Innspill til utkast Normen v6.0

Fra	
Kontaktperson	
Kontaktinfo	
Dato sendt inn	

Spørsmål fra oversendelsesbrev

Er Normens virkeområde nå dekkende for det Normen bør dekke?	
Er Normens virkeområde nå tydelig nok? Vil f.eks. en leverandør forstå om virksomheten er forpliktet til å følge Normens krav?	
I nytt kapittel 4 er det gjort et utvalg av temaer og behandlingsaktiviteter. Gir kapittelet verdi for brukerne? Er det noen viktig som mangler?	
Et av hovedmålene har vært å øke leser- og brukervennlighet. Dette er gjort gjennom forenkling av tekst, fjerning av krav, språklig gjennomgang, økt profesjonsnøytralitet og generell språkvask. Vi ønsker tilbakemeldinger på dette.	
Ved å gjennomgående bruke "skal" og "bør" samt peke på forholdsmessighet og "egnede" tiltak både i kap 1.4 og 3.1 forsøker Normen v6.0 å vise at virksomheten selv må vurdere og ta valg om hva som er egnede tiltak. Kommer dette tydelig nok frem? Er det f.eks. tydelig hvilke informasjonssikkerhetskrav som gjelder sekundærbruk og er det lettere for en liten virksomhet og forstå hvilke krav som gjelder for den?	

Innspill til utkast Normen versjon 6.0

Nr	Overskrift	Kommentar	Evt. endringsforslag
0	**Overordnede kommentarer og innspill til utkastet**		
0.1	Generelle kommentarer og innspill		
0.2	Forslag til innhold - mangler i utkastet		
0.3	Lesbarhet og forenkling		
0.4	Format og stil		
0.5	Andre kommentarer		
1	**Om Normen**		
1	Generelle kommentarer og innspill til kap 1		
1.1	Bakgrunn for Normen		
1.2	Formål		
1.3	Målgruppe – hvem Normen gjelder for		
1.4	Virkeområde – hva Normen regulerer		
1.5	Normens utvikling og forvaltning		
2	**Ledelse og ansvar**		
2	Generelle kommentarer og innspill til kap 2		
2.1	Roller og ansvar for informasjonssikkerhet og personvern		
2.2	Dataansvarliges ansvar		
2.1	Databehandlers ansvar		
2.4	Styringssystem		
2.5	Ledelsens gjennomgang		
3	**Risikostyring**		
3	Generelle kommentarer og innspill til kap 3		
3.1	Forholdsmessighet ved valg av tiltak		
3.2	Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet		
3.3	Oversikt over informasjon og teknologi		

3.4	Risikovurdering og risikohåndtering		
3.5	Vurdering av personvernkonsekvenser		
4	**Grunnleggende om behandling av helse- og pesronopplysninger**		
4	Generelle kommentarer og innspill til kap 4		
4.1	Behandlingsgrunnlag		
4.2	Plikter og krav ved behandling av helse- og personopplysninger		
4.2.1	Taushetsplikten		
4.2.2	Informasjon til den registrerte		
4.2.3	Innsyn		
4.2.4	Retting og sletting		
4.2.5	Sperring av opplysninger i journal		
4.2.6	Tilgjengeliggjøring og utlevering		
4.2.7	Krav til lagring av helse- og personopplysninger		
5	**Informasjonssikkerhet**		
5	Generelle kommentarer og innspill til kap 5		
5.1	Ansatte, kompetanse og holdningsskapende arbeid		
5.1.1	Vilkår og betingelser		
5.1.2	Opplæring og kompetanse		
5.2	Tilgangsstyring		
5.2.1	Autorisering		
5.2.2	Autentisering		
5.2.3	Kontroll av tilgangsrettigheter		
5.3	Fysisk sikkerhet og håndtering av utstyr		
5.3.1	Nøkler/adgangskort		
5.3.2	Brukerutstyr (PC og printere - stasjonære)		
5.3.3	Infrastruktur		
5.3.4	Mobilt utstyr og hjemmekontor		
5.3.5	Kryptering		
5.3.5	Medisinsk utstyr		
5.4	Sikker IT-drift		
5.4.1	Sikkerhetsarkitektur		
5.4.2	Konfigurasjonskontroll		
5.4.3	Endringsstyring		
5.4.4	Sikkerhetskopiering		
5.4.5	Logging		
5.4.6	Styring og håndtering av tekniske sårbarheter		
5.4.7	Sikkerhetsrevisjon av informasjonssystemer		
5.5	Kommunikasjonssikkerhet		
5.5.1	Styring av nettverkssikkerhet		
5.5.2	Sikring av nettjenester		
5.5.3	Meldingsformidling		
5.5.4	E-post, SMS og sosiale medier		
5.5.5	Tilkobling til Internett		
5.6	Digital kommunikasjon med den registrerte		
5.6.1	Digital meldingskommunikasjon med den registrerte		
5.7	Leverandørforhold og avtaler		
5.7.1	Generelt om avtaler og leverandøroppfølging		
5.7.2	Krav til leverandørers håndtering av helse- og personopplysninger		
5.7.3	Databehandler		
5.7.4	Tjenesteutsetting (utkontraktering)		

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		
5.8	Håndtering av informasjonssikkerhetsbrudd		
5.8.1	Avvikshåndtering		
5.8.2	Melding til Datatilsynet om brudd på personopplysningssikkerheten		
5.8.2	Underretting til den registrerte		
5.9	Kontinuitetsplanlegging		
6	Vedlegg		
6	Generelle kommentarer og innspill til resten av kap 6		
6.1	Definisjoner		
6.2	**Oversikt over Normens krav**		