

NORMEN

Normen i anskaffelser



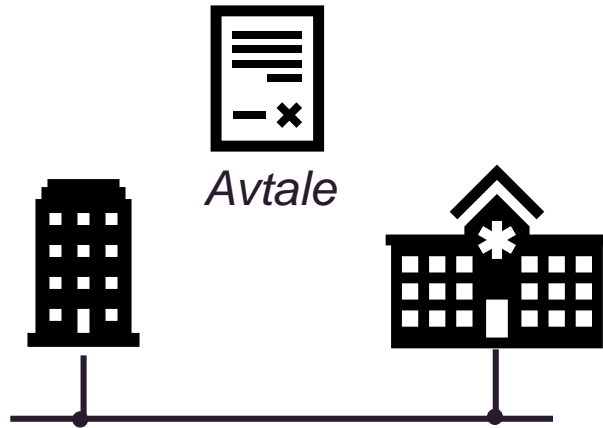
Sakset fra utallige kravspesifikasjoner...

**«Leverandøren skal
følge kravene i Normen»**

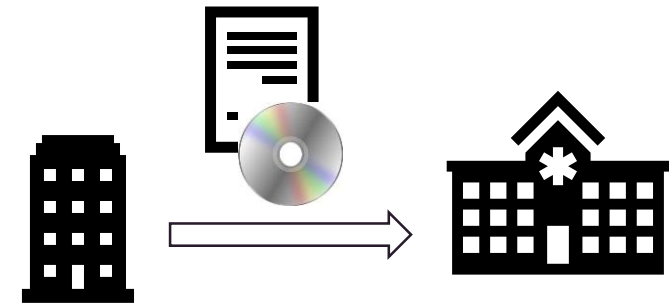
Hva betyr egentlig det?

Hvordan treffes leverandører av Normens krav?

- det avhenger av hva som leveres!

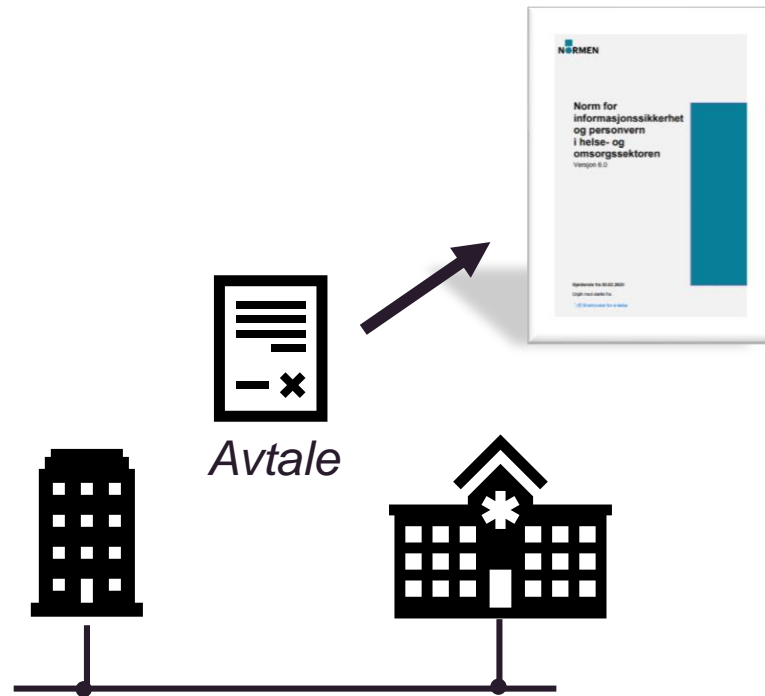


*Databehandler, tjenestetilbyder,
support osv*



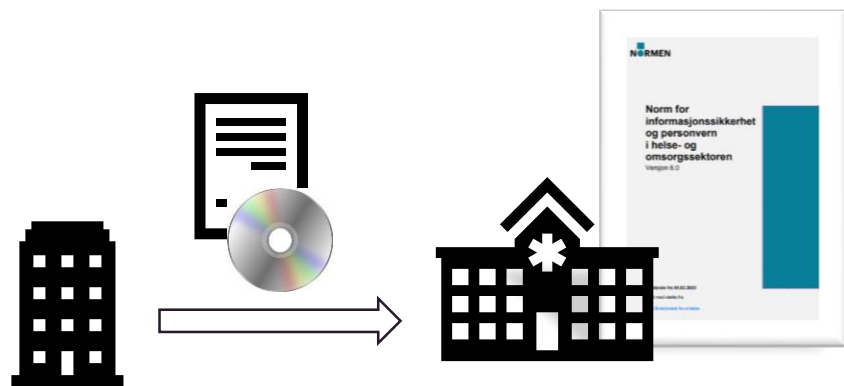
Programvareleverandør

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

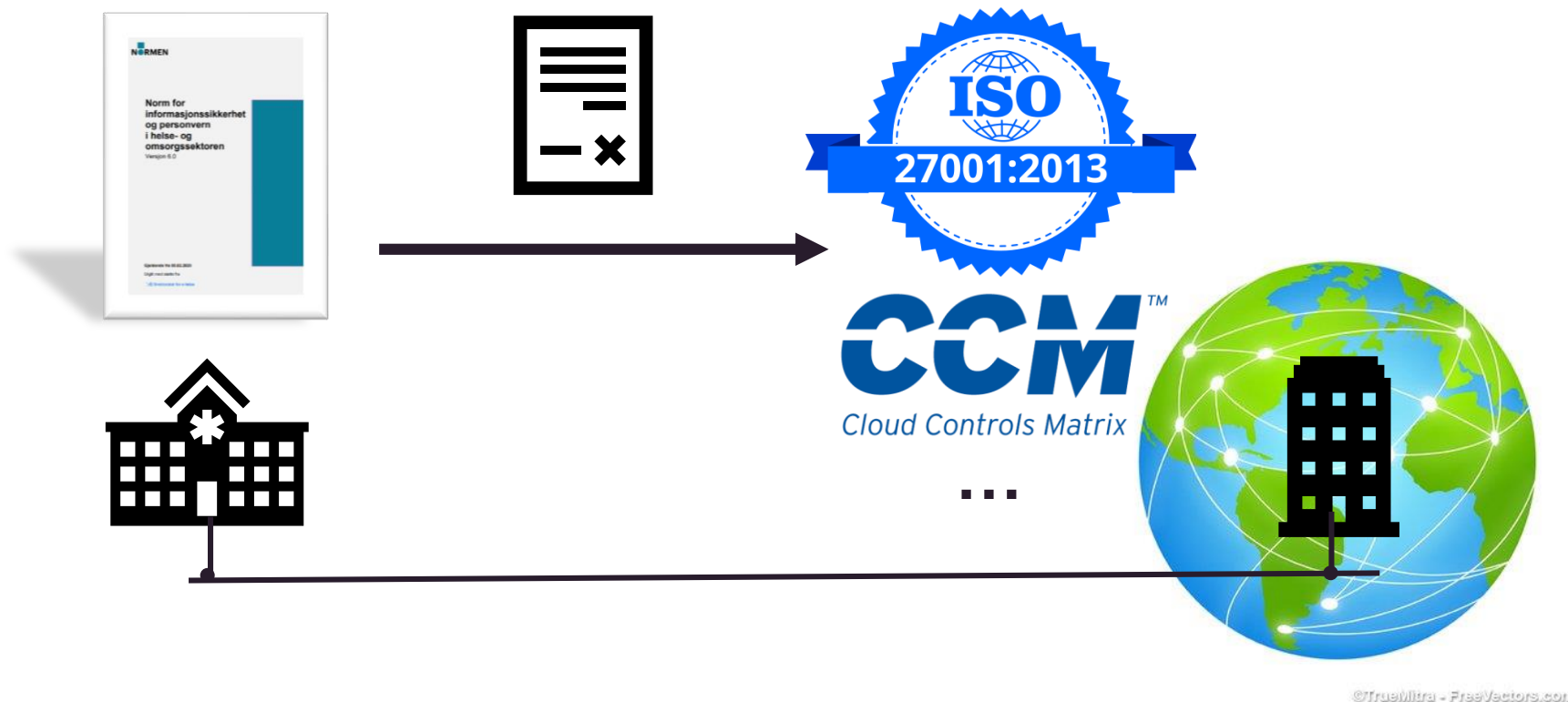


- For at virksomhetene skal kunne ivareta sitt ansvar som dataansvarlig, skal informasjonssystemene ha funksjonalitet som oppfyller lovbestemte krav og relevante krav i Normen
- Medfører at det må stilles **krav til funksjonalitet** i leverandørens programvare
- **Innbygd personvern**
- Hvis leverandøren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

**«Så Google og
Amazon skal
følge Normen
de nå?!»**



Ansvar for å *oversette* kravene ligger hos den dataansvarlige



©TrueMitra - FreeVectors.com

**«Hvordan skal
vi få til det?!»**



Den jobben har Normen allerede gjort for dere!

Normen

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



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	Systemkrav i behandlingsrettet helseregister	Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes)	Er kravet ivare tatt?	Hjemmel til kravet i lov eller forskrift	Kravet blir ivare tatt av data-behandler
			Direkte					
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*)			<input type="checkbox"/> Ja <input type="checkbox"/> Nei	PJL § 22 HRL § 21 PJF § 13, 2. ledd	<input type="checkbox"/> Ja <input type="checkbox"/> 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*			<input type="checkbox"/> Ja <input type="checkbox"/> Nei	PJL § 22 HRL § 21	<input type="checkbox"/> Ja <input type="checkbox"/> 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		<input type="checkbox"/> Ja <input type="checkbox"/> Nei	PJL § 22 HRL § 21 PJF § 13, 2. ledd	<input type="checkbox"/> Ja <input type="checkbox"/> Nei
148.	Identifiseres den enkelte rolle om roller benyttes?	5.2.2	A.9.1.1*	Autentisering		<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
149.	Gis det ved behov ny autentisering ved bytte av rolle (om roller benyttes)?	5.2.2	A.9.4.2*	Autentisering		<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> 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		<input type="checkbox"/> Ja <input type="checkbox"/> Nei	PVF artikkel 32 PJL § 22 HRL § 21 PJF § 13, 1. ledd bokstav e) og 3. ledd PVF art. 5 nr. 1 bokstav f	<input type="checkbox"/> Ja <input type="checkbox"/> Nei



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

Et triks:

Kap. i Normen	Kap. i ISO 27001 og Annex A	Systemkrav i behandlings-rettet helse-register	Kravet helt eller delvis tilfreds (Må...)
1.5	6.1.1 8.1		
1.5	6.1.3 8.3		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
1.5	6.1*		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Sorter

Sorter etter

Systemkrav i behandlings-rettet

Type: Tekst

Med: Avsnitt

Stigende

Synkende

Deretter etter

Type: Tekst

Med: Avsnitt

Stigende

Synkende

Deretter etter

Type: Tekst

Med: Avsnitt

Stigende

Synkende

Listen har

Overskriftsrad

Ingen overskriftsrad

Alternativer...

OK

Avbryt

= alle systemkrav samlet

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

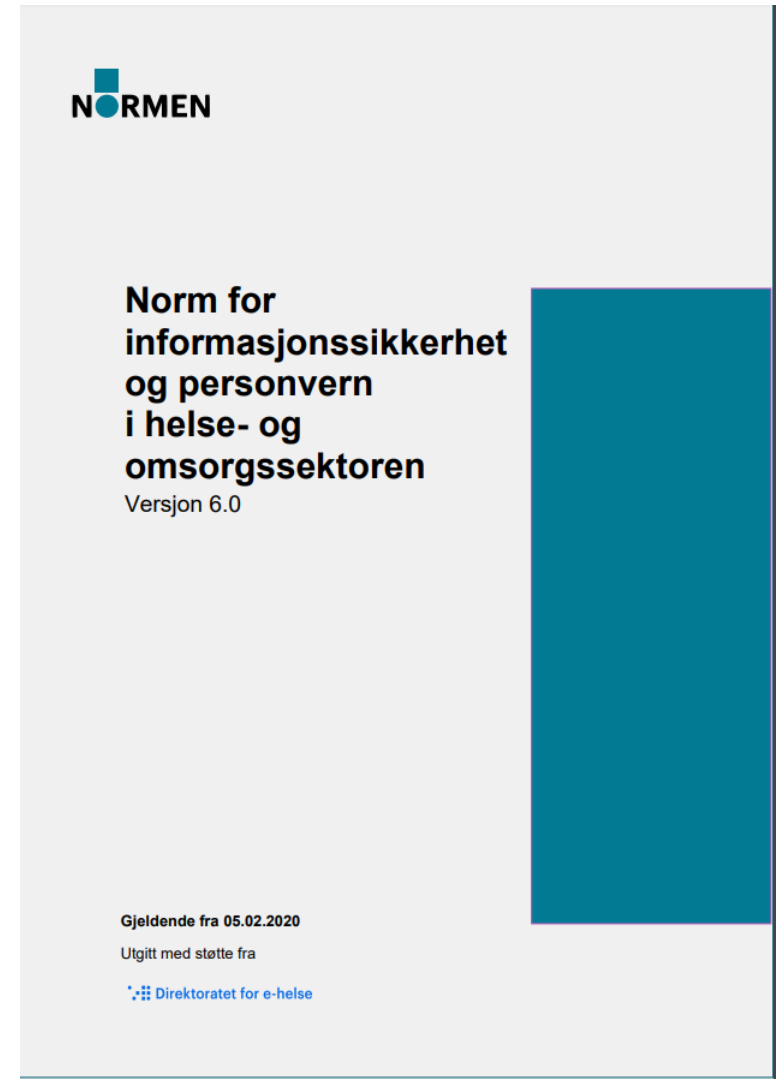
5.7.5 Vedlikehold, fjernaksess eller fysisk service

5.7.6 Systemleverandører

5.7.7 Leverandøroppfølging

5.7.8 Overføring av opplysninger til utlandet

5.7.9 Skytjenester



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 ivaretagelse av informasjonssikkerhet og personvern
 - Signert erklæring fra leverandør om tilbakelevering / sletting av data innen avtalt tid



5.7.7 Leverandøroppfølging

- **Informasjonssikkerhet og personvern knyttet til anskaffelser og leverandøroppfølging** skal inngå i virksomhetens **styringssystem for informasjonssikkerhet**.
- **Alle faser** i leverandørstyring, fra anskaffelse til avtalen er avsluttet, **skal omfattes**.
- Virksomheten skal sikre:
 - Klarhet i **ansvar og roller**
 - Kompetanseressurser innen informasjonssikkerhet og personvern **deltar**
 - Involvering av **ledelse (og styret)**
 - Dekkende **risikovurdering**
 - Som skal omfatte **leverandørens tilgang** til helse- og personopplysninger og annen taushetsbelagt informasjon
 - **Bestillerkompetanse og relevante sikkerhetskrav**



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 leveransmodellen** 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 ivaretagelse av informasjonssikkerhet og personvern **ved avslutning** av skytjenesten

