# WEBINAR:

# «Oversikt over Normens krav»

11. November 2020

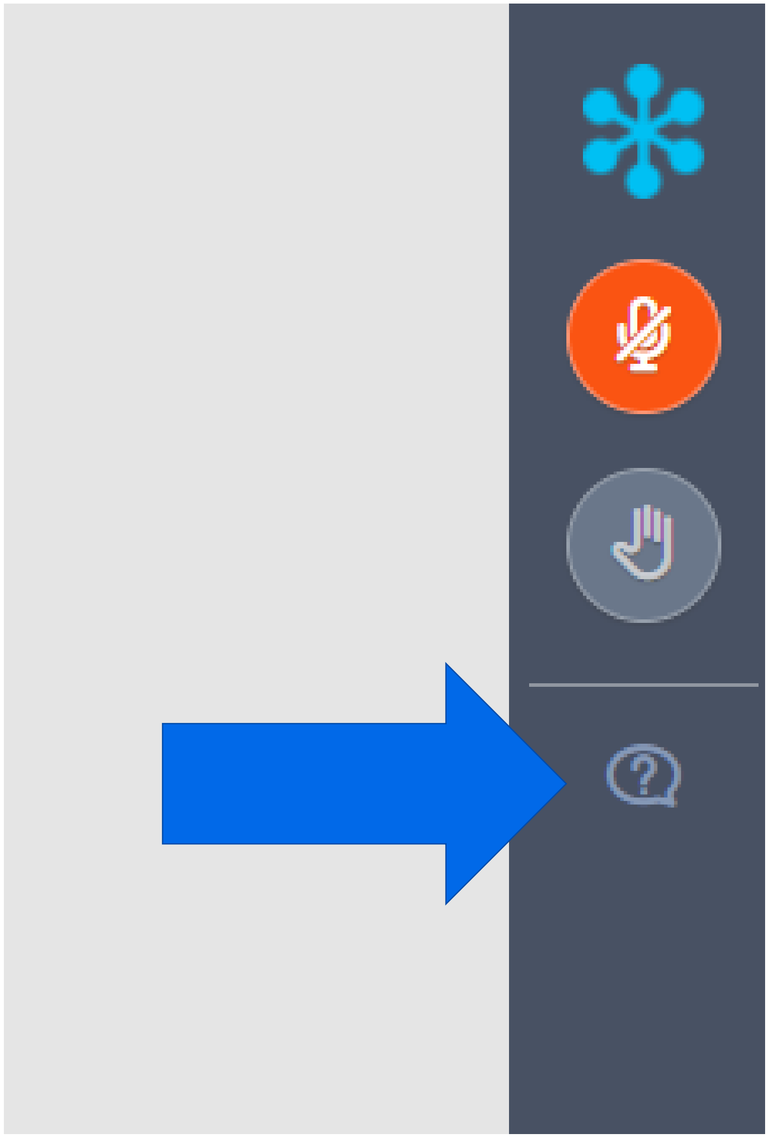
# Kjøreregler

- 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 vedlegget «Oversikt over Normens krav»
- Svare på spørsmål om vedlegget

# Bakgrunn

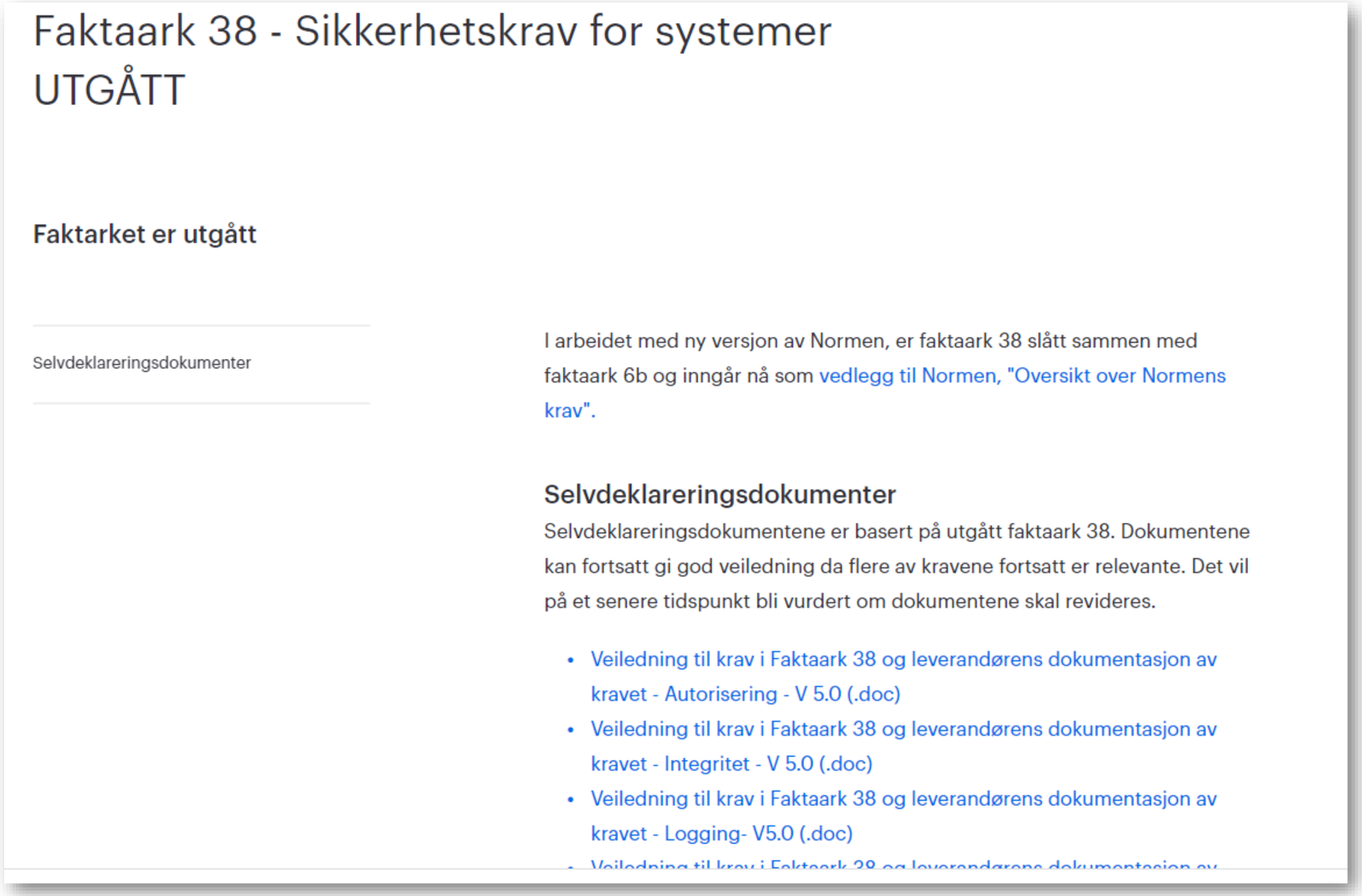

NORMEN
Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren
Versjon 6.0

# «Så mye hadde vi, og så mye fikk vi»

## Samlet oversikt Normens krav

| Nr | Krav (formulert som spørsmål) | Kap. i Normen | Kap. i ISO 27001 og Annex A | Systemkrav i behandlings-rettet helse-register | Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes) | Er kravet ivaretatt? | Hjemmel til kravet i lov eller forskrift | Kravet blir ivaretatt av data-behandler |
|---|---|---|---|---|---|---|---|---|
| 1. | Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv? | 1.5 | 6.1.1<br>8.1 | | | ☐ Ja ☐ Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21<br>FLK § 6 | |
| 2. | Er valgte tiltak basert på risikovurderinger? | 1.5 | 6.1.3<br>8.3 | | | ☐ Ja ☐ Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | ☐ Ja ☐ Nei |
| 3. | Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger? | 1.5 | 6.1*<br>8.1.* | | | ☐ Ja ☐ Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | |
| 4. | Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges? | 2 | 5.1<br>5.2<br>5.3 | | | ☐ Ja ☐ Nei | PJL § 22<br>HRL § 21<br>HTL § 5-10 første punktum<br>PVF artikkel 24<br>FLK § 7 | |
| 5. | Har virksomhetens øverste leder bestemt nivå for akseptabel risiko? | 2<br>3.2 | 6.1.2 | | | ☐ Ja ☐ Nei | PJL § 22<br>HRL § 21<br>PVF artikkel 32<br>FLK § 5 og 6 | ☐ Ja ☐ Nei |
| 6. | Har virksomhetens øverste leder bestemt regler for håndtering av risiko? | 2 | 6.1.3 | | | ☐ Ja ☐ Nei | PJL § 23<br>HRL § 22<br>PLF § 6 | ☐ Ja ☐ Nei |

# 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)

# «Så mye hadde vi, og så mye fikk vi»

## Samlet oversikt Normens krav

| Nr | Krav (formulert som spørsmål) | Kap. i Normen | Kap. i ISO 27001 og Annex A | 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 |
|---|---|---|---|---|---|---|---|---|
| 1. | Er valg av egnede tekniske og organisatoriske tiltak vurdert forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv? | 1.5 | 6.1.1<br>8.1 | | | ☐Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21<br>FLK § 6 | |
| 2. | Er valgte tiltak basert på risikovurderinger? | 1.5 | 6.1.3<br>8.3 | | | ☐Ja ☐Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 3. | Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger? | 1.5 | 6.1*<br>8.1.* | | | ☐Ja ☐Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | |
| 4. | Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges? | 2 | 5.1<br>5.2<br>5.3 | | | ☐Ja ☐Nei | PJL § 22<br>HRL § 21<br>HTL § 5-10 første punktum<br>PVF artikkel 24<br>FLK § 7 | |
| 5. | Har virksomhetens øverste leder bestemt nivå for akseptabel risiko? | 2<br>3.2 | 6.1.2 | | | ☐Ja ☐Nei | PJL § 22<br>HRL § 21<br>PVF artikkel 32<br>FLK § 5 og 6 | ☐Ja ☐Nei |
| 6. | Har virksomhetens øverste leder bestemt regler for håndtering av risiko? | 2 | 6.1.3 | | | ☐Ja ☐Nei | PJL § 23<br>HRL § 22<br>PLF § 6 | ☐Ja ☐Nei |

# Vedleggets hjemmelskolonne

- Formålet med kolonnen er å angi hvor kravet er hjemlet i lov eller forskrift, eller hvor kravet kan utledes fra.
- Kolonnen er ikke ment å være uttømmende
- Virksomheten er selv ansvarlig for å vurdere hvilke lovkrav som er gjeldende for sin virksomhet.

| Hjemmel til kravet i lov eller forskrift |
| --- |
| PVF artikkel 32<br>PJL § 22<br>HRL § 21<br>FLK § 6 |
| PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 |
| PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 |
| PJL § 22<br>HRL § 21<br>HTL § 5-10 første punktum<br>PVF artikkel 24<br>FLK § 7 |

NORMEN

# Databehandlerkolonnen

| Nr | Krav (formulert som spørsmål) | Kap. i Normen | Kap. i ISO 27001 og Annex A | Systemkrav i behandlings-rettet helse-register | Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes) | Er kravet ivaretatt? | Hjemmel til kravet i lov eller forskrift | Kravet blir ivaretatt av data-behandler |
|---|---|---|---|---|---|---|---|---|
| 1. | Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv? | 1.5 | 6.1.1<br>8.1 | | | ☐Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21<br>FLK § 6 | |
| 2. | Er valgte tiltak basert på risikovurderinger? | 1.5 | 6.1.3<br>8.3 | | | ☐Ja ☐Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 3. | Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger? | 1.5 | 6.1*<br>8.1.* | | | ☐Ja ☐Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | |
| 4. | Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges? | 2 | 5.1<br>5.2<br>5.3 | | | ☐Ja ☐Nei | PJL § 22<br>HRL § 21<br>HTL § 5-10 første punktum<br>PVF artikkel 24<br>FLK § 7 | |
| 5. | Har virksomhetens øverste leder bestemt nivå for akseptabel risiko? | 2<br>3.2 | 6.1.2 | | | ☐Ja ☐Nei | PJL § 22<br>HRL § 21<br>PVF artikkel 32<br>FLK § 5 og 6 | ☐Ja ☐Nei |
| 6. | Har virksomhetens øverste leder bestemt regler for håndtering av risiko? | 2 | 6.1.3 | | | ☐Ja ☐Nei | PJL § 23<br>HRL § 22<br>PLF § 6 | ☐Ja ☐Nei |
| 7. | Har virksomhetens øverste leder sørget for velfungerende styring og kontroll? | 2 | 6.2 | | | ☐Ja ☐Nei | PVF artikkel 24 første ledd<br>FLK §§ 3 og 4<br>PLF § 7 | ☐Ja ☐Nei |
| 8. | Er alle tiltak dokumentert | 2 | 6.1.3 | | | ☐Ja ☐Nei | PVF artikkel 5 nr. 2 og 32<br>PJL §§ 22 og 23 | ☐Ja ☐Nei |

# «ISO-mapping»

## Samlet oversikt Normens krav

| Nr | Krav (formulert som spørsmål) | Kap. i Normen | Kap. i ISO 27001 og Annex A | Systemkrav i behandlings-rettet helse-register | Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes) | Er kravet ivaretatt? | Hjemmel til kravet i lov eller forskrift | Kravet blir ivaretatt av data-behandler |
|---|---|---|---|---|---|---|---|---|
| 1. | Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv? | 1.5 | 6.1.1<br>8.1 | | | ☐Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21<br>FLK § 6 | |
| 2. | Er valgte tiltak basert på risikovurderinger? | 1.5 | 6.1.3<br>8.3 | | | ☐Ja ☐Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 3. | Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger? | 1.5 | 6.1*<br>8.1.* | | | ☐Ja ☐Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | |
| 4. | Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges? | 2 | 5.1<br>5.2<br>5.3 | | | ☐Ja ☐Nei | PJL § 22<br>HRL § 21<br>HTL § 5-10 første punktum<br>PVF artikkel 24<br>FLK § 7 | |
| 5. | Har virksomhetens øverste leder bestemt nivå for akseptabel risiko? | 2<br>3.2 | 6.1.2 | | | ☐Ja ☐Nei | PJL § 22<br>HRL § 21<br>PVF artikkel 32<br>FLK § 5 og 6 | ☐Ja ☐Nei |
| 6. | Har virksomhetens øverste leder bestemt regler for håndtering av risiko? | 2 | 6.1.3 | | | ☐Ja ☐Nei | PJL § 23<br>HRL § 22<br>PLF § 6 | ☐Ja ☐Nei |
| 7. | Har virksomhetens øverste leder sørget for velfungerende styring og kontroll? | 2 | 6.2 | | | ☐Ja ☐Nei | PVF artikkel 24 første ledd<br>FLK §§ 3 og 4<br>PLF § 7 | ☐Ja ☐Nei |
| 8. | Er alle tiltak dokumentert | 2 | 6.1.3 | | | ☐Ja ☐Nei | PVF artikkel 5 nr. 2 og 32<br>PJL §§ 22 og 23 | ☐Ja ☐Nei |

# ISO-mapping:
# Krav som har fullstendig overenstemmelse


Det er 114 av kravene i Normen som har fullstendig overenstemmelse med kravene i ISO 27001

# ISO-mapping:
# Krav i Normen som ikke er eksplisitt og fullstendig dekket i ISO 27001


166 krav er ikke eksplisitt og fullstendig dekket i ISO 27001
Av disse er 141 krav i Normen delvis dekket av ISO 27001.

# Cloud Security Alliance

## Samlet oversikt Normens krav

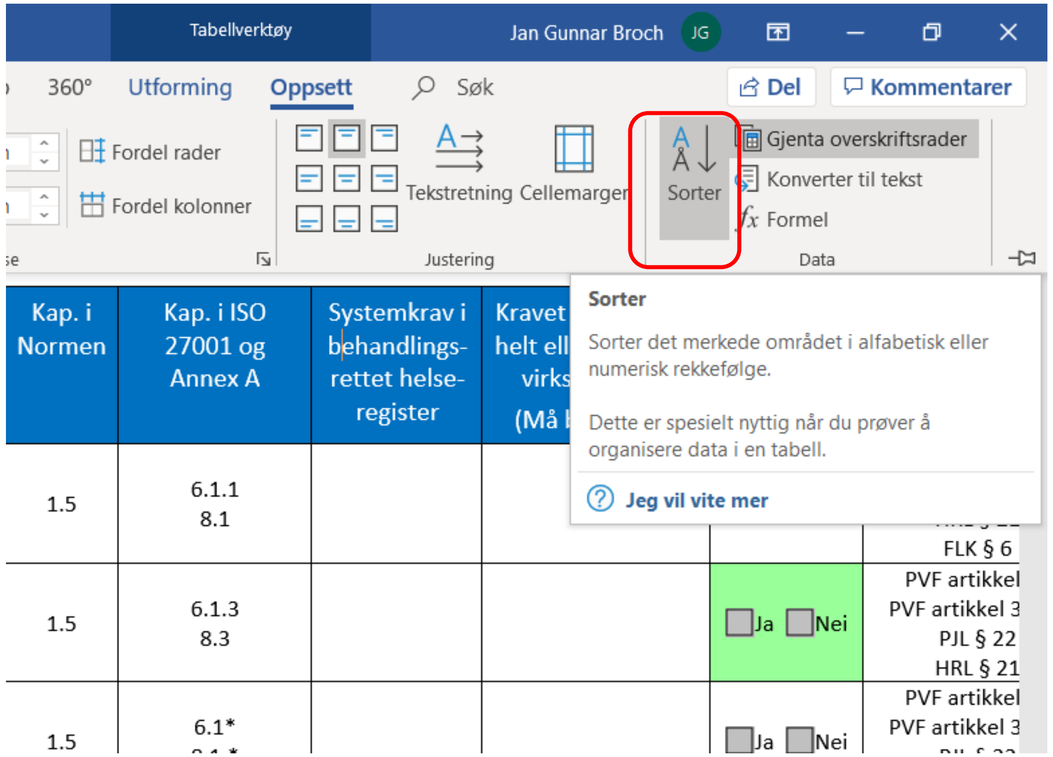
| Nr | Krav (formulert som spørsmål) | Kap. i Normen | Kap. i ISO 27001 og Annex A | CSA CCM Control ID | Systemkrav i behandlings-rettet helse-register | Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes) | Er kravet ivaretatt? | Hjemmel til kravet i lov eller forskrift | Kravet blir ivaretatt av data-behandler |
|---|---|---|---|---|---|---|---|---|---|
| 1. | Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv? | 1.5 | 6.1.1<br>8.1 | (GRM-09) | | | ☐Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21<br>FLK § 6 | |
| 2. | Er valgte tiltak basert på risikovurderinger? | 1.5 | 6.1.3<br>8.3 | GRM-08<br>STA-04 | | | ☐Ja ☐Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 3. | Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger? | 1.5 | 6.1*<br>8.1.* | (GRM-09) | | | ☐Ja ☐Nei | PVF artikkel 32<br>PVF artikkel 35 (1)<br>PJL § 22<br>HRL § 21 | |

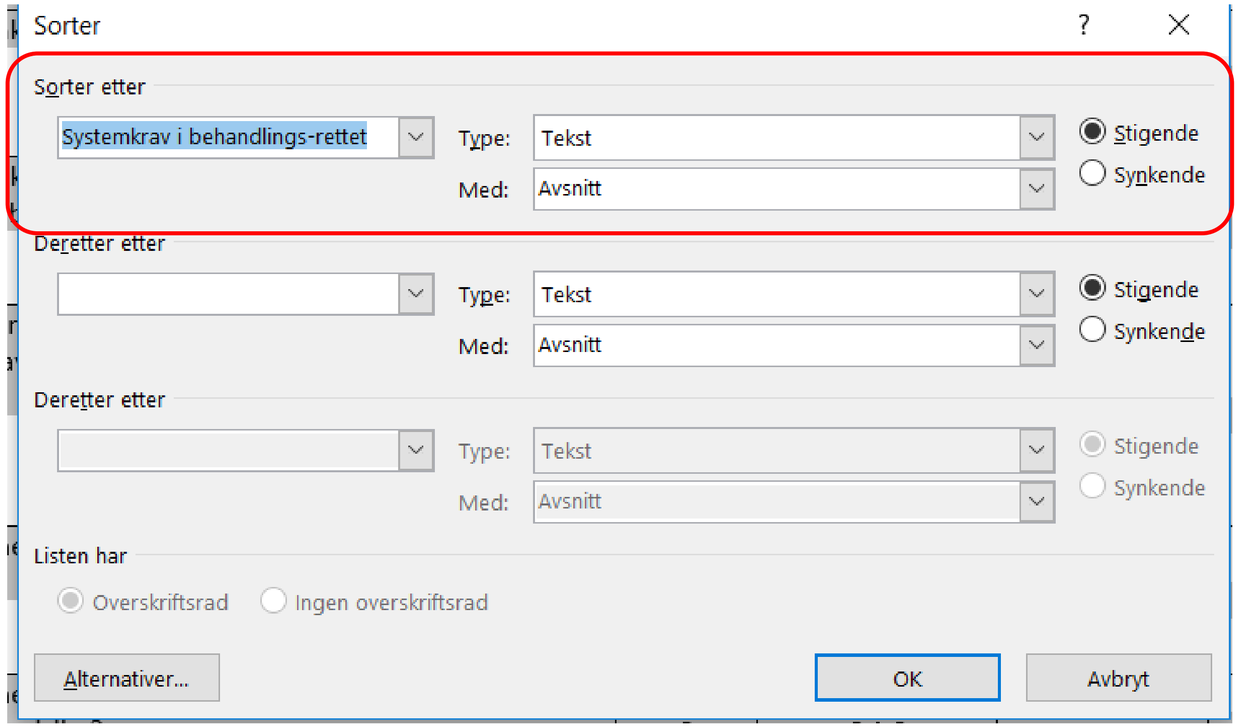
til Normens krav (Excel)

***«Hvordan kan vi plukke ut de kravene som er aktuelle i kravspesifikasjoner? (Savner faktaark 38 jeg..)»***

NORMEN

# Et triks:




**= alle systemkrav samlet**

# Forslag til bruk - revisjonssjekkliste

| Nr | Krav (formulert som spørsmål) | Kap. i Normen | Kap. i ISO 27001 og Annex A | Systemkrav i behandlings-rettet helse-register | Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes) | Er kravet ivaretatt? | Hjemmel til kravet i lov eller forskrift | Kravet blir ivaretatt av data-behandler |
|---|---|---|---|---|---|---|---|---|
| | • vurdering av risikoene for personvernet til den registrerte<br>• planlagte risikoreduserende tiltak for ivaretakelse av personvernet | | | | | | | |
| 62. | Blir personvernombudet, om det er utpekt, rådført ved gjennomføring av personvernkonsekvensvurderingen? | 3.5.1 | | | Er kun en ansatt, trenger ikke PVO | ☐ Ja ☒ Nei | PVF artikkel 39 (c) | ☐ Ja ☐ Nei |
| 63. | Blir det planlagt tiltak som reduserer risikoen for personvernet iht. personvernkonsekvensvurderingen? | 3.5.1 | | | | ☒ Ja ☐ Nei | PVF artikkel 35 | ☐ Ja ☐ Nei |
| 64. | Rådfører den dataansvarlige seg med Datatilsynet, før behandlingen starter, om behandlingen av helse- og personopplysninger vil medføre høy risiko som ikke kan reduseres ved hjelp av rimelige tiltak? | 3.5.1 | A.6.1.3* | | Har ikke behandlinger som medfører høy risiko | ☐ Ja ☐ Nei | PVF artikkel 36 | ☐ Ja ☐ Nei |
| 65. | Er behandlingsgrunnlag fastsatt før behandlingen av helse og personopplysningen starter, eller ved endringer i behandlingen? | 4.1 | | | | ☒ Ja ☐ Nei | PVF artikkel 5 nr. 1 bokstav a og 6 | |
| 66. | Dekker behandlingsgrunnlaget alle behandlingene som utføres, innsamling, registrering, lagring, sletting, utlevering, mv? | 4.1 | | | | ☒ Ja ☐ Nei | PVF artikkel 6 | |

# Forslag til bruk - anskaffelser

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 262. | Identifiseres den enkelte rolle om roller benyttes? | 5.2.2 | A.9.1.1* | Autentisering | | ☐Ja ☐Nei | | ☐Ja ☐Nei |
| 263. | 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 |
| 264. | Registreres all tildeling av autorisasjon i et autorisasjonsregister? | 5.2.1 | A.9.2.1* | Autorisasjon | | ☐Ja ☐Nei | PJF 13, 1.ledd, c) | ☐Ja ☐Nei |
| 265. | Er tilgangsstyring etablert for alle informasjonssystemer? | 5.2 | A.9.1 | Autorisering | | ☐Ja ☐Nei | PJL § 22<br>PJF § 13<br>HFL § 7, 1. ledd<br>HPL §25, 2.ledd<br>PVF artikkel 32 nr. 1 bokstav b | ☐Ja ☐Nei |
| 266. | Er tilgangsstyring etablert for administrator- og systembrukere? | 5.2 | A.9.2.3 | Autorisering | | ☐Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 267. | Gis tilgang til behandlingsrettede hels etter en konkret beslutning basert på iverksatt eller skal iverksettes tiltak fo medisinsk behandling av pasienten? | | | | | | | |
| 268. | Sikrer tildelt autorisasjon at den enke tilgang til relevante og nødvendige he personopplysninger i samsvar med pe ansvar og oppgaver, så langt lovbeste taushetsplikt ikke er til hinder for det | | | | | | | |
| 269. | Benyttes det roller i virksomheten ska autorisering for hver rolle skje uavher personellets øvrige roller? | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | PJF § 13 | |
| 123. | Sørger virksomheten for, innenfor rammen av taushetsplikten, at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte? | 5.2 | A.9.2* | AIS-04 | | | ☐Ja ☐Nei | PJL §§ 15,19<br>HPL §§ 21, 25<br>PVF artikkel 32 nr. 1 bokstav b | ☐Ja ☐Nei |
| 124. | Sørger virksomheten for at opplysningene gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten og personvernet? | 5.2 | A.9.1.1* | AIS-04 | | | ☐Ja ☐Nei | PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 125. | Er tilgangsstyring etablert for alle informasjonssystemer? | 5.2 | A.9.1 | IAM-02 | Autorisering | | ☐Ja ☐Nei | PJL § 22<br>PJF § 13<br>HFL § 7, 1. ledd<br>HPL §25, 2.ledd<br>PVF artikkel 32 nr. 1 bokstav b | ☐Ja ☐Nei |
| 126. | Er tilgangsstyring etablert for administrator- og systembrukere? | 5.2 | A.9.2.3 | IAM-09 | Autorisering | | ☐Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |

# Forslag til bruk -
# Leverandør som må følge Normens krav

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 110. | Er sikkerhetstiltak egnede og valgt på grunnlag av risikovurderinger? | 5 | 6.1.3 | | | ☒Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei | Ja, rutine for risikovurdering ivaretar kravet. Se rutine. |
| 111. | Vurderer virksomheten om det er nødvendig å gjennomføre mer omfattende tiltak enn det som er beskrevet i kapittel 5 i Normen? | 5 | 6.1.3 | | | ☒Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21<br>FLK § 8 | ☐Ja ☐Nei | Ja, rutine for risikovurdering ivaretar kravet. Se rutine. |
| 112. | Læres alle medarbeidere i virksomheten kontinuerlig opp i krav som gjelder ivaretakelse av taushetsplikten, informasjonssikkerheten og personvernet? | 5.1.1 | 7.2*<br>7.3*<br>A.7.2.2* | | | ☒Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21<br>FLK § 7 | ☐Ja ☐Nei | Ja, se ISMS for rutiner for opplæring |
| 113. | Innhenter virksomheten taushetserklæring for den enkelte medarbeider? | 5.1.1 | A.7.1.2<br>A.13.2.4 | | | ☒Ja ☐Nei | PJL § 15, 23<br>HRL § 22 | ☐Ja ☐Nei | Taushetserklæring signeres ved ansettelse. Se ellers rutine for bruk av eksterne/ konsulenter |

# Forslag til bruk - Leverandør som bruker ISO 27001

| Ref: ISO/IEC 27001:2017 | Fullstendig/delvis mapping | Kap i Normen | Nr i vedlegg i Normen | Krav i Normen | Kap i Normen | Nr i vedlegg i Normen | Krav i Normen | Kap i Normen | Nr i vedlegg i Normen | Krav i Normen |
|---|---|---|---|---|---|---|---|---|---|---|
| 4.1 | Fullstendig | 2.4 | 18 | Er styringssystemet tilpasset virksomhetens størrelse, risiko, egenart og aktiviteter og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i? | | | | | | |
| 4.2 | Delvis | | | | | | | | | |
| 4.3 | Fullstendig | | | | | | | | | |
| 4.4 | Fullstendig | | | | | | | | | |

| Nr | Krav (formulert som spørsmål) | Kap. i Normen | Kap. i ISO 27001 og Annex A | Systemkrav i behandlings-rettet helse-register | Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes) | Er kravet ivaretatt? | Hjemmel til kravet i lov eller forskrift | Kravet blir ivaretatt av data-behandler |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | PJF § 13 | |
| 123. | Sørger virksomheten for, innenfor rammen av taushetsplikten, at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte? | 5.2 | A.9.2* | | | ☐Ja ☐Nei | PJL §§ 15,19<br>HPL §§ 21, 25<br>PVF artikkel 32 nr. 1 bokstav b | ☐Ja ☐Nei |
| 124. | Sørger virksomheten for at opplysningene gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten og personvernet? | 5.2 | A.9.1.1* | | | ☐Ja ☐Nei | PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 125. | Er tilgangsstyring etablert for alle informasjonssystemer? | 5.2 | A.9.1 | Autorisering | | ☐Ja ☐Nei | PJL § 22<br>PJF § 13<br>HFL § 7, 1. ledd<br>HPL §25, 2.ledd<br>PVF artikkel 32 nr. 1 bokstav b | ☐Ja ☐Nei |
| 126. | Er tilgangsstyring etablert for administrator- og systembrukere? | 5.2 | A.9.2.3 | Autorisering | | ☐Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 127. | Sikres det at bare autorisert personell med tjenstlige behov får tilgang til helse- og personopplysninger? | 5.2 | A.9.1* | | | ☐Ja ☐Nei | PVF artikkel 32<br>PJL § 22<br>HRL § 21 | ☐Ja ☐Nei |
| 128. | Gis tilgang til behandlingsrettede helseregistre etter en | | | | | | | |

# Forbedringspotensiale?

- Skrive om fra spørsmål til krav
- Gå gjennom «Systemkrav» på nytt
- Forbedre sorteringsfunksjonen
- Kunne sortere på flere områder; f.eks. MU, video, innebygget personvern
- Kommentarfelt
- Interaktivt verktøy

- Handlingsplan 2021

# Fremtidige webinarer fra Normen

- 18. november: Normen 6.0 for leverandører.
- 24. november: Normkonferansen 2020. Sted: Digitalt.
- 4. desember: Nytt mandat og forvaltningsmodell for Normen

- Andre tema som kommer:
  - «PVO-rolle; Lessons learned»
  - Veileder for små virksomheter
  - Digitalt med.tek kurs

  - Innspill til tema for webinar, kontakt oss på sikkerhetsnormen@ehelse.no

NORMEN

**Se mer på normen.no**

# Normkonferansen 2020

## 24.november

- **Digital** Normkonferanse
- Vi bruker GoTo Webinar
- 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
- Vi gir beskjed når det går an å melde seg på igjen!

# Takk for i dag

Hold deg oppdatert på Normen på normen.no, Normen på Facebook og LinkedIN, og meld deg på vårt nyhetsbrev!

NORMEN