Direktoratet for e-helse

Digitaliseringsdirektoratet - Digdir
Postboks 1382 Vika
0114 OSLO

Deres ref.:
Vår ref.: 22/497-2
Saksbehandler: Aasta Margrethe Hetland
Dato: 25.08.2022

Høringsuttalelse - Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning

Vedlagt følger høringsuttalelse på Digitaliseringsdirektoratets høring Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning, datert 16.06.2022

Vennlig hilsen

Mariann Hornnes
direktør

Birgitte Jensen Egset
avdelingsdirektør

Dokumentet er godkjent elektronisk

Vedlegg:
Høringsuttalelse

Direktoratet for e-helse

Postboks 221 Skøyen, 0213 OSLO • Besøksadresse: Verkstedveien 1 • postmottak@ehelse.no
Tlf.: 21 49 50 70 • Org.nr.: 915 933 149 • www.ehelse.no

Direktoratet for e-helse

Høringsuttalelse

Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning

Høringsbrev og notat fra Digitaliseringsdirektoratet datert 22.06.2022

Direktoratet for e-helse takker for muligheten til å gi innspill til pågående arbeid «Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning». Direktoratet for e-helse benytter anledningen til å gi innspill til notat som foreligger i forbindelse med høringsrunden.

Direktoratet for e-helse styrker digitaliseringen i helse- og omsorgssektoren ved å understøtte effektive og sammenhengende helse- og omsorgstjenester. Direktoratet legger til rette for nasjonal samordning og en helhetlig og forutsigbar e-helseutvikling. Direktoratet for e-helse skal sørge for nasjonal styring og koordinering i samarbeid med helseforetak, kommuner, fagmiljø og interesseorganisasjoner.

Overordnet tilbakemelding

Direktoratet for e-helse bruker Digitaliseringsdirektoratet og andre sentrale veiledningsaktørers materiell i sitt veiledningsarbeid, både i rollen som fagorgan for informasjonssikkerhet i sektoren og som sekretariat for Normen. Direktoratet for e-helse viser til sentrale aktørers veiledningsmateriell på sektorovergripende og generelle temaer og problemstillinger, og jobber selv med sektorrettet veiledning og tiltak.

Direktoratet for e-helse er positive til at Digitaliseringsdirektoratet forsøker å løse utfordringene som beskrives i utfordingsbildet. Helse- og omsorgssektoren er avhengig av god samhandling og deling av data i og mellom virksomheter.

Direktoratet for e-helse er positive til at Digitaliseringsdirektoratet tar initiativ for å samle og koordinere veiledningsaktører og veiledningsaktiviteter. Som både fagorgan for informasjonssikkerhet i helse- og omsorgssektoren og som sekretariat for Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren (Normen)[1] har vi identifisert behovet for felles retning på dette feltet. Høringsutkastet innholdet mange gode momenter og ideer.

Det er mange aktører som stiller krav, tilbyr veiledning og tolker regelverk på området. Og det er krav til informasjonssikkerhet i flere ulike lover og forskrifter. Aktørene må bli bedre omforent om begreper, og deres ansvarsområder må klargjøres. I Direktoratet for e-helses arbeid med digital sikkerhet blir vi møtt med at det er mer enn nok veiledningsmateriale, at det er utfordrende å finne frem til det som passer den enkelte virksomhet og at det er behov for konkret bistand. Det er positivt at Digitaliseringsdirektoratet tar initiativ til å gjøre noe med dette.

[1] https://www.ehelse.no/normen

Direktoratet for e-helse mener videre at konseptets forvalting og ansvar, samt økonomiske og administrative konsekvenser må utredes.

Begrepet «felles referanseramme» må tydeliggjøres og «normeringsgraden» må utredes nærmere i det videre arbeidet.

Vi vil komme nærmere inn på dette gjennom svarene på Digitaliseringsdirektoratets konkrete spørsmål.

Svar på Digitaliseringsdirektoratets spørsmål

Digitaliseringsdirektoratet ber særlig om innspill på følgende spørsmål:

1. Er det mangler i beskrivelsen av utfordringsbildet?
2. Vurderer dere den beskrevne strategiske retningen som egnet for å styrke arbeidet med informasjonssikkerhet i forvaltningen?
3. Hvilke synspunkter har dere på en tydeligere felles referanseramme (eller «norm») for offentlige virksomheters arbeid med informasjonssikkerhet og de andre konseptene som beskrives?
4. Hvordan vurderer dere behovet for samarbeid for å nå målsetningene som beskrives i notatet, og har dere innspill på hvordan et slikt samarbeid bør innrettes og organiseres?
5. Hvilke andre initiativer det er viktig å ta hensyn til i videre arbeid?

1. Er det mangler i beskrivelsen av utfordringsbildet?

Direktoratet for e-helse har nå ute på høring «Innspill til kommende stortingsmelding om helseberedskap – Digital sikkerhet»[2]. I dette dokumentet gir vi på oppdrag fra Helse- og omsorgsdepartementet innspill innen området digital sikkerhet til arbeidet med ny stortingsmelding om helseberedskap. Denne meldingen skal legges frem våren 2023, og vil ta for seg digital beredskap og sikkerhet som ett blant flere temaer.

I innspillet gis en beskrivelse av utfordringsbildet for helse- og omsorgssektoren innen området digital sikkerhet. Vår sektor står overfor et skjerpet digitalt trusselbilde, samtidig som den preges av et komplekst systemlandskap og mangelfull implementering av grunnleggende sikkerhetstiltak (på lik linje med de fleste andre sektorer). Det er et udekket kompetansebehov blant sektorens virksomheter. Vurderinger og oppfølging av sikkerhet på komplekse områder som digitale verdikjeder og ny teknologi er særlig krevende, ikke minst for sektorens mange små virksomheter. I innspillet peker vi også på at ansvarsforholdene kan være komplekse. Dataansvar, leverandøroppfølging og verdikjeder samt nasjonal IKT-helseberedskap trekkes særlig frem som eksempler på dette.

Vi oppfatter at problembeskrivelsen som Digitaliseringsdirektoratet legger til grunn i sitt notat, for en stor del samsvarer eller overlapper med utfordringsbildet vi beskriver. Det er en grundig og god problembeskrivelse.

[2] https://www.ehelse.no/horinger/innspill-til-kommende-stortingsmelding-om-helseberedskap--tema-digital-sikkerhet

2. Vurderer dere den beskrevne strategiske retningen som egnet for å styrke arbeidet med informasjonssikkerhet i forvaltningen?

Som nevnt innledningsvis er Direktoratet for e-helse positive til at Digitaliseringsdirektoratet forsøker å løse utfordringene som beskrives i utfordingsbildet, samt tar initiativ for å samle og koordinere veiledningsaktører og veiledningsaktiviteter.

Høringsutkastet er delvis konkret på enkelte konsepter og vagt på andre deler. Det er noe uklart hva som er det strategiske og hva som er konkrete tiltak.

Konseptet og den strategiske retningen må ta hensyn til sektorregelverk og gi muligheter for å løse de særlige utfordringer, risikoer og behov som gjør seg gjeldende i ulike sektorer.

Det er ikke utredet hvilke økonomiske og administrative konsekvenser dette forslaget vil få for virksomhetene som skal følge kravene og veiledningen, og for aktørene som skal være med i arbeidet. Forvaltningen av tiltakene som skisseres vil bli ressurskrevende og gå på tvers av ansvarsområder.

Slik det er nå så oppleves det uklart hvordan foreslått konsept vil bidra til økt kompetanse og modenhet der den i dag er lav. Dette kommer nok an på hvordan løsningen blir i praksis. Det å få en peker til et sett av tiltak vil være bra i tilfeller med lav kompetanse, på den måten at man pekes i en god retning. Men det er ikke gitt at man skjønner hvorfor man trenger dette tiltaket. Et sikkerhetstiltak kan også ofte implementeres med ulik kvalitet, dermed er det ikke nødvendigvis så enkelt som at enten har man et tiltak eller så har man det ikke. Kvaliteten i implementeringen er også avhengig av planlagt og god opplæring, kommunikasjon og kulturbygging. Dette bør inn som egne overordnede tiltak.

Samtidig er det ofte mye læring i å samhandle med andre med større modenhet, for eksempel ved å gjøre felles risikoanalyser eller lære av andres risikoanalyser. For å øke modenhet kan det muligens være mer nyttig å samhandle med andre som har erfaring på området, eller se hvilke vurderinger andre har gjort i konkrete tilfeller.

En utfordring det pekes på er at anbefalinger/veiledninger ikke blir fulgt opp. Dette bør også tas med i det videre arbeidet.

Startpunkt i kommunene er positivt fordi modenheten i kommunesektoren er til dels lav. Direktoratet for e-helse vil samtidig peke på at kommunene er meget komplekse virksomheter og omfatter flere sektorer. Det vil være avgjørende med meget god samordning og ansvarsavklaring med KS og andre som stiller krav og veileder. Forsvarlig helsehjelp og andre tjenester i helse- og omsorgssektoren krever samhandling og deling av data mellom virksomheter i både stat, kommune og privat sektor. En risiko ved at kommuner blir fokus innledningsvis kan være at det legger premisser som kan gjøre samhandling og deling med andre sektorer vanskeligere.

Utfordringsbildet peker på flere ulike utfordringer. Det er ikke tilstrekkelig begrunnet at den beskrevne strategiske retningen (felles referanseramme for informasjonssikkerhet) vil hjelpe på alle disse ulike utfordringene. Det er også vanskelig å se for seg at disse ulike utfordringene (lav modenhet hos noen, kjeder av tjenester, leverandørrelasjoner) kan håndteres med samme tiltak. En videre utredning må også se på om bedre effekt kan oppnås ved alternative løsninger.

Direktoratet for e-helse støtter deler av den strategiske tanken, men mener at forvalting og ansvar, samt økonomiske og administrative konsekvenser må utredes først. Dette er tiltak med så stor betydning at Utredningsinstruksen må følges.

3. Hvilke synspunkter har dere på en tydeligere felles referanseramme (eller «norm») for offentlige virksomheters arbeid med informasjonssikkerhet og de andre konseptene som beskrives?

Direktoratet for e-helse mener at en bedre omforent forståelse av informasjonssikkerhet i det offentlige vil være positivt. Digitaliseringsdirektoratet tar et viktig initiativ og grep for å sikre dette med utsendt notat.

Direktoratet for e-helse mener videre det er uklart hva som menes med «en tydeligere felles referanseramme (eller «norm»)». Begrepet «norm» brukes kun i oversendelsesbrevet og ikke selve forslaget. Et sted i forslaget brukes også begrepet «sterke anbefalinger».

E-forvaltningsforskriften § 15 pålegger forvaltningen å ha styring og interkontroll av informasjonssikkerhet «som baserer seg på anerkjente standarder». Det kommer ikke frem hvilken status de skisserte tiltakene vil ha; vil den være nok en standard blant mange, eller vil man kunne legge til grunn at denne har forrang og vil sikre at man etterlever tilstrekkelig god informasjonssikkerhet om den følges? Hvilke konsekvenser vil en slik tiltaksbank ha i forhold til leverandørene, som gjerne forholder seg til internasjonale standarder?

Det er stor forskjell på veiledende råd og bindende krav. Det er ikke likt hva ulike forvaltningsaktørene legger i begrepene veileder, retningslinje, standard osv. Dette er noe forvaltningen burde jobbet med slik at underliggende etater og virksomheter som skal ta i bruk produktene vet hva som forventes av dem uansett hvilken offentlig myndighet det kommer fra. Dette vil igjen påvirke kompetanse, kultur og vilje til å ta i bruk og følge standarder.

Direktoratet for e-helse mener at begrepet «felles referanseramme» må tydeliggjøres og «normeringsgraden» må utredes nærmere i det videre arbeidet.

Helse- og omsorgssektoren består av flere små og store virksomheter, kommunale, statlige og private. I det videre arbeidet blir det viktig å avklare hvilke virksomheter i sektoren som er målgruppe for konseptet.

Vi vil gi noen konkrete tilbakemeldinger på utvalgte deler av tiltakene som skisseres.

Helhetlig virksomhets- og sikkerhetsstyring

Tiltakene må utformes på en måte som gjør at de kan inkorporeres i virksomhetsstyringen og en helhetlig sikkerhetsstyring.

Beskrivelser av konsekvenskategorier og -nivåer må legge til rette for at de enkelt kan integreres i øvrig risikorammeverk hos virksomhetene så ikke informasjonssikkerhet må håndteres på siden. De ulike konsekvensene og ulike risikoene må ses i sammenheng når man skal beslutte hva virksomheten skal gjøre. Dette gjelder ikke bare konsekvenskategorier. Om metodikken for informasjonssikkerhetsrisiko blir helt annerledes enn det man gjør for annen type risiko, så kan det gjøre det vanskeligere å få informasjonssikkerhet med i beslutningene.

Den nye Sikkerhetsloven setter f.eks. klare krav til overordnet sikkerhetsledelse/-styring i offentlig forvaltning. Selv om denne omhandler nasjonale sikkerhetsinteresser

særskilt, er prinsippene i dette arbeidet allmenngyldige for sikkerhetsarbeid generelt og godt beskrevet. NSMs Veileder i sikkerhetsstyring og Grunnprinsipper for sikkerhetsstyring beskriver i detalj hvordan den helhetlige sikkerhetsstyringen bør gjennomføres. Den peker på at alle verdier må sees i sammenheng for å kunne beskyttes, og det skilles ikke mellom forebyggende sikkerhetsarbeid innen fysisk sikring, personellsikkerhet, informasjonssikkerhet eller beredskap. Det skal behandles helhetlig, ikke i båser.

Konseptet bør ikke skape unødvendig merarbeid og kostnad for virksomheter som har tilpasset sitt styringssystem og sine sikkerhetstiltak til eksisterende sektorregelverk og tilhørende veiledning

Summen av tiltak på området bidrar til økt sikkerhet, ikke bare fokus på etterlevelse av regelverk. Det viktigste er å utvikle sikkerhetskultur og –kompetanse i virksomhetene, og integrere sikkerhet i virksomhetsstyringen. Opplæring av lederne i virksomhetene er viktig slik at sikkerhetsstyringen blir en del av virksomhetsstyringen.

Bygge på det som finnes og er i bruk i dag

Det finnes etter hvert svært mye veiledningsmateriell, standarder, beste praksis osv. Digitaliseringsdirektoratet står selv for et omfattende veiledningsmateriale. Det er viktig å unngå at det nasjonale løftet ikke ender opp med mer av det samme som vi allerede har i dag. Tiltakene T3-T6 ser ut til å peke i en retning av mer konkrete verktøy og hjelpemidler enn vi har i dag, men samtidig er det klart at det allerede finnes en rekke standarder innenfor informasjonssikkerhet som inneholder diverse former for tiltaksbanker. Utfordringen er å plukke ut, implementere og vedlikeholde de riktige tiltakene.

Det er viktig å bygge på det som allerede finnes, som f.eks. NSM sine grunnprinsipper og deres anbefalinger om hva som er viktigst å begynne med for å øke sikkerheten, og i vår sektor Normens krav og veiledning i helse- og omsorgssektoren. Det må ikke bygges opp mer av det samme som skal virke parallelt.

Vi savner en nærmere drøfting av sammenhengen med NSM grunnprinsipper for IKT-sikkerhet. Mange virksomheter arbeider i dag med innføring av grunnprinsippene.

Begrepet «Sikkerhetstiltak»

Direktoratet for e-helse mener at det bidrar til usikkerhet at aktiviteter som omfattes av «Styring og kontroll» ikke anses som sikkerhetstiltak. Dette er ikke vanlig begrepsforståelse.

Basisnivå

Det bør vurderes om det er hensiktsmessig med et basisnivå (med et utvalg av tiltak) med tilleggsnivåer (som inkluderer flere tiltak), eller om man heller skal fokusere på å tegne et forslag til veikart for hvordan man løpende skal jobbe for å dekke fler og fler relevante tiltaksområder og parallelt komme opp på ønsket modenhetsnivå. Her er det mye som allerede er beskrevet i NSMs grunnprinsipper.

I en modell med basisnivå er det viktig at man finner måter å sikre at virksomhetene uansett tar sitt ansvar for å løpende inkludere sikkerhet i virksomhetsstyringen, og ikke bare stopper ved å implementere minimum sikringstiltak som en engangsoppgave.

Basisnivå kan gi inntrykk av at basis er nok, spesielt i umodne virksomheter.

Ved utforming av «basistiltak» må man ta hensyn til mangfoldet av regelverk/krav som stilles, slik at man ikke ender opp med «basistiltak» som ikke tilfredsstiller kravene virksomhetene er pålagt å etterleve.

Personvern

Personvern blir nevnt, men ikke tilstrekkelig. Dette må også utredes nærmere. Selv om personvern og informasjonssikkerhet har svært mange felles trekk og deler av arbeidet må ses i sammenheng, må man være obs på at det er forskjeller mellom de to som kan ha betydning.

Det er avgjørende at Datatilsynet stiller seg bak konseptet og samordner sitt veiledningsmateriell med konseptet som er skissert.

Sikkerhetskrav i Normen

Det foreslås at Normens kapittel 5 kan byttes ut med basisnivå for helsetjenester. Det er alle Normens skal-krav, ikke bare kapittel 5, som i dag utgjør basisnivået for helsetjenester. Konseptet må utredes nærmere før det går an å si noe mer om det skisserte eksemplet er realiserbart.

Det er sektoren gjennom Styringsgruppen for Normen som sammen beslutter Normens krav. Høringen er ikke sendt til Styringsgruppen for Normen og Direktoratet for e-helse kan ikke svare på om styringsgruppen vil støtte dette forslaget.

Trusselvurderinger

Digitaliseringsdirektoratet som faginstans kan bruke sin kompetanse i samarbeid med andre for å gi forvaltningen mer konkrete og praktiske råd enn man gjør i dag. Et mulig eksempel på et slikt område er trusselvurderinger. Ideelt sett skal enhver virksomhet gjøre sine egne vurderinger av hvilke trusler og risikoscenarier som er relevante. Et nasjonalt løft i form av for eksempel en tiltaksbank, normering av konsekvenskategorier og-nivåer med mere kan være positivt fordi det gir en helhetlig oversikt. Men det kan også oppleves som en akademisk tilnærming som ikke gir verdi «her og nå». Trusselbildet er stadig i endring og det varierer hva som peker seg ut som «ti på topp». Forvaltningen består av små og store virksomheter og det krever en god del kunnskap og ressurser å ha oversikt over hva som til enhver tid er «verstinger» man må ha kontroll på. Her kan Digitaliseringsdirektoratet eller andre ta et mer aktivt ansvar for å holde forvaltningen oppdatert om trusselbildet og gjerne også redegjøre for relevante risikoscenarier. Flere aktører informerer og veileder om trusselbildet. Digitaliseringsdirektoratet kan samarbeide med dem og veilede forvaltningen på det som er spesielt for dem. Dette kan være til stor praktisk hjelp i virksomhetenes risikoarbeid.

Slike konkrete vurderinger kan ha en pedagogisk effekt med tanke på å skape forståelse for betydningen av informasjonssikkerhetsarbeidet og kan øke forståelsen for at informasjonssikkerhetsarbeidet er «ferskvare» og må pågå kontinuerlig.

Leverandører og andre utenfor forvaltningen

Det er mye som taler for mer standardisering på krav til leverandører. Flere leverandører bruker anerkjente internasjonale standarder. Norge er et relativt lite marked og særnasjonale krav kan bli fordyrende.

Helsesektoren består av både offentlige og private helseforetak som skal samarbeide. Det er viktig for samhandlingen i sektoren at man ikke isolert ser på forvaltningen, men også de som forvaltningen samhandler med.

Spredning av konseptet

Vi anbefaler at det tidlig i det videre arbeidet lages planer for opplæring og spredning av konseptet. Målgruppe, både på virksomhets- og rollenivå må avklares.

4. Hvordan vurderer dere behovet for samarbeid for å nå målsetningene som beskrives i notatet, og har dere innspill på hvordan et slikt samarbeid bør innrettes og organiseres?

Direktoratet for e-helse støtter behovet for tettere samarbeid på området og ser det som avgjørende når utfordringene beskrevet innledningsvis skal håndteres.

Som tidligere nevnt er det mange aktører som stiller krav, tilbyr veiledning og tolker regelverk på området. Disse må bli bedre omforent om begreper, og deres ansvarsområder må klargjøres. Aktørene må instrueres til å samarbeide og samarbeidet må koordineres.

Tydeligere krav og oppfølging (f.eks. måling) fra overordnet virksomhet i styringsdialogen om forhold som angår informasjonssikkerhet vil være med på å holde høyere fokus og kvalitet på arbeidet med informasjonssikkerhet i virksomhetene. Virksomhetene får på denne måten også tildelt/prioritert nødvendige ressurser til forbedringsarbeid innen informasjonssikkerhet.

Direktoratet for e-helse, både som fagdirektorat og som sekretariat for Normen, er meget positive til å være med i arbeidet videre.

Direktoratet er usikre på hvilke målsetninger det pekes på her, Som nevnt tidligere må konseptet utredes videre med tanke på forvaltning, ansvarsfordeling og økonomiske/ administrative konsekvenser.

5. Hvilke andre initiativer det er viktig å ta hensyn til i videre arbeid?

Normen er en bransjenorm som er utarbeidet og forvaltes av organisasjoner og virksomheter i helse- og omsorgssektoren. Kravene i Normen er et omforent kravsett basert på norsk lov og beste praksis, og inneholder en rekke krav til helsevirksomhetene innen personvern og informasjonssikkerhet. Normen gjelder for enhver virksomhet som ved avtale har forpliktet seg til å følge den. Dette skjer blant annet ved medlemskap i Helsenettet. I tillegg bruker mange virksomheter Normen som grunnlag for å stille krav til sine kunder og leverandører. Direktoratet for e-helse er sekretariat for arbeidet til Normens styringsgruppe, sammen med NHN.

Normens aktiviteter består i tillegg til selve kravsettet for informasjonssikkerhet og personvern av veiledningsmateriell til Normens krav og er en arena for kompetanseheving og nettverksbygging for sektoren. Veiledningsmateriellet i Normen utbedres og suppleres kontinuerlig i tråd med utviklingen og behovene i sektoren. Normen driver også utstrakt utadrettet kompetansehevings- og nettverksaktivitet. Sekretariatet for Normen holder løpende foredrag, kurs og webinarer for sektoren.

Ny stortingsmelding om helseberedskap skal legges frem våren 2023, og vil ta for seg digitale beredskap og sikkerhet som ett blant flere tema. Se mer om denne under spørsmål 1.