Norm for informasjonssikkerhet i helse og omsorgstjenesten

@Normen_no

Sammen om velferdsteknologi på Agder

10. mars 2017

@johnhorve

Ikke lenge til
21. mars

Norm

for informasjonssikkerhet

Helse- og omsorgstjenesten

Utgitt med støtte av:

Direktoratet for e-helse

Oslo, 2016

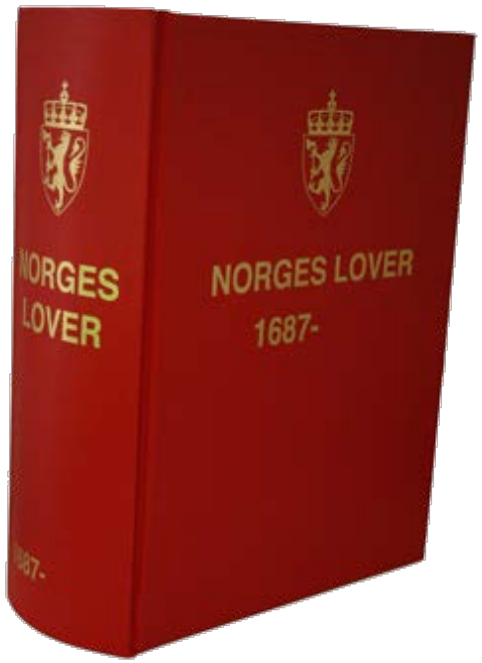
JO NESBØ

TØRST

EN NY HARRY HOLE-THRILLER

HAR JEG NOE SÆRE INTERESSER?

PERSONOPPLYSNINGSFORSKRIFTEN



§ 2-15.*Sikkerhet hos andre virksomheter*

Den behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her.

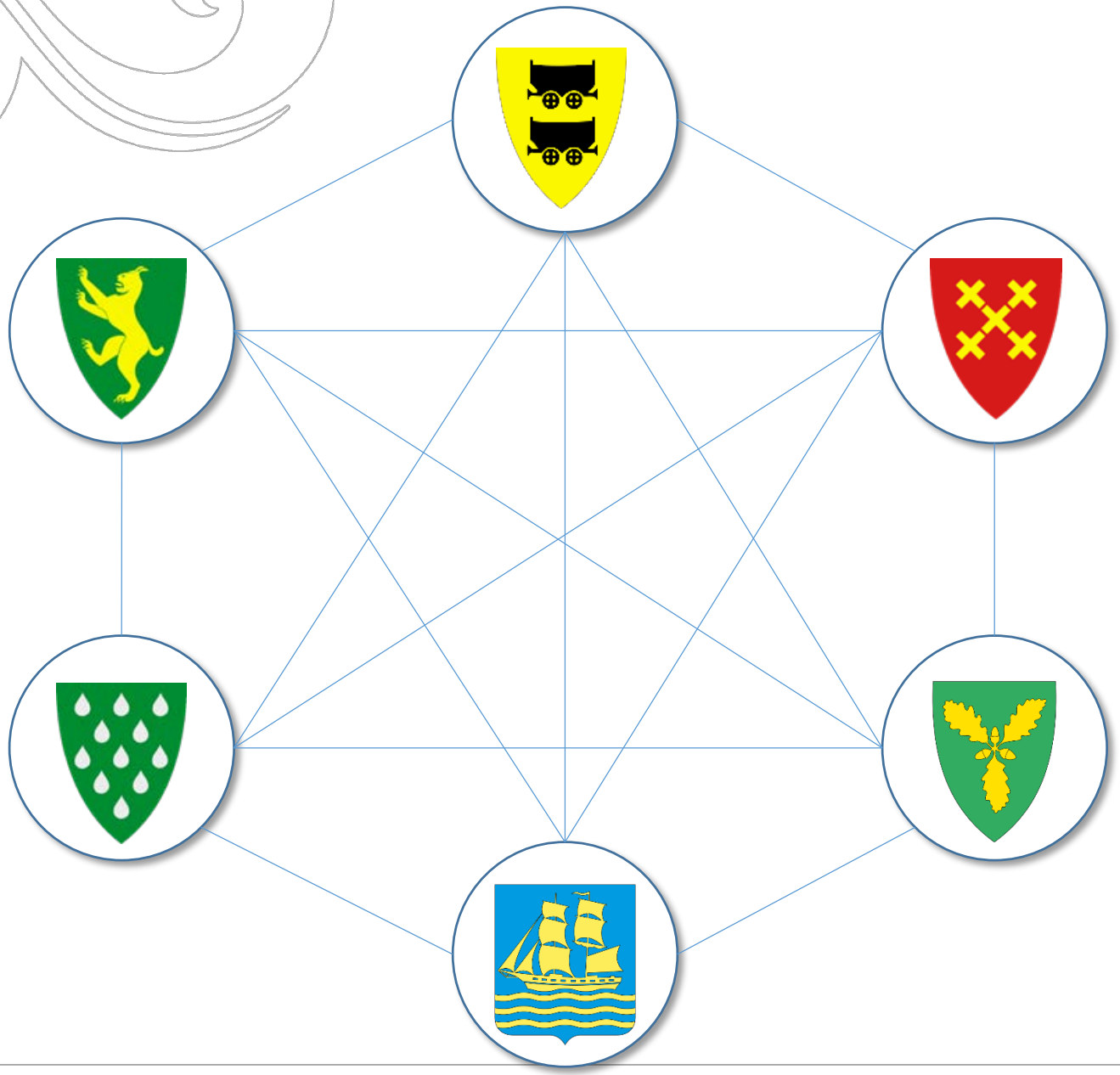
Den behandlingsansvarlige kan overføre personopplysninger til enhver dersom overføringen skjer i samsvar med reglene i personopplysningsloven §§ 29 og 30, eller når det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register.

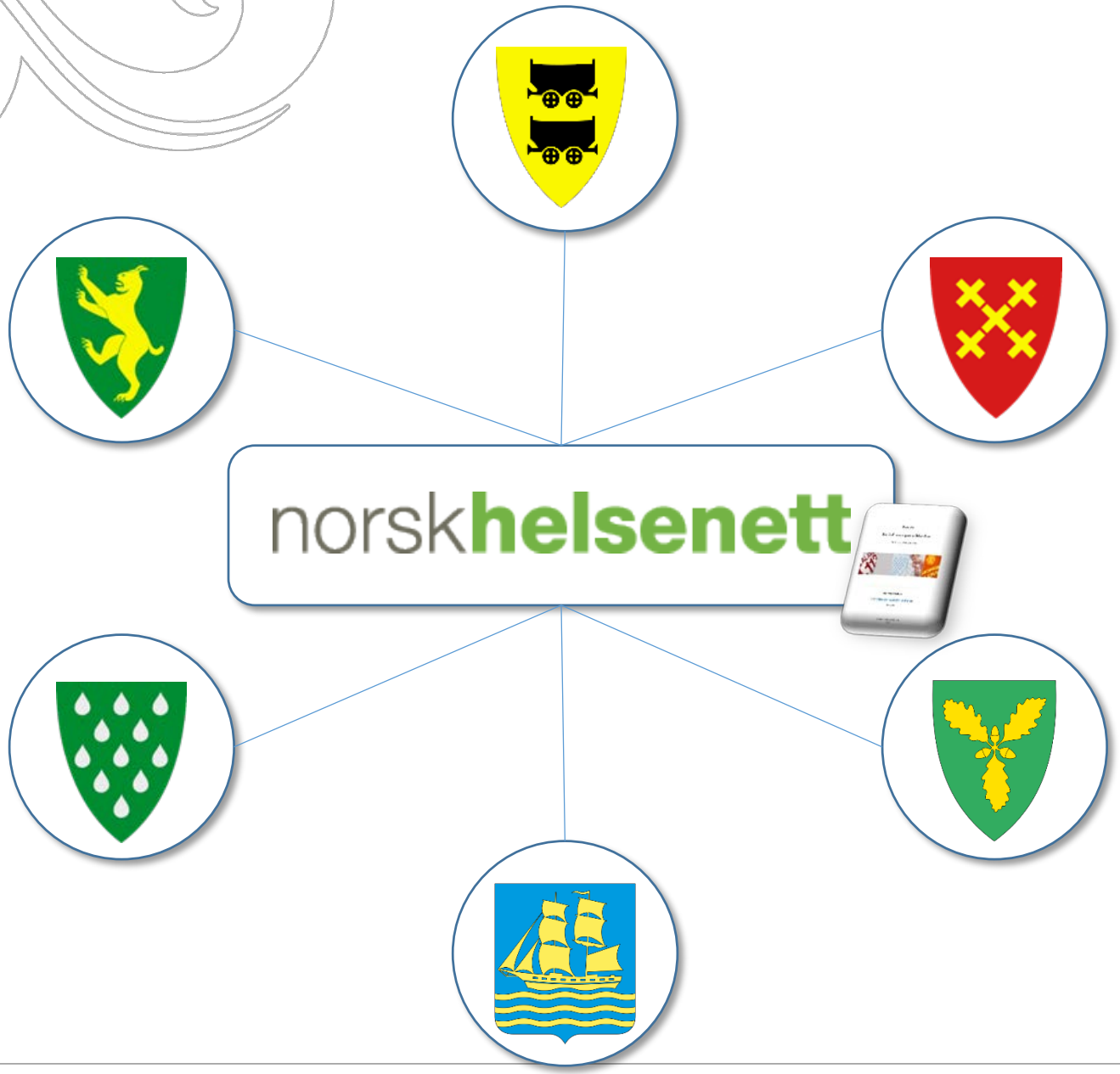
Leverandører som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i dette kapittelet.

Den behandlingsansvarlige skal etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører. Ansvars- og myndighetsforhold skal beskrives i særskilt avtale.

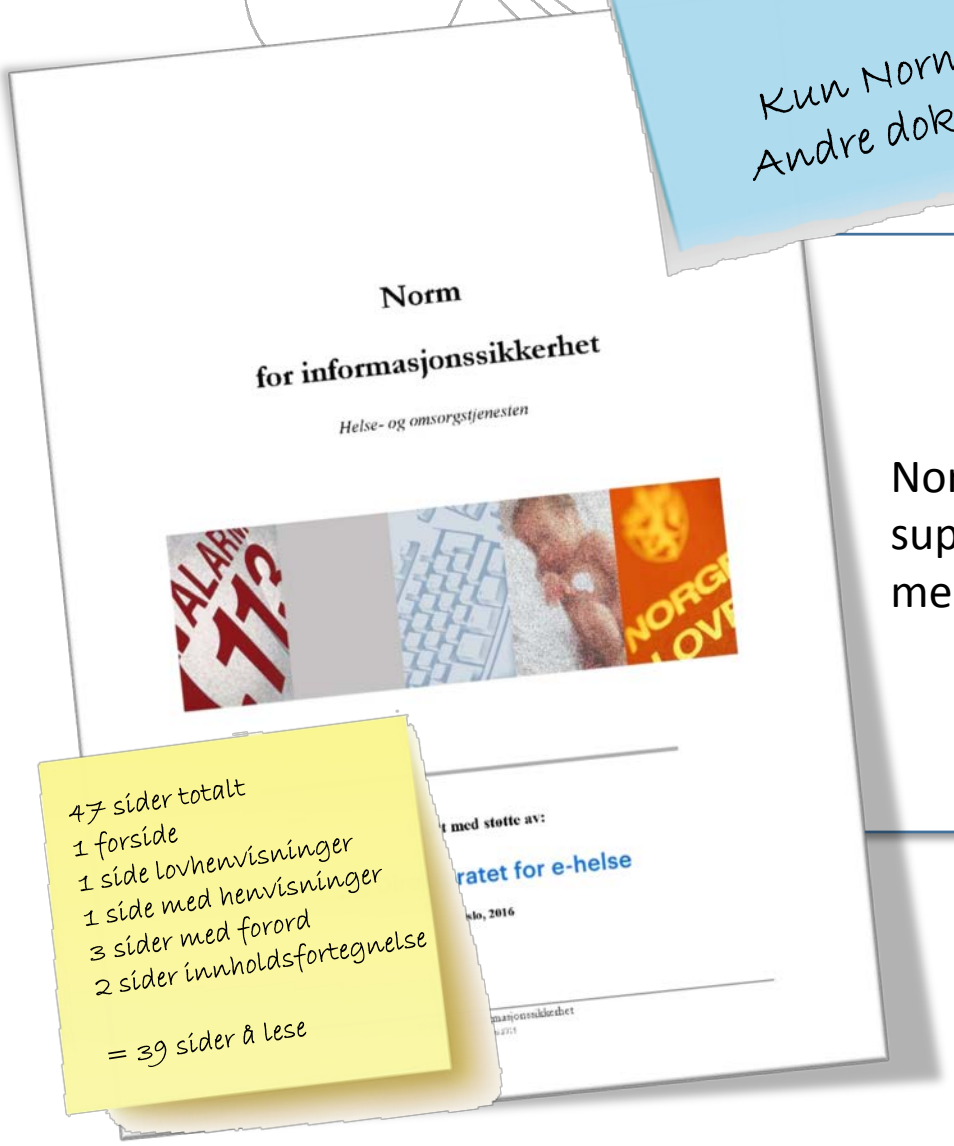
Den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.

LMT SETESDAL




norskhelsenett

Kun Normen er bindende !!!
Andre dokument er veiledende



Normen suppleres med

Faktaark

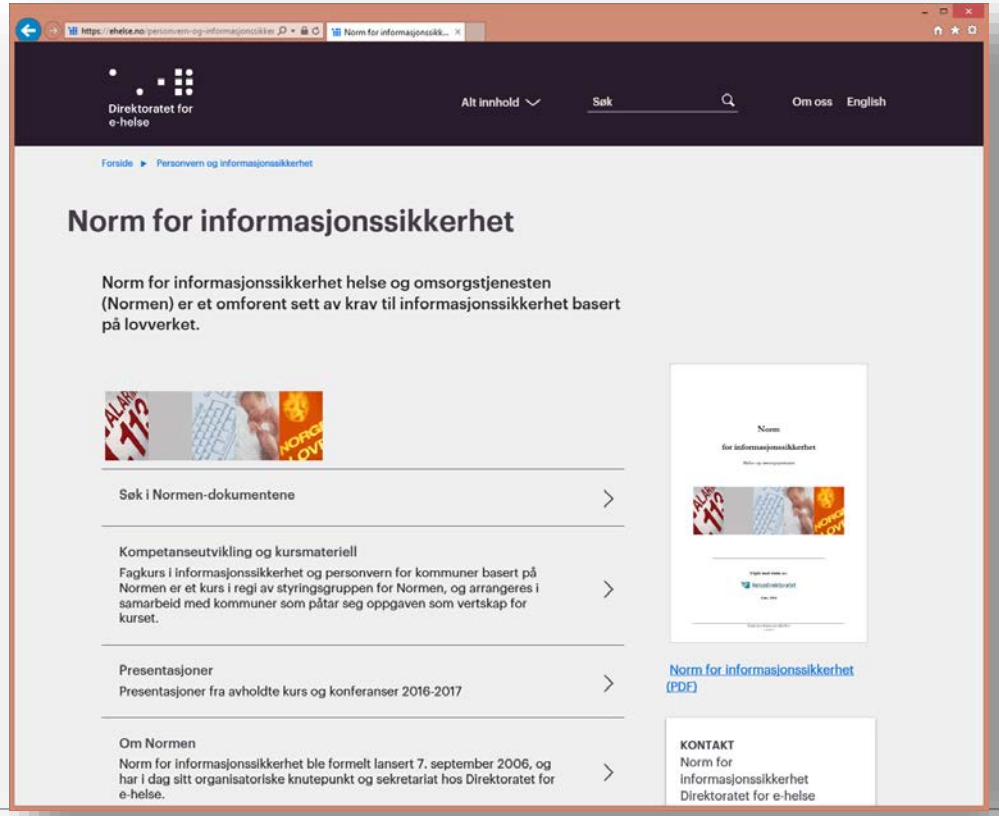
En **kort** forklaring på hvordan ting kan løses

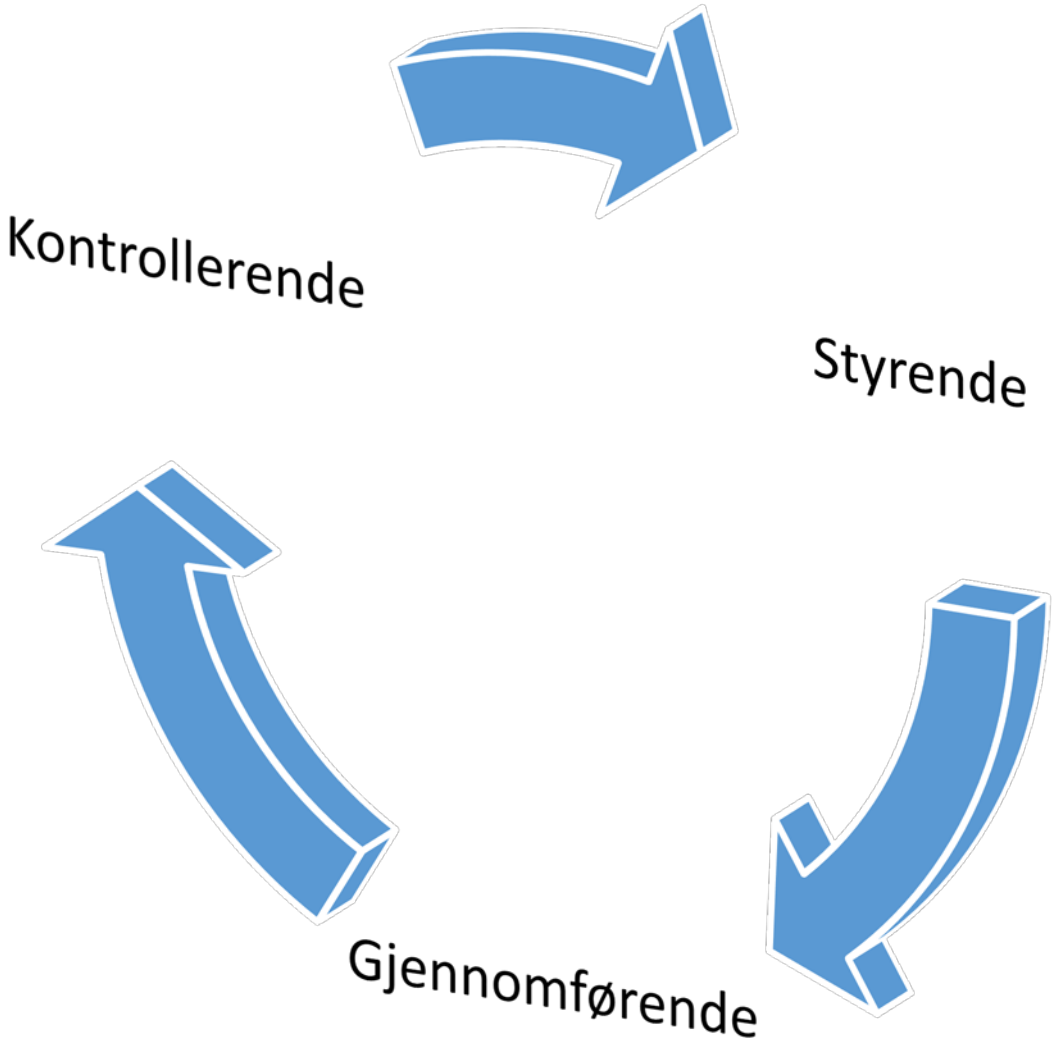
Veiledere

En **omfattende** forklaring på hvordan ting kan løses

Andre dokumenter

NORMEN ER ET STYRINGSSYSTEM





HVEM STÅR BAK NORMEN?

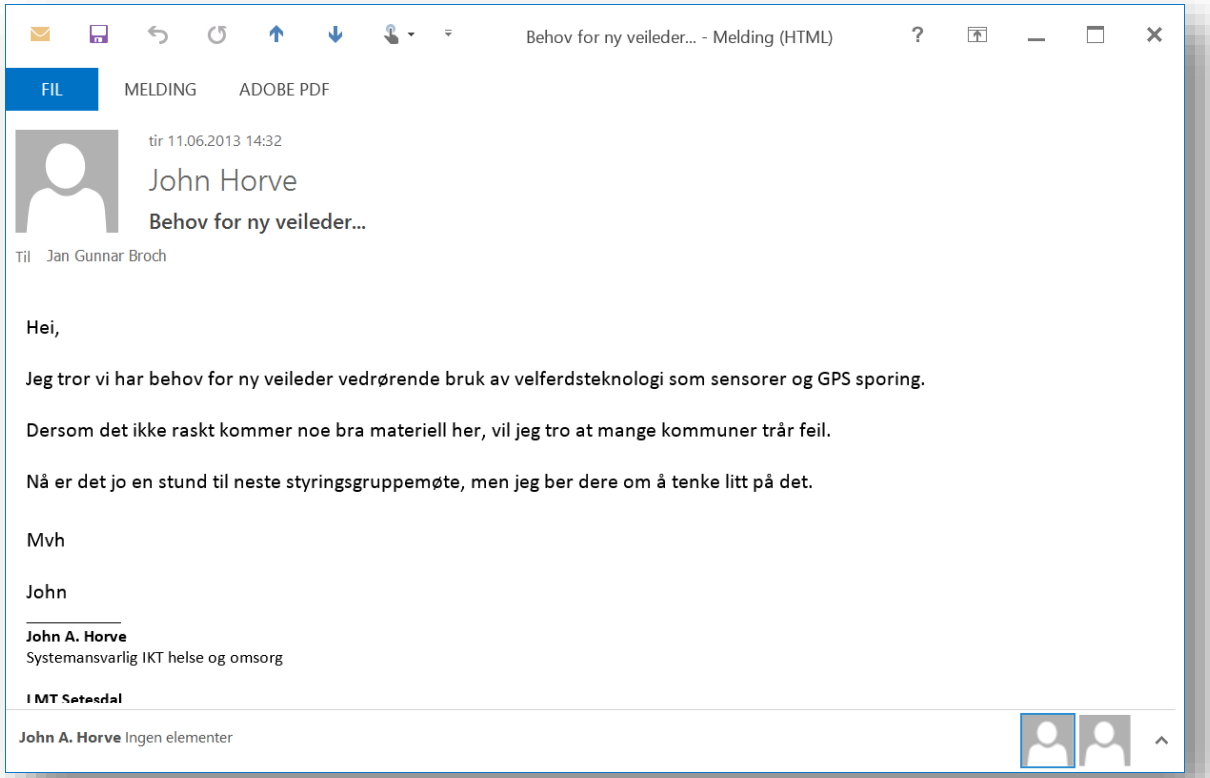
Tor Ottersen


Norrmen

STYRINGSGRUPPE

- KS (2)
- Den norske legeforening
- Den norske tannlegeforening
- Norsk sykepleieforbund
- Apotekforeningen
- Norsk farmaceutisk forening
- Regionale helseforetak
  - Helse Nord
  - Helse Midt-Norge
  - Helse Vest
  - Helse Sør-Øst
- Norsk helsenett
- Helsedirektoratet (2)
- Direktoratet for e-helse
- Folkehelseinstituttet
- AS Med-Lab
- NAV
- Den offentlige tannhelsetjeneste
- Norsk psykologforening
- Norsk fysioterapiforbund
- Observatører:
  - Datatilsynet
  - Helse- og omsorgsdepartementet
  - Difi

NORMEN OG VELFERDSTEKNOLOGI



VEILEDER I BRUK AV PORTALLØSNINGER, SMS OG EPOST

Eksempler på informasjon som **ikke kan** sendes som SMS

- Fødselsnummer (11 siffer)

- Helseopplysninger. Dette gjelder for eksempel diagnose i form av kode eller tekst som viser pasienten/brukerens helsetilstand.

- Reseptinformasjon. Dette gjelder for eksempel innhold i eller forordning av legemiddel

- Avdelingsnavn (som kan knyttes til diagnose eller helseforhold. Unngå for eksempel ”...psykiatrisk poliklinikk...”, ”...gynekologisk avdeling...”)

Eksempler på informasjon som **ikke bør** sendes som SMS

- Telefonnummer til avsender (slik at det ikke er mulig å identifisere avsender/avdeling med navn som kan angi helseforhold eller diagnose).

VEILEDER I BRUK AV PORTALLØSNINGER, SMS OG EPOST

Eksempler på informasjon som **ikke kan** sendes i ordinær e-post

- Fødselsnummer (11 siffer)

- Helseopplysninger. For eksempel diagnose i form av kode eller tekst som viser pasienten/brukerens helsetilstand

- Reseptinformasjon. For eksempel innhold i eller forordning av legemiddel

- Avdelingsnavn (som kan knyttes til diagnose eller helseforhold. Unngå for eksempel ”...psykiatrisk poliklinikk...”, ”...gynekologisk avdeling...”)

Eksempler på informasjon som **ikke bør** sendes i e-post

- Telefonnummer til avsender (slik at det ikke er mulig å identifisere avsender/avdeling med navn. som kan angi helseforhold eller diagnose)

VENNEFORESPØRSLER PÅ SOSIALE MEDIER


VG NYHETER

< Nyheter | Innenriks | Utenriks | Siste 48t | Meninger

Sykehus laget Snapchat-konto - lekket taushetsbelagt pasientinfo

Pågående oppdrag (4)

Oppdrag	Tid	Hentested	Problem
535610-1	A 08:45		sentrale brystsmerter, ti
535626-1	10:32		Våknet natt til tirsdag m

Takk for henvendelsen om å bli satt i forbindelse her på Facebook.

Dessverre må jeg avslå tilbudet ditt. Det kan noen ganger være vanskelig å gjøre gode, faglige vurderinger og gi behandling til noen en også har et personlig forhold til.

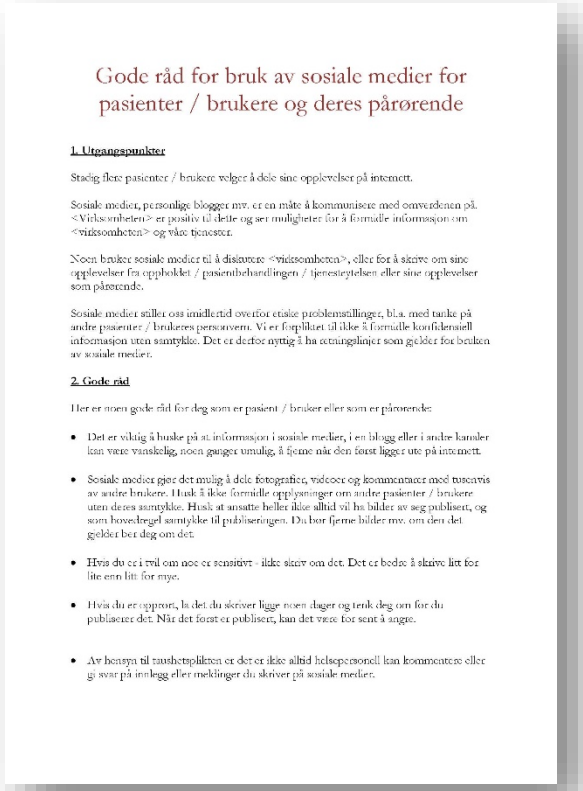
De ansatte i kommunen frarådes generelt å ha nåværende eller tidligere pasienter / brukere som forbindelser på Facebook.

Jeg håper du har forståelse for dette.

Med vennlig hilsen <NN>


DU ER PÅ JAKT ETTER FACEBOOK, SIER DU?
HELST POCKET-UTGAVEN . . .

GODE RÅD FOR PASIENTER OG DERES PÅRØRENDE



Gode råd for bruk av sosiale medier for pasienter / brukere og deres pårørende

1. Utgangspunkter

Stadig flere pasienter / brukere velger å dele sine opplevelser på internett.

Sosiale medier, personlige blogger mv. er en måte å kommunisere med omverdenen på. <Virksomheten> er positiv til dette og ser muligheter for å formidle informasjon om <virksomheten> og våre tjenester.

Noen bruker sosiale medier til å diskutere <virksomheten>, eller for å skrive om sine opplevelser fra oppholdet / pasientbehandlingen / tjenesteytelsen eller sine opplevelser som pårørende.

Sosiale medier stiller oss imidlertid overfor etiske problemstillinger, bl.a. med tanke på andre pasienter / brukeres personvern. Vi er forpliktet til ikke å formidle konfidensiell informasjon uten samtykke. Det er derfor nyttig å ha retningslinjer som gjelder for bruken av sosiale medier.

2. Gode råd

Her er noen gode råd for deg som er pasient / bruker eller som er pårørende:

- Det er viktig å huske på at informasjon i sosiale medier, i en blogg eller i andre kanaler kan være vanskelig, noen ganger umulig, å fjerne når den først ligger ute på internett.
- Sosiale medier gjør det mulig å dele fotografier, videoer og kommentarer med tusenvis av andre brukere. Husk å ikke formidle opplysninger om andre pasienter / brukere uten deres samtykke. Husk at ansatte heller ikke alltid vil ha bilder av seg publisert, og som hovedregel samtykke til publiseringen. Du bør fjerne bilder mv. om den det gjelder ber deg om det.
- Hvis du er i tvil om noe er sensitivt - ikke skriv om det. Det er bedre å skrive litt for lite enn litt for mye.
- Hvis du er opprørt, la det du skriver ligge noen dager og tenk deg om før du publiserer det. Når det først er publisert, kan det være for sent å angre.
- Av hensyn til taushetsplikten er det er ikke alltid helsepersonell kan kommentere eller gi svar på innlegg eller meldinger du skriver på sosiale medier.

Her er noen gode råd for deg som er pasient / bruker eller som er pårørende:

- Det er viktig å huske på at informasjon i sosiale medier, i en blogg eller i andre kanaler kan være vanskelig, noen ganger umulig, å fjerne når den først ligger ute på internett.
- Sosiale medier gjør det mulig å dele fotografier, videoer og kommentarer med tusenvis av andre brukere. Husk å ikke formidle opplysninger om andre pasienter / brukere uten deres samtykke. Husk at ansatte heller ikke alltid vil ha bilder av seg publisert, og som hovedregel samtykke til publiseringen. Du bør fjerne bilder mv. om den det gjelder ber deg om det.
- Hvis du er i tvil om noe er sensitivt - ikke skriv om det. Det er bedre å skrive litt for lite enn litt for mye.
- Hvis du er opprørt, la det du skriver ligge noen dager og tenk deg om før du publiserer det. Når det først er publisert, kan det være for sent å angre.
- Av hensyn til taushetsplikten er det er ikke alltid helsepersonell kan kommentere eller gi svar på innlegg eller meldinger du skriver på sosiale medier.

GO

kan

av andre
mtykke.
ykke til

enn litt for

det. Når

gi svar på

http://www.fvn.no/nyheter/lokalt/Anmelder-person-som-filme

Anmelder person som filmet...

Fædrelandsvennen Nyheter Sport Kultur God Helg John A. Meny

Rådmann Svein Skisland i Vennesla kommune mener ansatte på jobb ikke skal skal oppleve å bli hengt ut på Facebook.
FOTO: Arkivfoto Odd Inge Uleberg

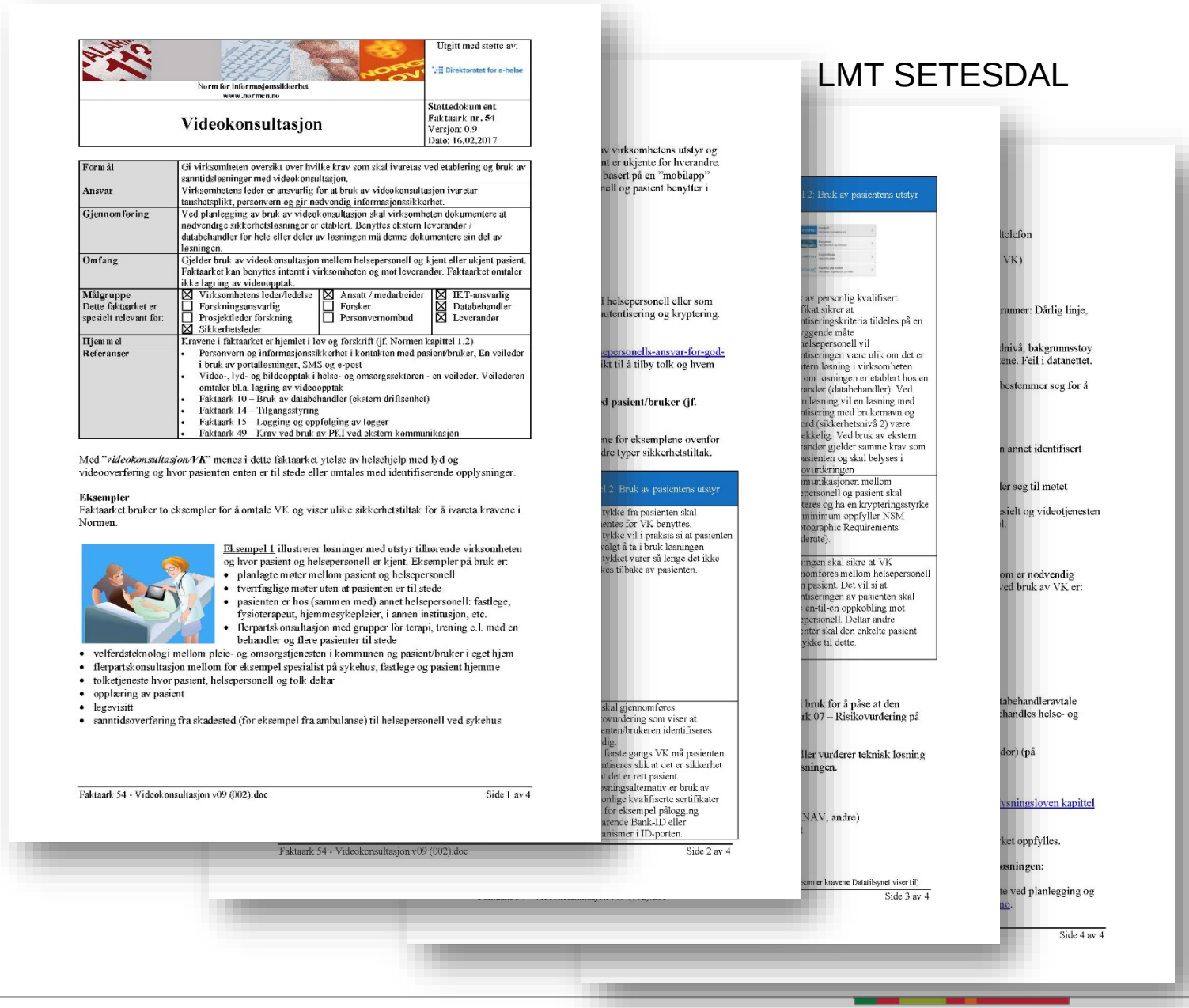
F+ LOKALT

Anmelder person som filmet kommuneansatt

Rådmann Svein Skisland i Vennesla har anmeldt en privatperson for å poste film av en kommuneansatt i tjeneste på Facebook.

JANNE BIRGITTE PRESTVOLD

NYHET – FAKTAARK NR 54:



Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:
Direktoratet for e-helse

Videokonsultasjon

Støttedokument
Faktaark nr. 54
Versjon: 0.9
Dato: 16.02.2017

Formål	Gi virksomheten oversikt over hvilke krav som skal ivaretas ved etablering og bruk av sanntidsløsninger med videokonsultasjon.
Ansvar	Virksomhetens leder er ansvarlig for at bruk av videokonsultasjon ivaretar taushetsplikt, personvern og gir nødvendig informasjonssikkerhet.
Gjennomføring	Ved planlegging av bruk av videokonsultasjon skal virksomheten dokumentere at nødvendige sikkerhetsløsninger er etablert. Benyttes ekstern leverandør / databehandler for hele eller deler av løsningen må denne dokumentere sin del av løsningen.
Omfang	Gjelder bruk av videokonsultasjon mellom helsepersonell og kjent eller ukjent pasient. Faktaarket kan benyttes internt i virksomheten og mot leverandør. Faktaarket omtaler ikke lagring av videoopptak.
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig ☐ Prosjektleder forskning ☒ Sikkerhetsleder ☒ Ansatt / medarbeider ☐ Forsker ☐ Personvernombud ☒ IKT-ansvarlig ☒ Databehandler ☒ Leverandør
Hjemmel	Kravene i faktaarket er hjemlet i lov og forskrift (jf. Normen kapittel 1.2)
Referanser	• Personvern og informasjonssikkerhet i kontakten med pasient/bruker, En veileder i bruk av portalløsninger, SMS og e-post • Video-, lyd- og bildeopptak i helse- og omsorgssektoren - en veileder. Veilederen omtaler bl.a. lagring av videoopptak • Faktaark 10 – Bruk av databehandler (ekstern driftsenhet) • Faktaark 14 – Tilgangsstyring • Faktaark 15 Logging og oppfølging av logger • Faktaark 49 – Krav ved bruk av PKI ved ekstern kommunikasjon

Med "*videokonsultasjon/VK*" menes i dette faktaarket ytelse av helsehjelp med lyd og videooverføring og hvor pasienten enten er til stede eller omtales med identifiserende opplysninger.

Eksempler
Faktaarket bruker to eksempler for å omtale VK og viser ulike sikkerhetstiltak for å ivareta kravene i Normen.

Eksempel 1 illustrerer løsninger med utstyr tilhørende virksomheten og hvor pasient og helsepersonell er kjent. Eksempler på bruk er:
- planlagte møter mellom pasient og helsepersonell
- tverrfaglige møter uten at pasienten er til stede
- pasienten er hos (sammen med) annet helsepersonell: fastlege, fysioterapeut, hjemmesykepleier, i annen institusjon, etc.
- flerpartskonsultasjon med grupper for terapi, trening e.l. med en behandler og flere pasienter til stede
- velferdsteknologi mellom pleie- og omsorgstjenesten i kommunen og pasient/bruker i eget hjem
- flerpartskonsultasjon mellom for eksempel spesialist på sykehus, fastlege og pasient hjemme
- tolketjeneste hvor pasient, helsepersonell og tolk deltar
- opplæring av pasient
- legevisitt
- sanntidsoverføring fra skadested (for eksempel fra ambulanse) til helsepersonell ved sykehus

Faktaark 54 - Videokonsultasjon v09 (002).doc Side 1 av 4

Faktaark 54 - Videokonsultasjon v09 (002).doc Side 2 av 4

Side 3 av 4

Side 4 av 4

LMT SETESDAL

NYHET –

LMT SETESDAL

LMT SETESDAL
LOKALMEDISINSKE
TJENESTER

Setesdalssamarbeid
Bykle, Valle, Bygland,
Evje og Hornnes

Videokonsultasjon

ved bruk av

Lync

og

Skype for Business

Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av: Direktoratet for e-helse

Videokonsultasjon

Støttedokument
Faktaark nr. 54
Versjon: 0.9
Dato: 16.02.2017

Gi virksomheten oversikt over hvilke krav som skal ivaretas ved etablering og bruk av sanntidsløsninger med videokonsultasjon.

Virksomhetens leder er ansvarlig for at bruk av videokonsultasjon ivaretar taushetsplikt, personvern og gir nødvendig informasjonssikkerhet.

Ved planlegging av bruk av videokonsultasjon skal virksomheten dokumentere at nødvendige sikkerhetsløsninger er etablert. Benyttes ekstern leverandør / behandler for hele eller deler av løsningen må denne dokumentere sin del av

av videokonsultasjon mellom helsepersonell og kjent eller ukjent pasient,
n benyttes internt i virksomheten og mot leverandør. Faktaarket omtaler
av videoopptak.

hetens leder/ledelse	☒ Ansatt / medarbeider	☒ IKT-ansvarlig
gsansvarlig	☐ Forsker	☒ Databehandler
eder forskning	☐ Personvernombud	☒ Leverandør
tsleder		

taarket er hjemlet i lov og forskrift (jf. Normen kapittel 1.2)
rn og informasjonssikkerhet i kontakten med pasient/bruker, En veileder
portalløsninger, SMS og e-post
yd- og bildeopptak i helse- og omsorgssektoren - en veileder. Veilederen
bl.a. lagring av videoopptak
10 – Bruk av databehandler (ekstern driftsenhet)
14 – Tilgangsstyring
15 Logging og oppfølging av logger
49 – Krav ved bruk av PKI ved ekstern kommunikasjon

es i dette faktaarket ytelse av helsehjelp med lyd og
enten er til stede eller omtales med identifiserende opplysninger.

å omtale VK og viser ulike sikkerhetstiltak for å ivareta kravene i

sempel 1 illustrerer løsninger med utstyr tilhørende virksomheten
hvor pasient og helsepersonell er kjent. Eksempler på bruk er:
planlagte møter mellom pasient og helsepersonell
tverrfaglige møter uten at pasienten er til stede
pasienten er hos (sammen med) annet helsepersonell: fastlege,
fysioterapeut, hjemmesykepleier, i annen institusjon, etc.
flerpartskonsultasjon med grupper for terapi, trening e.l. med en
behandler og flere pasienter til stede
og omsorgstjenesten i kommunen og pasient/bruker i eget hjem
eksempel spesialist på sykehus, fastlege og pasient hjemme
personell og tolk deltar

l (for eksempel fra ambulanse) til helsepersonell ved sykehus

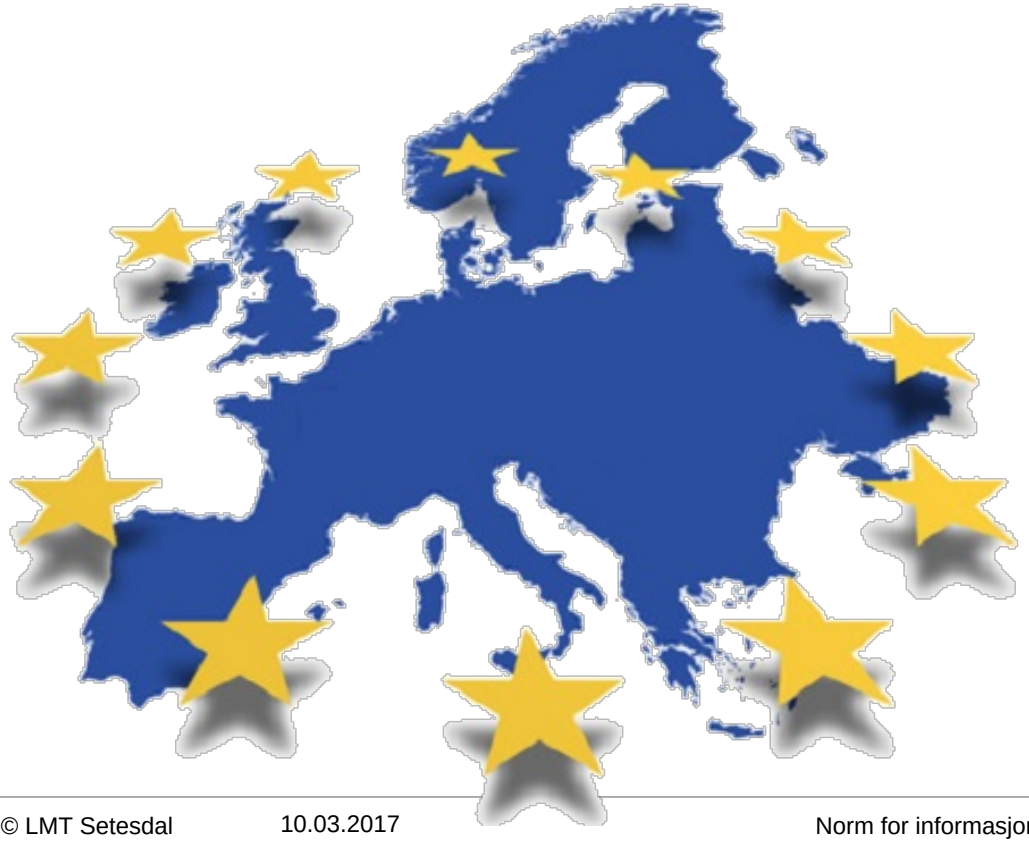
002).doc Side 1 av 4

Faktaark 54 - Videokonsultasjon v09 (002).doc Side 2 av 4

Side 3 av 4

Side 4 av 4

NYTT REGELVERK FRA VÅREN 2018 – EUs PERSONVERNFORORDNING



- Alle offentlige og mange private virksomheter skal opprette personvernombud
- Systemer skal ha innebygd personvern
- Dersom et tiltak utgjør en stor risiko for personvernet, må virksomheten også utrede hvilke personvernkonsekvenser det kan ha
- Informasjon om hvordan din virksomhet behandler personopplysninger skal være lett tilgjengelig og skrevet på en forståelig måte
- Alle virksomheter må sette seg inn i den nye lovgivningen og finne ut hvilke nye plikter som gjelder dem
- Alle avvik som kan medføre risiko for privatpersoner skal meldes til Datatilsynet innen 72 timer
- De nye reglene oppmuntrer til sektorvis utforming av retningslinjer og **bransjenormer**
- Skjerpede sanksjoner der Datatilsynene gis kompetanse til å ilegge overtredelsesgebyr på opp til 4 % av virksomheters globale omsetning

KLM


02-13-;5 06:00p Directory C:\WP51*.*
Document size: 337 Free: 20,070,400 Used: 2,499,881 Files: 54
. Current <Dir>
LEARN . <Dir> 02-13-15 12:53p
CHARACTR.DOC 42,223 11-06-89 12:00p
CONVERT .EXE 105,141 11-06-89 12:00p
ENDFOOT .WPM 3,623 11-06-89 12:00p
EQUATION.WPK 2,978 11-06-89 12:00p
FOOTEND .WPM 3,561 11-06-89 12:00p
GRAPHCNV.EXE 107,520 11-06-89 12:00p
KEYS .MRS 4,800 11-06-89 12:00p
LIBRARY .STY 5,887 11-06-89 12:00p
MACROS .WPK 32,835 11-06-89 12:00p
PRINTER .TST 8,665 11-06-89 12:00p
REVEALCO.WPM 19,117 11-06-89 12:00p
SHORTCUT.WPK 23,381 11-06-89 12:00p
STANDARD.CRS 2,555 11-06-89 12:00p
STANDARD.PRS 1,942 11-06-89 12:00p
WP .EXE 218,112 11-06-89 12:00p
WP .LRS 18,741 11-06-89 12:00p
WP .QRS 16,869 11-06-89 12:00p
.. Parent <Dir>
ALTRNAT .WPK 919 11-06-89 12:00p
CODES .WPM 7,335 11-06-89 12:00p
CURSOR .COM 1,452 11-06-89 12:00p
ENHANCED.WPK 3,355 11-06-89 12:00p
FIXBIOS .COM 50 11-06-89 12:00p
GRAB .COM 15,842 11-06-89 12:00p
INSTALL .EXE 52,224 11-06-89 12:00p
LABELS .WPM 21,176 11-06-89 12:00p
MACROCNV.EXE 26,021 11-06-89 12:00p
NWPSETUP.EXE 27,648 11-06-89 12:00p
REVEALBX.WPM 1,061 11-06-89 12:00p
REVEALTX.WPM 14,609 11-06-89 12:00p
SPELL .EXE 53,760 11-06-89 12:00p
STANDARD.IRS 4,475 11-06-89 12:00p
STANDARD.VRS 29,833 11-06-89 12:00p
WP .FIL 572,569 11-06-89 12:00p
WP .MRS 5,912 11-06-89 12:00p
WP{WP} .BK1 0 02-13-15 06:00p
1 Retrieve; 2 Delete; 3 Move/Rename; 4 Print; 5 Short/Long Display;
6 Look; 7 Other Directory; 8 Copy; 9 Find; N Name Search: 6
WordPerfect
WordPerfect

TAKK FOR OPPMERKSOMHETEN

john.horve@e-h.kommune.no

@johnhorve

916 84 694