansegruppe med deltagere fra bredden av sektoren hadde møte i går
  - Konstruktiv faglig diskusjon om internkontroll og risikostyring, fokus på struktur og innhold i veiledningsmateriellet



# Målsetninger/prinsipper for veiledningsmaterieell i pakken

- Vise sammenhengene mellom ulike delprosesser
  - For eksempel mellom ulike typer risikovurderinger (informasjonssikkerhet, pasientsikkerhet, DPIA)
- Synliggjøre behovet for å veie ulike hensyn opp mot hverandre som del av risikostyringen
- Synliggjøre ledelsens ansvar og behov for beslutningsgrunnlag
- Ikke skrive mye om det samme mange steder
  - Unngå dobbeltarbeid både i arbeidet med veiledningsmateriellet og for virksomhetene som skal benytte materiellet i sine prosesser
- Sektorspesifikt og praktisk rettet
  - Ikke for teoretikerne, men for de som skal gjøre dette i praksis i sektoren

Hvordan  
oppnår vi  
dette?

# ... ved å organisere de faglige temaene på denne måten

## Internkontroll

Faktaark 01 - Ansvar og organisering
Faktaark 02 - Styringssystem for info.sikkerhet og personvern
Faktaark 08 - Avviksbehandling
Faktaark 09 - Opplæring av ledere og medarbeidere
Faktaark 27 - Retningslinjer for daglig informasjonssikkerhet
Nytt tema: sikkerhetskultur i helse- og omsorgssektoren
Maler og eksempler (bl.a. fra maler for internkontroll for små virksomheter)
Sette de ulike prosessene som er en del av internkontrollen mer i sammenheng
Beskrive at risikostyring er en del av den totale internkontrollen, henvise til risikoveileder

## Risikostyring

Faktaark 04 - Kartlegge og klassifisere systemer
Faktaark 05 - Fastsette nivå for akseptabel risiko
Faktaark 07 - Risikovurdering
DPIA – eget faktaark eller del av risikoveileder?
Maler og eksempler
Sette de ulike prosessene som er en del av risikostyringen mer i sammenheng

Oppdatere og tilpasse veileder for små virksomheter ved behov, i tråd med ny veiledning og med riktige henvisninger

# Veileder i internkontroll – forslag til innhold/struktur

<b>1</b>	<b>Innledning.....</b>	<b>6</b>
1.1	Om veilederen.....	6
1.1.1	Kjært barn har mange navn .....	6
1.1.2	Avgrensninger.....	6
1.1.3	Om forholdet til veileder i risikostyring .....	6
1.2	Om Normen.....	6
<b>2</b>	<b>Om internkontroll i helse- og omsorgssektoren .....</b>	<b>6</b>
2.1	Hvorfor er internkontroll viktig i helse- og omsorgssektoren? .....	7
2.2	Helhetlig internkontroll i virksomheten .....	7
<b>3</b>	<b>Sentrale krav i Normen .....</b>	<b>7</b>
3.1	Roller og ansvar for informasjonssikkerhet og personvern .....	7
3.1.1	Dataansvarliges ansvar .....	7
3.1.2	Databehandlers ansvar.....	7
3.2	Styringssystem for informasjonssikkerhet og personvern.....	9
3.2.1	Styrende, gjennomførende og kontrollerende.....	10
3.2.2	Om forholdet til standarden ISO/IEC 27001 .....	12
3.2.3	Om forholdet til virksomhetens øvrige styringssystem.....	12
3.3	Ledelsens gjennomgang.....	12

# Veileder i internkontroll forts.

3.4	Avvik.....	13
3.4.1	Sikkerhetsbrudd og brudd på personopplysningssikkerheten .....	13
3.4.2	Avvikshåndtering.....	14
3.5	Medarbeidere, kompetanse og holdningsskapende arbeid .....	19
3.5.1	Sikkerhetskultur .....	19
3.5.2	Opplæringsprogram .....	19
3.5.3	Retningslinjer for daglig informasjonssikkerhet.....	20
<b>4</b>	<b>Vedlegg – maler og eksempler .....</b>	<b>23</b>
4.1	Eksempel på roller og ansvar i virksomhet .....	23
4.2	Eksempel på avviksskjema .....	23
4.3	Eksempel på opplæringsplan.....	24

# Veileder i risikostyring – forslag til innhold/struktur

<b>1</b>	<b>Innledning.....</b>	<b>7</b>
1.1	Om veilederen.....	7
1.1.1	Avgrensninger.....	7
1.1.2	Om forholdet til veileder i internkontroll.....	7
1.1.3	Om forholdet til faktaark DPIA (dersom eget faktaark) .....	7
1.2	Om Normen.....	7
<b>2</b>	<b>Om risiko i helse- og omsorgssektoren .....</b>	<b>7</b>
2.1	Risiko, risikostyring og risikovurdering .....	8
2.2	Risiko for informasjonssikkerheten, personvernet og pasientsikkerheten .....	8
2.3	Helhetlig risikostyring – et lederansvar .....	8
2.3.1	Å veie ulike hensyn opp mot hverandre .....	8
<b>3</b>	<b>Sentrale krav i Normen .....</b>	<b>9</b>
3.1	Forholdsmessighet og risikobasert tilnærming.....	9
3.2	Normens minimumskrav .....	9
3.2.1	Konfidensialitet.....	9
3.2.2	Integritet .....	9
3.2.3	Tilgjengelighet.....	9
3.2.4	Robusket.....	9

# Veileder i risikostyring forts.

3.3	Hvem har ansvar for hva?.....	9
3.3.1	Roller og ansvar.....	9
3.3.2	Særlig om ledelsens ansvar.....	9
3.4	Hvordan skaffe oversikt?.....	9
3.4.1	Kartlegge og klassifisere systemer .....	9
3.4.2	Fylle ut behandlingsprotokollen .....	12
3.4.3	Fastsette nivå for akseptabel risiko.....	12
3.5	Risikovurdering .....	12
3.5.1	Verdivurdering.....	14
3.5.2	Scenarier og trusselvurdering .....	14
3.5.3	Sannsynlighet og konsekvens .....	14
3.5.4	Risikoreduserende tiltak.....	14
3.5.5	Risikoaksept.....	14
3.6	Vurdering av personvernkonsekvenser.....	15
<b>4</b>	<b>Vedlegg – maler og eksempler.....</b>	<b>16</b>
4.1	Eksempel på skala for sannsynlighet og konsekvens.....	16
4.2	Eksempel på mal for risikovurdering .....	18



Diskusjon – ordet er fritt!



# Hva tenker dere?

- Opplevs det hensiktsmessig å dele opp veiledningsmateriellet i to veiledere med tema internkontroll og risikostyring?
- Fordeler og ulemper?



# Hva tenker dere?

- Hvordan fungerer rekkefølgen i innholdsfortegnelsene?
- Er det temaer som mangler i innholdsfortegnelsene som bør med?
- Er det temaer som bør strykes eller løftes ut i andre veiledningsprodukter (egne faktaark eller lignende)?



# Hva tenker dere?

- Bør personvernkonsekvensvurdering (DPIA) være en del av risikostyringsveilederen eller være et eget faktaark?
- Fordeler og ulemper?





Veien videre for veiledningspakken og referansegruppen

## Veien videre ...

- Etterarbeid fra referansegruppemøte i går og dagens innspillswebinar – skriveperiode juni-august
- Innspill og beslutninger i styringsgruppemøte 20. september
- Referansegruppemøter i oktober
- Legges frem for godkjenning av Normens styringsgruppe 1-2. desember
- Planlagt publisering desember 2021



# Ta gjerne kontakt om du har innspill til Normens veiledningsmateriell!

- Hva trenger du?
- Hva mangler?
- Hva kan oppdatert veiledningsmateriell bidra med?



**[sikkerhetsnormen@ehelse.no](mailto:sikkerhetsnormen@ehelse.no)**

# PS! Vi fortsetter med webinarer etter sommerferien 😊

Temaer «på blokka» for høstens webinarer er blant annet nytt faktaark om personvernprinsippene, faktaark om hjemmekontor, veileder om medisinsk utstyr ...

Ta gjerne kontakt om du ønsker deg et tema!

**Følg med på [normen.no](https://normen.no), sosiale medier og Normens nyhetsbrev!**



Takk for gode innspill – og ikke minst  
**god sommer fra oss i Normen!**