Normens krav og anbefalinger fra kravspek til innføringsprosjekt

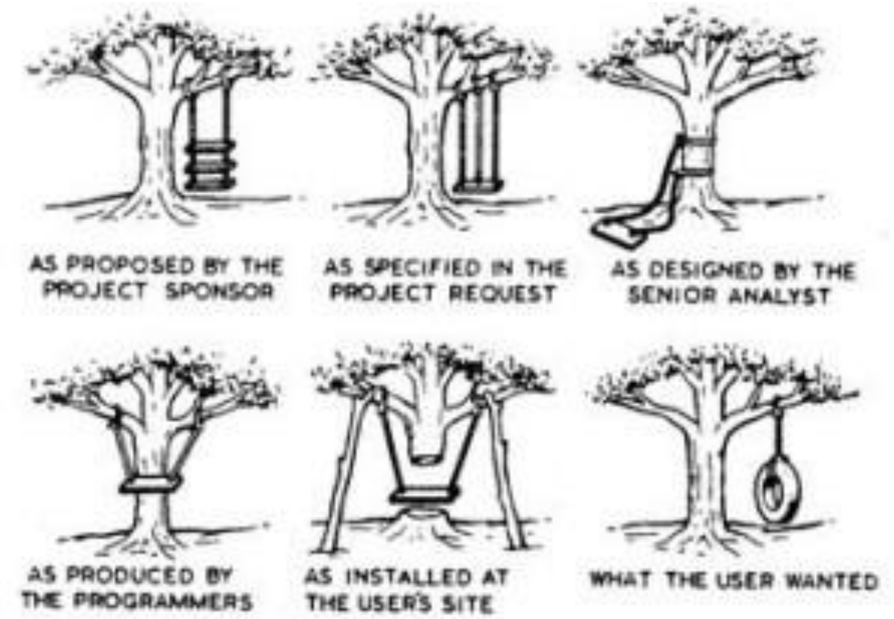
13.02.2020

Innhold

- Normens krav
- Krav til medisinsk utstyr
- Nærmere om Normens krav til leverandøroppfølging og avtaler
  - Databehandleravtale

Om krav i Normen

- Er minimumskrav
  - Fritar selvsagt ikke for risikovurdering
  - Bruk av andre «beste praksis» kan være nødvendig
- Normen er teknologinøytral
- «Tekniske krav»
  - Noen uendret fra 2006
  - Mange krav er oppdatert i versjon 6.0
- Normens krav dekker alle
  - Fra fotpleieren på hjørnet til nasjonale løsninger
  - Hvordan skalerer kravene?



Sakset fra utallige kravspesifikasjoner…

«Leverandøren skal følge kravene i Normen»

Hva betyr egentlig det?

Hvordan treffes leverandører av Normens krav?

Databehandler, tjenestetilbyder, support osv

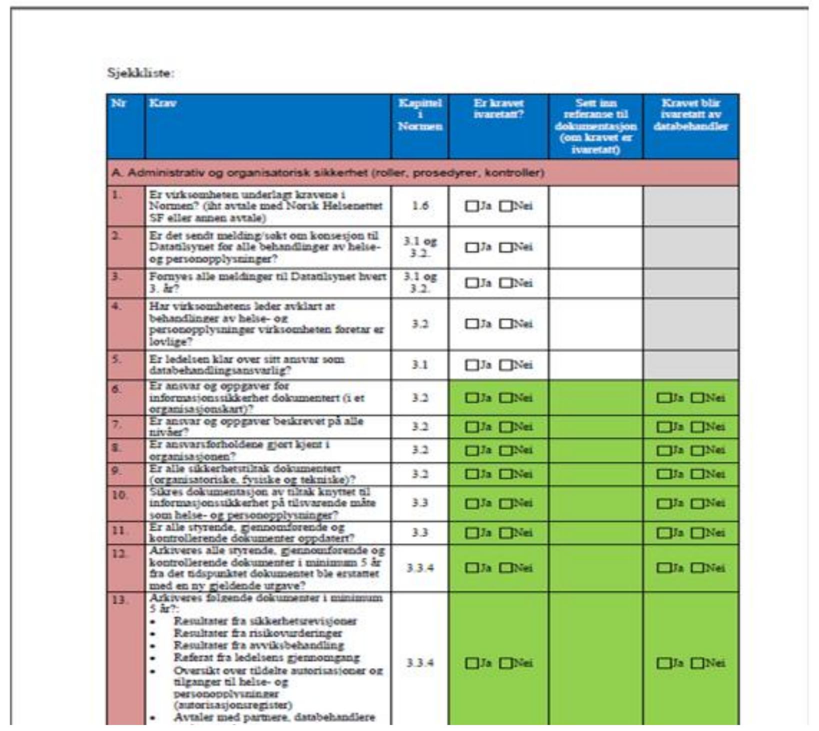
Programvare – eller hardwareleverandør

Oversikt over Normens krav

Normen 5.3:

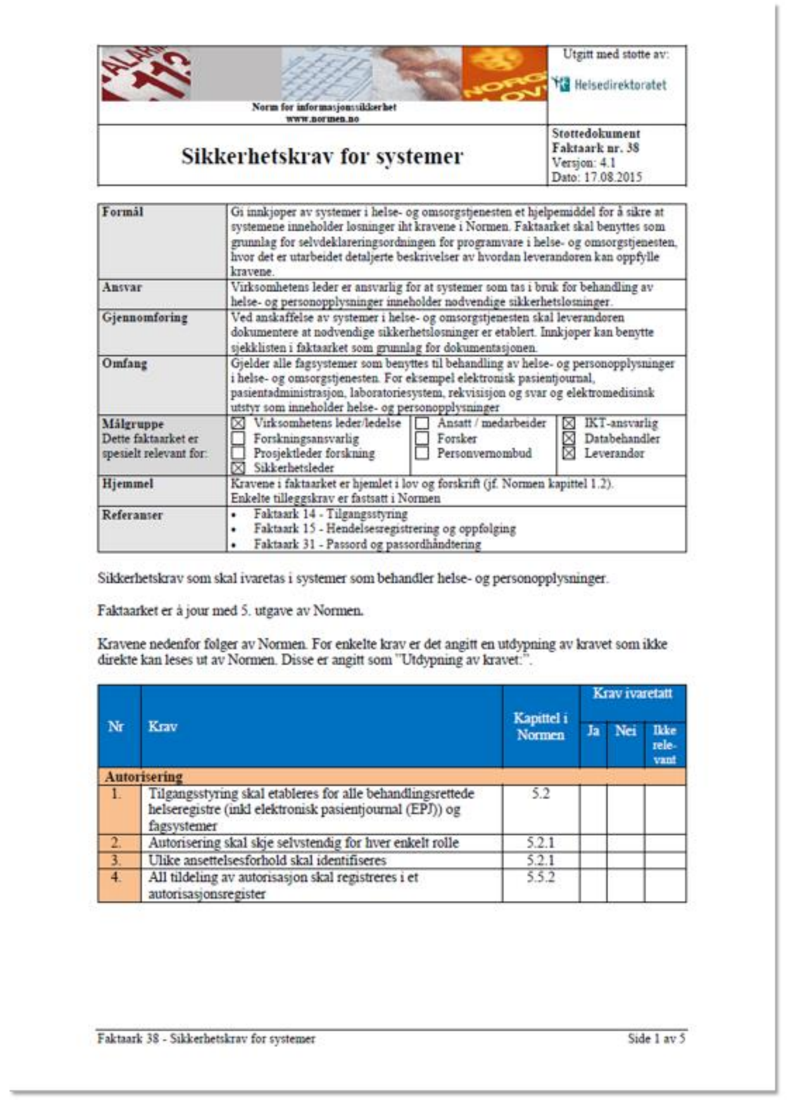
[Faktaark 6b](#) - Sjekkliste for å ivareta kravene i Normen

- 208 krav med referanse til Normen
- Tematisk inndeling
  - Administrativ og organisatorisk sikkerhet
  - EPJ / fagsystem
  - Fysisk sikring
  - Teknisk løsning
- Angivelse av om kravet kan oppfylles av databehandlingsansvarlig, databehandler, eller begge.



Krav til programvare

- [Faktaark 38 - Sikkerhetskrav for systemer](#) **(med referanse til Normen)**
- Tilhørende [selvdeklareringsdokumenter](#)



Normen 6.0:

Samlet oversikt Normens krav

Nr.	Krav	KIT	Kap. i Normen	Kap. i ISO 27001 Direkte	Kap. i ISO 27001 Indirekte (krav i lov)	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
	A. LEDELSE OG ANSVAR									
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?	KIT	1.5	6.1.1 8.1	A.18.1			☐Ja ☐Nei	PVF artikkel 32 PJL § 22 HRL § 21	
2.	Er valgte tiltak basert på risikovurderinger?	KIT	1.5	6.1.3 8.3	A.18.1			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	☐Ja ☐Ne
3.	Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger?	KIT	1.5	6.1* 8.1.*	A.18.1			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	
4.	Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges?	KIT	2	5.1 5.2 5.3	A.18.1			☐Ja ☐Nei	PJL § 22 HRL § 21 HTL § 5-10 første punktum PVF artikkel 24	
5.	Har virksomhetens øverste leder for virksomheten bestemt nivå for akseptabel risiko?	KIT	2 3.2	6.1.2	A.18.1			☐Ja ☐Nei	PJL § 22 HRL § 21 PVF artikkel 32	☐Ja ☐Ne
6.	Har virksomhetens øverste leder for virksomheten bestemt regler for håndtering av risiko?	KIT	2	6.1.3	A.18.1			☐Ja ☐Nei	PJL § 23 HRL § 22	☐Ja ☐Ne
7.	Har virksomhetens øverste leder for virksomheten sørget for velfungerende styring og kontroll?	KIT	2	6.2	A.18.1			☐Ja ☐Nei	PVF artikkel 24 første ledd	☐Ja ☐Ne

Vedlegg - Samlet oversikt Normens krav 17012020.docx — Side 4 av 46

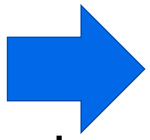
Vedlegg til Normen 6.0: Samlet oversikt over Normens krav

Samlet oversikt Normens krav

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
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 8.1			☐ Ja ☐ Nei	PVF artikkel 32 PJL § 22 HRL § 21 FLK § 6	
2.	Er valgte tiltak basert på risikovurderinger?	1.5	6.1.3 8.3			☐ Ja ☐ Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	☐ Ja ☐ Nei
3.	Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger?	1.5	6.1* 8.1.*			☐ Ja ☐ Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	
	...							
282.	Øves, testes, revideres og oppdateres nødrutinene minst en gang i året?	5.9	A.17.1*			☐ Ja ☐ Nei	PVF artikkel 24 og 32 PJL § 22 HRL § 21 FLK § 8	☐ Ja ☐ Nei

Krav til medisinsk utstyr

- OUS (del av felles styringssystem HSØ):
  - Kravspesifikasjon ved anskaffelser av MTU-løsninger med IKT-grensesnitt og tilkobling til nettverk
  - https://ehandboken.ous-hf.no/document/112278/fields/23
- Informasjonssikkerhetskrav til bruk ved anskaffelser av MU i Helse Vest



- Overordnet systembeskrivelse
  - Overvåkning og endrings- / oppdateringsregime
  - Redundanskrav
- Lisenshåndtering
- Nettverk
- Maskinvare
- OS og programvare
- Informasjonssikkerhet og IDM
- Backup
- Integrasjoner
- IKT-relatert drift og forvaltning

5.7 Leverandørforhold og avtaler

- Leverandøren skal tilrettelegge for at dataansvarlig som tar i bruk leverandørens produkter og tjenester, kan oppfylle lovbestemte krav og krav i Normen.

- Taushetsplikt
  - Leverandøren skal forsikre at de har rutiner som pålegger alle medarbeidere taushetsplikt om helse- og personopplysninger og annen taushetsbelagt informasjon.
  - Leverandøren kan selv administrere og oppbevare taushetserklæringer for eget personell, men den dataansvarlige skal sikres innsyn ved behov.

- Den dataansvarlige har ansvaret for at krav til informasjonssikkerhet og personvern følges gjennom **hele leveransekjeden**.

- I leveranser av f.eks. tjenester, maskinvare eller systemer skal det avtales **skriftlig** med leverandører hvilke sikkerhetskrav som skal oppfylles for at den dataansvarlige skal kunne oppfylle sitt ansvar.
  - Hvilke av Normens krav - avhengig av hva slags leveranse

Tjenesteutsetting

- Dokumentert risikovurdering
  - Ved tjenesteutsetting av IKT-tjenester til andre land bør forhold ved vertslandet vurderes fordi de kan påvirke risikovurderingen.
- Beskrive hvilke oppgaver av sikkerhetsmessig betydning som er omfattet, og ansvarsforholdene for disse
- Beskrivelse av leverandørens løsning og grensesnitt mot virksomheten i form av konfigurasjonskart
- Rett til revisjon (3. partsrevisjon er en mulighet)
- Exit-strategi- signert erklæring sletting / tilbakelevering

Viktige begreper

Behandlingsansvarlig

Den som alene eller sammen med andre **bestemmer formålet** med behandlingen av personopplysninger og hvilke midler som skal benyttes

Kan **utpekes** i lov eller forskrift

Er **ansvarlig** for behandlingen av personopplysninger

Dataansvarlig

Begrepet som brukes **om behandlingsansvarlig i helse**

Eget begrep i lovgivningen i vår sektor for å unngå forveksling med ansvar for pasientbehandling

Oslo universitetssykehus

Databehandler

En som behandler personopplysninger **på vegne** av behandlingsansvarlig

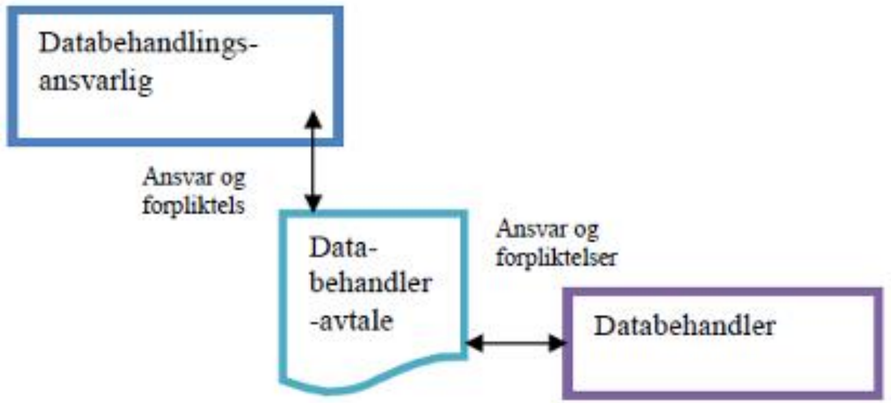
SYKEHUSPARTNER

Microsoft

NORMEN

Databehandler

- *Databehandler* skal ikke behandle *helse- og personopplysninger* på annen måte enn det som er avtalt med *databehandlingsansvarlig.*
- *Databehandleren* skal ikke engasjere underleverandører uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den *dataansvarlige*.
- *Databehandler* har et selvstendig ansvar for informasjonssikkerhet
- *Databehandlingsansvarlig* skal sikres innsynsrett
- Skiller mellom data tilhørende ulike kunder
- Tilgangsstyring – hvem kan ha tilgang
- Når trengs det (ikke) databehandleravtale?



- Se mer i faktaark 10

+


Datatilsynet

Veileder

Behandlingsansvarlig og databehandler

Personvernforordningen skiller mellom begrepene *behandlingsansvarlig* og *databehandler*. Den behandlingsansvarlige bestemmer over personopplysningene, mens databehandleren opptrer på vegne av den behandlingsansvarlige. Databehandleren kan derfor bare behandle personopplysninger etter instruks fra den behandlingsansvarlige.

Quiz: Når trengs databehandleravtale?

- Leverandør drifter EPJ-system for legekontor

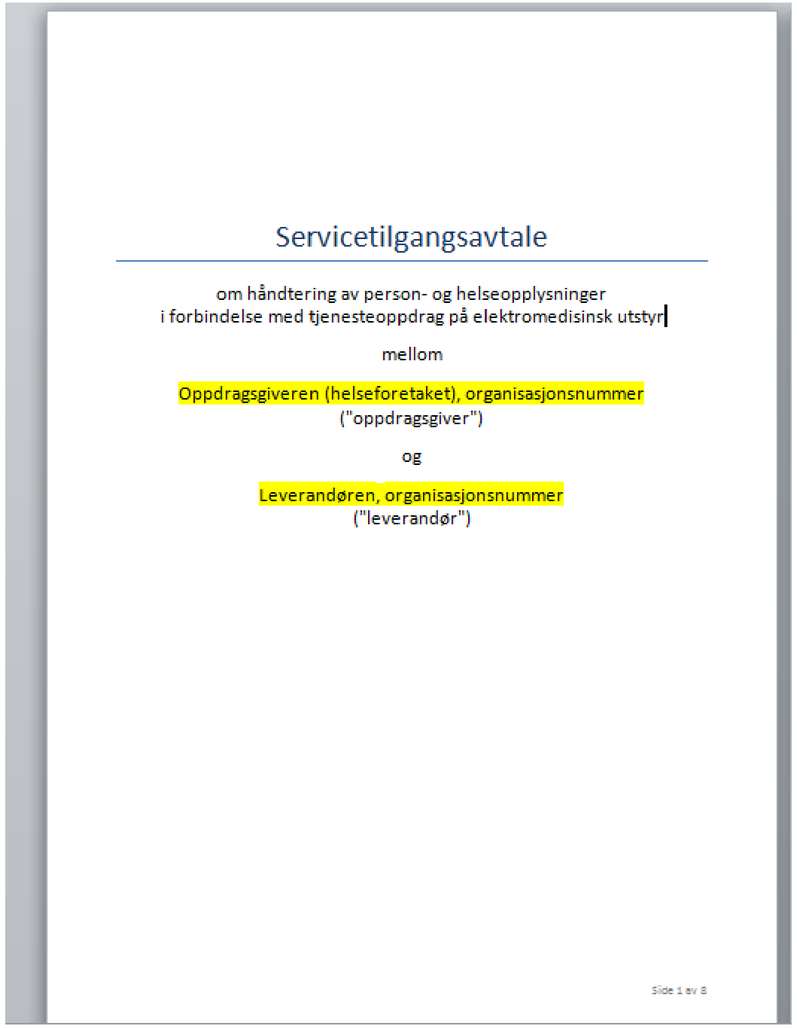
- Programvareleverandør får kundens data for å gjennomføre prøvekonvertering

- Leverandøren skal skifte en server hos kunden

- Leverandør oppgraderer programvare hos kunden

Servicetilgangsavtale – eksempel fra Helse Midt-Norge

- Denne avtalen gjelder for tjenesteoppdrag som omfatter installasjon, konfigurasjon, vedlikehold og andre tekniske tjenester som utføres av leverandøren på elektromedisinsk utstyr som eies, leies eller på annen måte disponeres av oppdragsgiveren



Servicetilgangsavtale

om håndtering av person- og helseopplysninger
i forbindelse med tjenesteoppdrag på elektromedisinsk utstyr

mellom

Oppdragsgiveren (helseforetaket), organisasjonsnummer
("oppdragsgiver")

og

Leverandøren, organisasjonsnummer
("leverandør")

Side 1 av 8

Systemleverandører

- Virksomheter i helse- og omsorgssektoren som tar i bruk informasjonssystemer som behandler helse- og personopplysninger, skal stille krav om innebygd personvern i løsningene.
- Informasjonssystemene ha funksjonalitet som oppfyller lovbestemte krav og relevante krav i Normen

Samlet oversikt over Normens krav

Nr	Krav	Kap. i Normen	Kap. i ISO 27001 – Direkte	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
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

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**

Overføring av opplysninger til utlandet

- Virksomheter som overfører personopplysninger til utlandet, skal passe på at beskyttelsesnivået i personopplysningsloven ikke undergraves ved overføringen.

- EU/EØS
- Godkjente tredjeland

Personopplysninger kan fritt overføres til disse statene. ***Dette forutsetter at personopplysningslovens øvrige vilkår er oppfylt*** -> Risikovurdering, landrisikovurdering

- Når virksomheten overfører personopplysninger til stater utenfor EU/EØS-området, såkalte «tredjeland», skal den bruke et av overføringsgrunnlagene i forordningen

- Ha tilstrekkelig kompetanse tilgjenglig

- Se ellers Datatilsynets veileder

NORMEN

Krav til

Test

- Faktaark 43 - Bruk av testdata i systemer som inneholder helse- og personopplysninger
- Faktaark 48 - Informasjonssikkerhet ved utførelse av testing