Normen for leverandører

Webinar 18. november 2020

Normkonferansen 2020

24.november

- Hovedtema: «Hva har 2020 lært oss med tanke på digital sikkerhet og personvern?»
  - Hvordan håndterte helsesektoren personvern og informasjonssikkerhetsspørsmål i 2020?
  - 10 års digitalisering på 3 dager
  - Er det noen som utnytter krisen? (Trusselbildet)
  - Krystallkulen

- Påmelding https://attendee.gotowebinar.com/register/8787026147467072l6
- Link for påmelding og fullt program finnes også på ehelse.no → Arrangementer

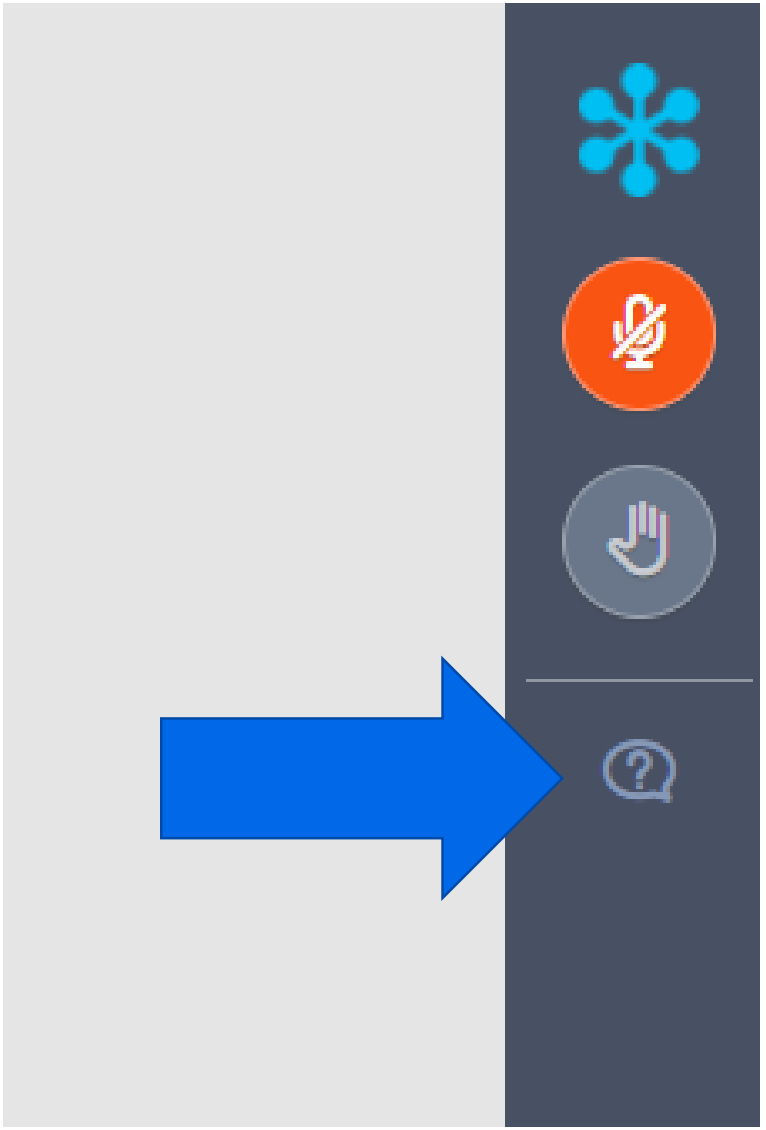
Kjøreregler

- Møteleder styrer ordet
- Deltagernes mikrofoner er mutet som standardinnstilling
- Det foretas ikke opptak av dette webinaret
- Deaktiver fullskjermsmodus dersom du har problemer med å svare på poll
- Presentasjonene legges ut på kurssiden på normen.no

- Vil du vite mer om hvordan vi jobber med GoToWebinar? Se mer på https://ehelse.no/normen/aktuelt-om-normen/digital-kompetanseheving-med-normen

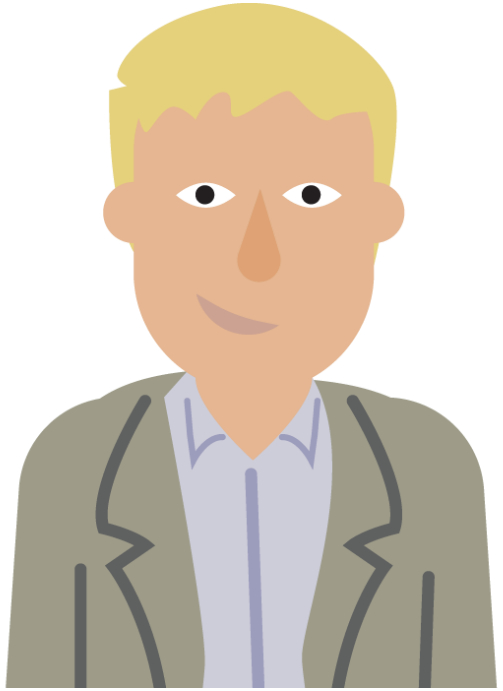
Spørsmål underveis

- Bruk spørsmålsfunksjonen når som helst under foredragene
- Vi lagrer spørsmålet ditt, men ikke hvem det kommer fra.
- Hvis du har spørsmål som ikke blir besvart under kurset, send oss en epost til sikkerhetsnormen@ehelse.no



Hensikten med webinaret

- Orientere om hvordan Normens krav treffer leverandører av IKT-tjenester og produkter til helse- og omsorgssektoren
- Gå nærmere inn på noen få krav



Poll nr 1:

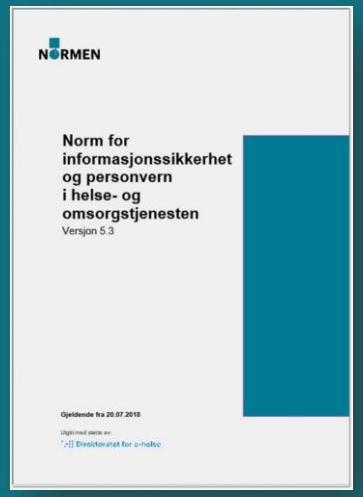
Hvem har vi med oss?

NORMEN

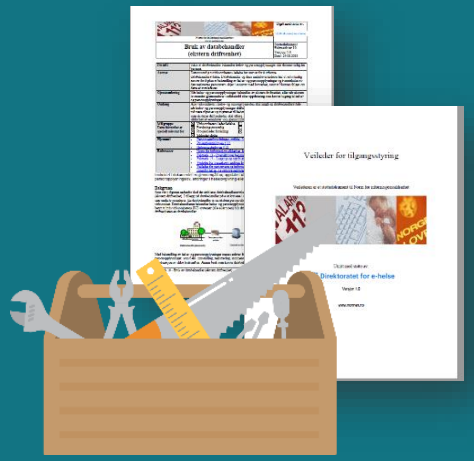
Hva er Normen?

Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren

Bransjenormen



Veiledning



Arena

Norges første og største bransjenorm for informasjonssikkerhet – og fra 2018 også for personvern

Vil du vite mer: **normen.no**

NORMEN

NORMEN

Gjelder Normen for leverandører?

Gjelder Normen for leverandører?

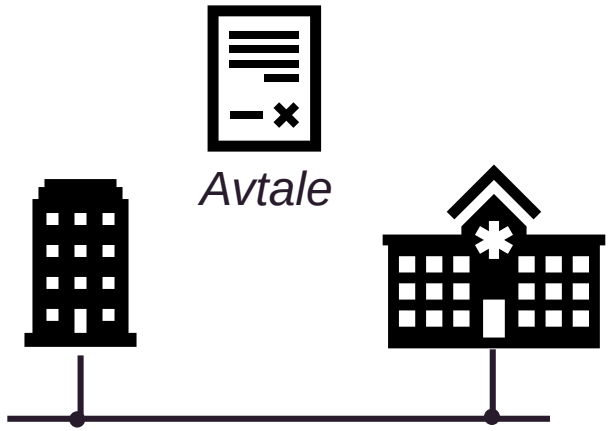
- Normen gjelder for enhver virksomhet som **ved avtale** har forpliktet seg til å følge den.
- Leverandøren skal t**ilrettelegge for at dataansvarlig** som tar i bruk leverandørens produkter og tjenester, **kan oppfylle lovbestemte krav og krav i Normen**.
- **Hvilke av Normens krav** som gjennom avtale gjelder for leverandører, er **avhengig av hva slags type leveranse** det er snakk om, for eksempel:
  - databehandling, i form av for eksempel skytjenester eller driftstjenester
  - vedlikehold, for eksempel ved fysisk service eller fjernaksess
  - leveranse av løsninger og systemer

NORMEN

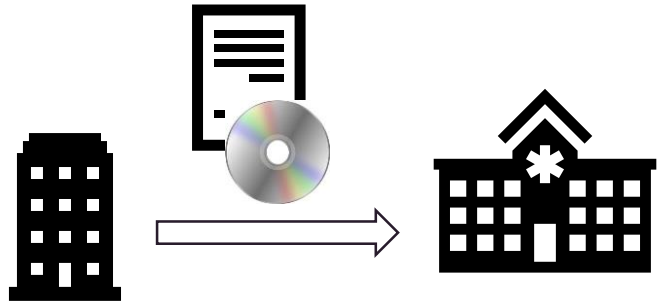
NORMEN

Det står i kravspesifikasjonen:
«Leverandøren skal følge kravene i Normen»
Hva betyr egentlig det?

Hvordan treffes leverandører av Normens krav? - det avhenger av hva som leveres!



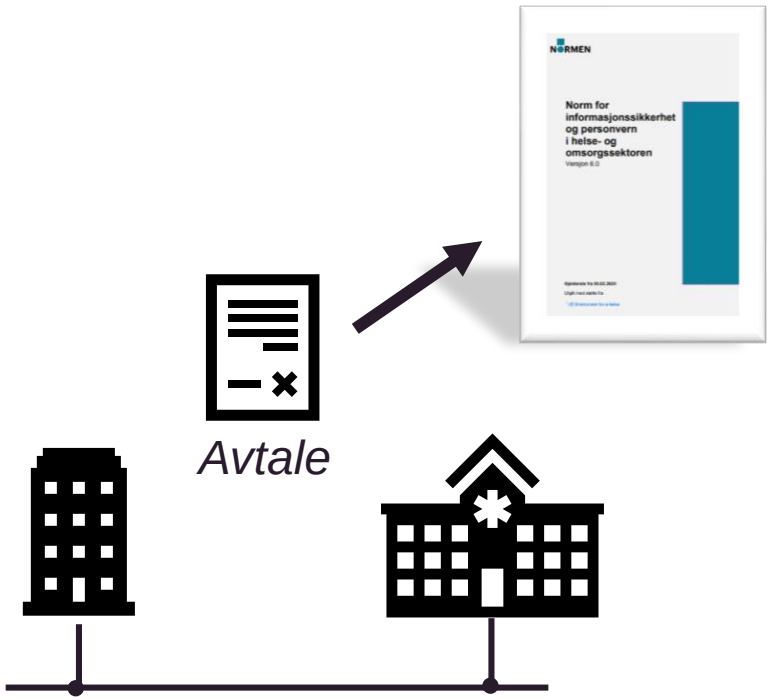
Databehandler, tjenestetilbyder, support osv



Programvareleverandør

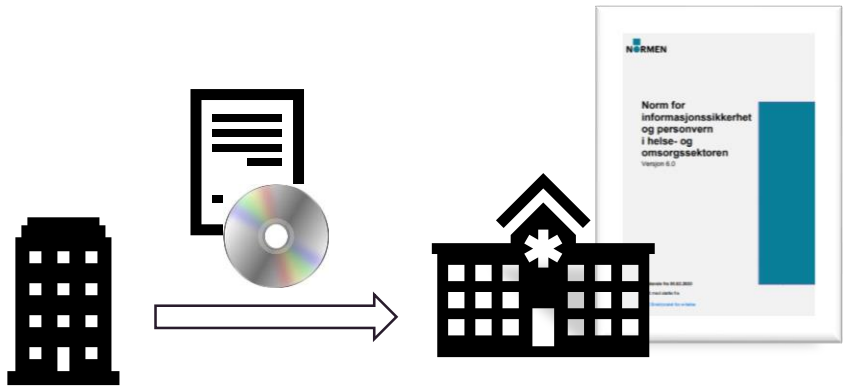
NORMEN

Databehandler, tjenestetilbyder, supportleverandør…



- Leverandøren er gjennom **avtale** forpliktet til å følge relevante krav i Normen
  - **Gjennom tilknytning til helsenettet**
  - Gjennom andre avtaler
    - Databehandleravtaler
    - Tjenesteavtale
    - Avtale om fjernsupport
    - …

Programvareleverandører



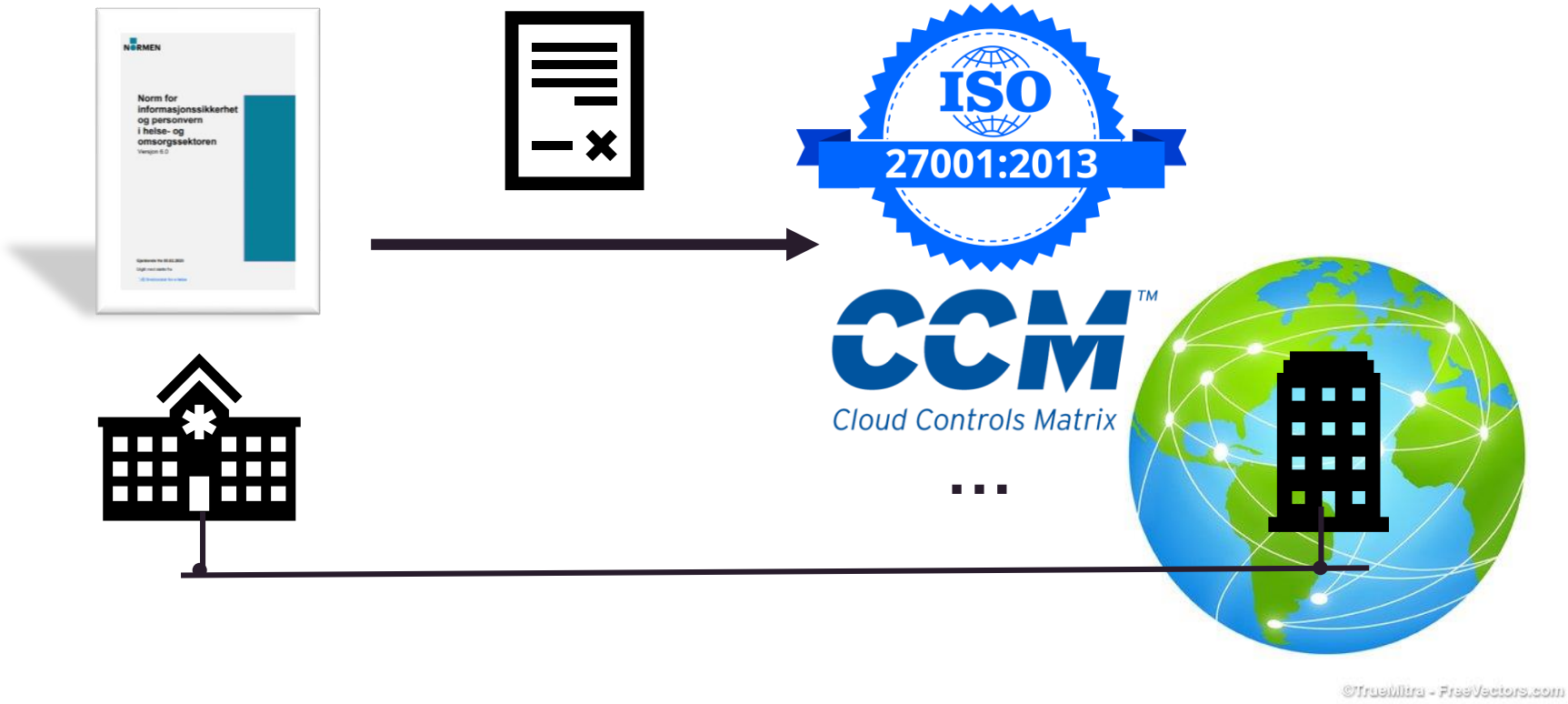
- For at virksomhetene skal kunne ivareta sitt ansvar som dataansvarlig, skal informasjonssystemene ha funksjonalitet som oppfyller lovbestemte krav og relevante krav i Normen
- Medfører at det må stilles **krav til funksjonalitet** i leverandørens programvare
- **Innbygd personvern**
- Hvis leverandøren **også** tilbyr support-tjenester, drift, SaaS osv vil leverandøren gjennom avtale kunne omfattes av Normens krav direkte

NORMEN

NORMEN

Så Google og Amazon skal følge Normen de nå ?!

Ansvaret for å om nødvending *oversette* kravene ligger hos den dataansvarlige



NORMEN

Hvordan skal vi få til dette?

Et nyttig hjelpemiddel: Vedlegget Normens krav

Normen

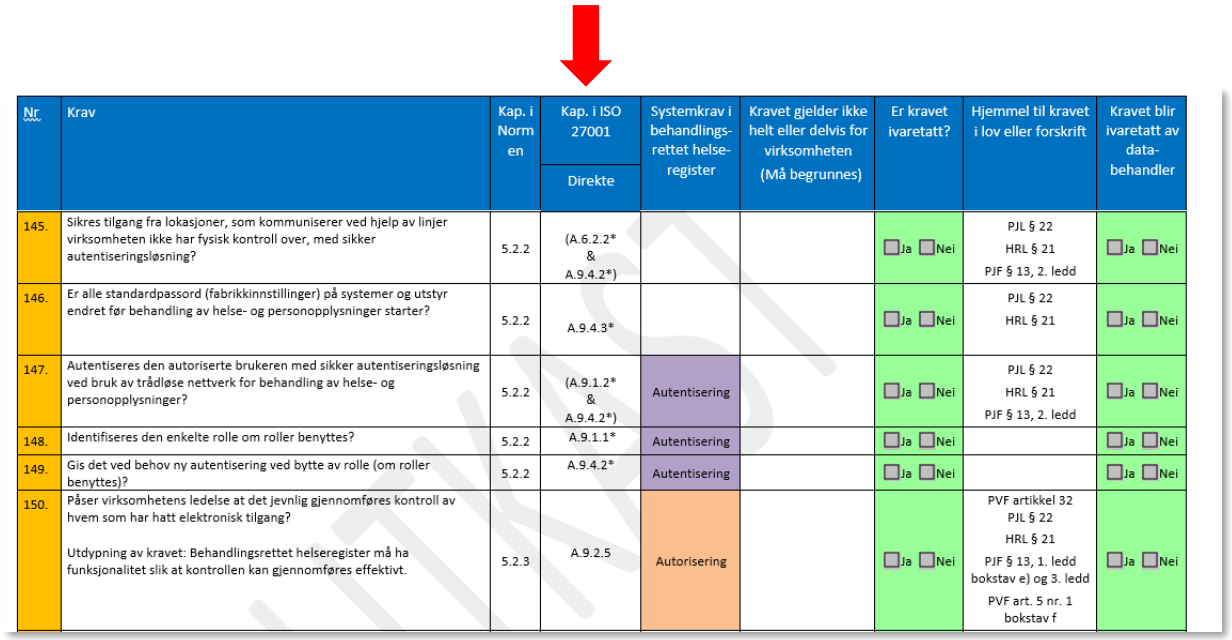
Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket.

NORMEN

Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren →

Normen er en bransjenorm for informasjonssikkerhet og personvern og utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren

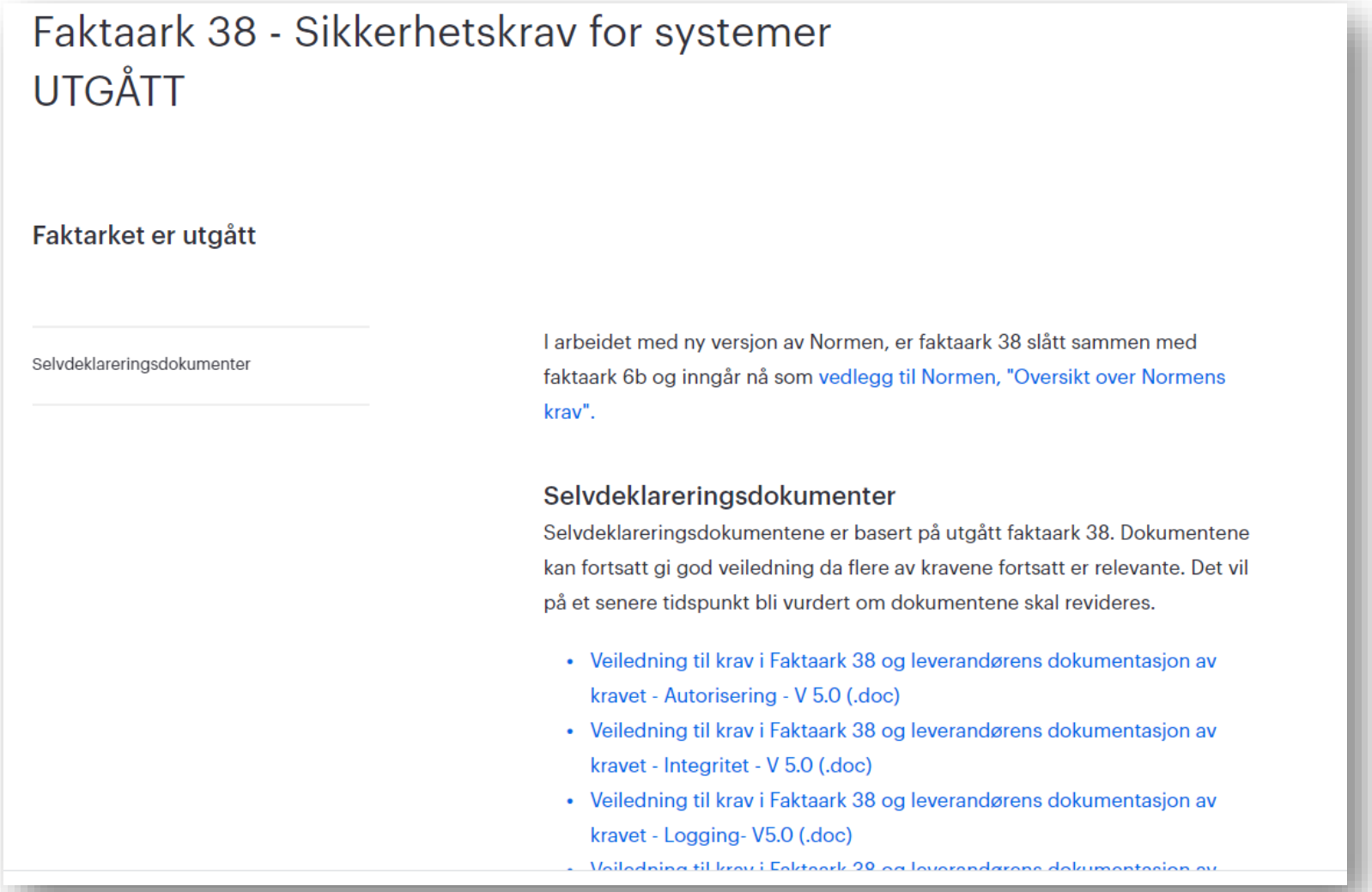
Oversikt over Normens krav, og mapping mellom ISO og Normen →



Nr	Krav	Kap. i Normen	Kap. i ISO 27001 Direkte	Systemkrav i behandlingsrettet helseregister	Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes)	Er kravet ivaretatt?	Hjemmel til kravet i lov eller forskrift	Kravet blir ivaretatt av databehandler
145.	Sikres tilgang fra lokasjoner, som kommuniserer ved hjelp av linjer virksomheten ikke har fysisk kontroll over, med sikker autentiseringsløsning?	5.2.2	(A.6.2.2* & A.9.4.2*)			☐Ja ☐Nei	PJL § 22 HRL § 21 PJF § 13, 2. ledd	☐Ja ☐Nei
146.	Er alle standardpassord (fabrikkinnstillinger) på systemer og utstyr endret før behandling av helse- og personopplysninger starter?	5.2.2	A.9.4.3*			☐Ja ☐Nei	PJL § 22 HRL § 21	☐Ja ☐Nei
147.	Autentiseres den autoriserte brukeren med sikker autentiseringsløsning ved bruk av trådløse nettverk for behandling av helse- og personopplysninger?	5.2.2	(A.9.1.2* & A.9.4.2*)	Autentisering		☐Ja ☐Nei	PJL § 22 HRL § 21 PJF § 13, 2. ledd	☐Ja ☐Nei
148.	Identifiseres den enkelte rolle om roller benyttes?	5.2.2	A.9.1.1*	Autentisering		☐Ja ☐Nei		☐Ja ☐Nei
149.	Gis det ved behov ny autentisering ved bytte av rolle (om roller benyttes)?	5.2.2	A.9.4.2*	Autentisering		☐Ja ☐Nei		☐Ja ☐Nei
150.	Påser virksomhetens ledelse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang? Utdypning av kravet: Behandlingsrettet helseregister må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt.	5.2.3	A.9.2.5	Autorisering		☐Ja ☐Nei	PVF artikkel 32 PJL § 22 HRL § 21 PJF § 13, 1. ledd bokstav e) og 3. ledd PVF art. 5 nr. 1 bokstav f	☐Ja ☐Nei

Bruk sorteringsfunksjonen i Word for å sortere krav f.eks alle systemkrav

Selvdeklareringsdokumetene da?



Faktaark 38 - Sikkerhetskrav for systemer
UTGÅTT

Faktarket er utgått

Selvdeklareringsdokumenter

I arbeidet med ny versjon av Normen, er faktaark 38 slått sammen med faktaark 6b og inngår nå som vedlegg til Normen, "Oversikt over Normens krav".

Selvdeklareringsdokumenter

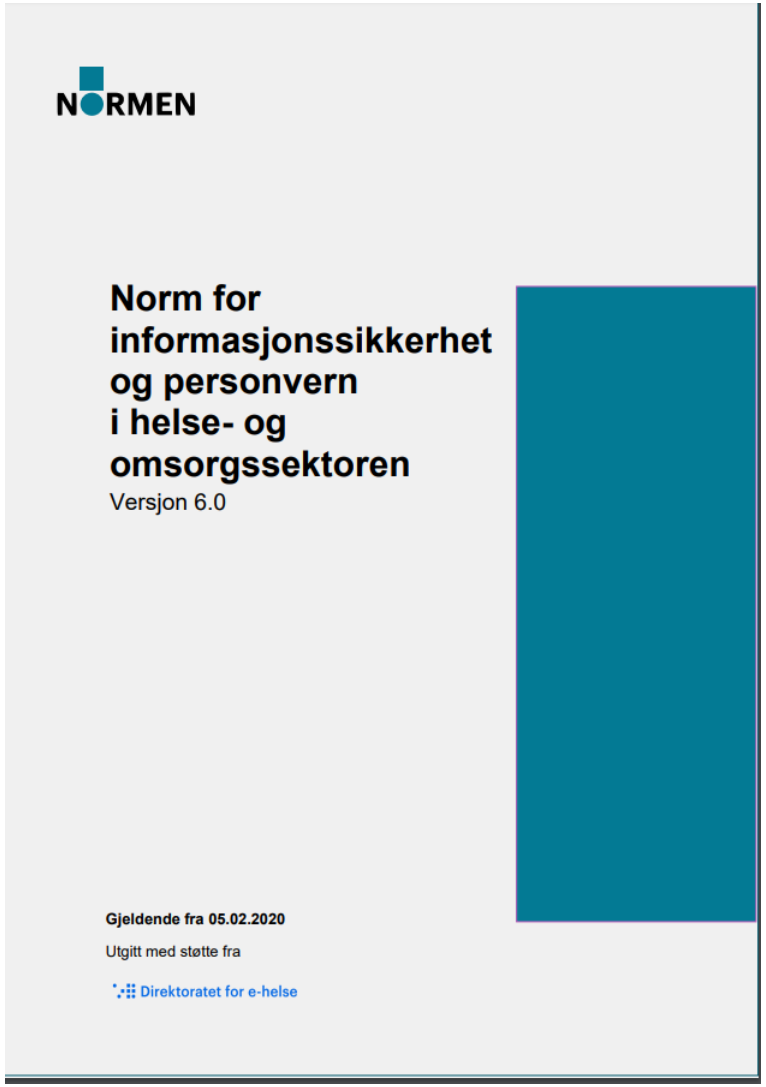
Selvdeklareringsdokumentene er basert på utgått faktaark 38. Dokumentene kan fortsatt gi god veiledning da flere av kravene fortsatt er relevante. Det vil på et senere tidspunkt bli vurdert om dokumentene skal revideres.

- Veiledning til krav i Faktaark 38 og leverandørens dokumentasjon av kravet - Autorisering - V 5.0 (.doc)
- Veiledning til krav i Faktaark 38 og leverandørens dokumentasjon av kravet - Integritet - V 5.0 (.doc)
- Veiledning til krav i Faktaark 38 og leverandørens dokumentasjon av kravet - Logging- V5.0 (.doc)

Hvilke krav stiller Normen til leverandøroppfølging og avtaler?

Normen 6.0:
Kapittel 5.7 Leverandører og avtaler

5.7.1 Krav til leverandørers taushetsplikt
5.7.2 Generelt om avtaler og leverandøroppfølging
5.7.3 Tjenesteutsetting
5.7.4 Databehandler
5.7.5 Vedlikehold, fjernaksess eller fysisk service
5.7.6 Systemleverandører
5.7.7 Leverandøroppfølging
5.7.8 Overføring av opplysninger til utlandet
5.7.9 Skytjenester



Poll nr 2:

Hva sier Normen om taushetserklæringer fra leverandørens ansatte?

5.7.3: Tjenesteutsetting:

- Dokumentert risikovurdering
  - Vurdering av landrisiko hvis relevant
- Beskrivelse av oppgaver og ansvar
- Løsning og konfigurasjonskart
- Rett til revisjon (kan foretas av avtalt tredjepart)
- Ved terminering:
  - God plan for ivaretakelse av informasjonssikkerhet og personvern
  - Signert erklæring fra leverandør om tilbakelevering / sletting av data innen avtalt tid

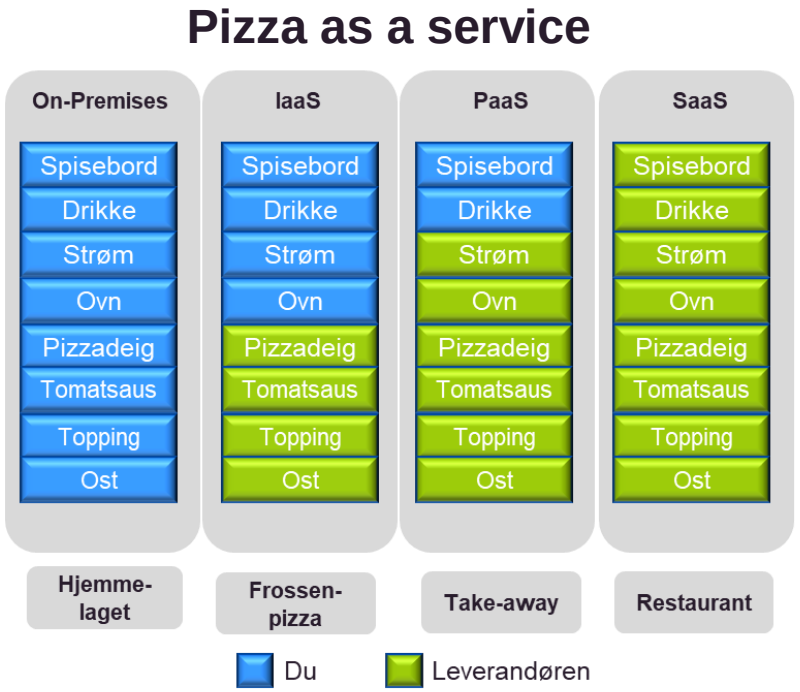
NORMEN

5.7.5 Vedlikehold, fjernaksess eller fysisk service

- Virksomheten skal, i tillegg til øvrige krav i Normen, gjennom avtale sørge for at
  - leverandørens utstyr som benyttes ved online oppkobling ved hjelp av kommunikasjonsnett, eller medbrakt utstyr som knyttes til virksomhetens utstyr, **ikke har ondsinnet programvare som inneholder virus e.l., og at utstyret er sikret mot adgang fra uvedkommende.**
  - all tilgang og fysisk adgang skal være **autorisert av virksomheten. Tilgangen skal logges og adgangen skal kontrolleres.**
  - tilgjengelighet til helse- og personopplysninger **så vidt mulig skal opprettholdes** når leverandøren utfører arbeid på virksomhetens utstyr/programvare.

5.7.9 Skytjenester

- Bruk av skytjenester ved behandling av helse- og personopplysninger krever at den dataansvarlige **gjør dekkende risikovurderinger**, og ellers følger kravene til avtaler og leverandøroppfølging i Normen.
- **Ansvarsfordelingen** avklart, og **tilpasset leveransemodellen** som benyttes
- Dataansvarlig har oversikt over **hvor data behandles geografisk**, slik at kravene i kapittel 5.7.8 kan ivaretas
- Dataansvarlig skal **påse at skyleverandørens eventuelle standardavtaler ikke er i motstrid** med lovbestemte krav og Normens krav
- Dataansvarlig har sørget for å ha en **god plan** for ivaretakelse av informasjonssikkerhet og personvern **ved avslutning** av skytjenesten



NORMEN

Flere spørsmål?

sikkerhetsnormen@ehelse.no

Normkonferansen 2020

24.november

- Hovedtema: «Hva har 2020 lært oss med tanke på digital sikkerhet og personvern?»
  - Hvordan håndterte helsesektoren personvern og informasjonssikkerhetsspørsmål i 2020?
  - 10 års digitalisering på 3 dager
  - Er det noen som utnytter krisen? (Trusselbildet)
  - Krystallkulen

- Påmelding https://attendee.gotowebinar.com/register/8787026147467072l6
- Link for påmelding og fullt program finnes også på ehelse.no → Arrangementer