

Direktoratet for e-helse
Postboks 221 Skøyen
0213 OSLO

Deres ref.:
23/596

Vår ref.:
23/7-87

Saksbehandler:
KSV

Dato:
14.09.2023

Høringssvar sak 23/596 - apper for helse og velvære - kvalitet og pålitelighet - NS-CEN TS/ISO 82304-2:2021 og veileder for kvalitetssikring av ikke-medisinske helseapper

Innledning

Digitaliseringsdirektoratet (Digdir) viser til høring om Apper for helse og velvære – Kvalitet og pålitelighet (TS/ISO 82304-2:2021) og Veileder for kvalitetssikring av ikke-medisinske helseapper.

Det er positivt at Direktoratet for e-helse ønsker å gi veiledning på kvalitetssikring og pålitelighet ved utvikling av slike produkter, og veiledningen har et viktig virkeområde.

Dette høringssvaret er utarbeidet av Statens kompetansemiljø for informasjonssikkerhet i Digdir. Innspillene er gitt med grunnlag i Digdirs rolle som premissgiver og veiledningsaktør for styring av informasjonssikkerhet for offentlig sektor.

Apper for helse og velvære – Kvalitet og pålitelighet (TS/ISO 82304-2:2021)

Direktoratet for e-helse ønsker tilbakemelding på følgende:

- Er anbefalt standard riktig normeringsnivå? Hvis ikke, gi en begrunnelse

Digdir har ikke kjennskap til standarden «Apper for helse og velvære – Kvalitet og pålitelighet (TS/ISO 82304-2:2021)». Vi ser imidlertid at det er en standard som brukes i arbeidet med apper for helse og velvære i EU. Det vil være naturlig å reflektere standardens status i EU også innen Norge. Anbefalt standard virker derfor å være riktig normeringsnivå.

Veileder for kvalitetssikring av ikke-medisinske helseapper og digitale helseverktøy

Direktoratet for e-helse ønsker tilbakemelding på følgende:

- Er veileder riktig normeringsnivå? Hvis ikke, gi en begrunnelse
- Er kravene tydelige og dekkende? Hvis ikke, gi en begrunnelse og forslag til endringer

Digdir har ikke inngående kjennskap til normering av Direktoratet for e-helses produkter, men på generelt grunnlag anser vi veileder til å være et hensiktsmessig normeringsnivå.

Slik veilederen er utformet nå er det et godt utgangspunkt for de som skal utvikle eller ta i bruk ikke-medisinske helseapper. Det synes imidlertid å være en kombinasjon av lovpålagte krav (for eksempel universell utforming og personvern), og kriterier som ikke er lovpålagt (for eksempel bruk av prosess for sikker utvikling). Det kan være hensiktsmessig å tydeliggjøre

hva som er «må-krav», for å gjøre det klarere for brukerne hvilke krav som må gjennomføres fullt ut, og hvilke det er mer opp til brukerne å vurdere behov for og grad av oppfyllelse av.

Direktoratet for e-helse kan også vurdere om det i noen tilfeller kan være hensiktsmessig å henvise til ytterligere veiledning for å hjelpe brukerne i vurderingen av om de oppfyller et krav, og hva som eventuelt må gjøres for å oppfylle det. For eksempel kan man i kriterium nr. 39 angående styringssystem for informasjonssikkerhet vurdere å henvise til Digitaliseringsdirektoratets veiledning «[Internkontroll i praksis – informasjonssikkerhet](#)». Dette veiledningsmateriellet er basert på ISO 27001, og er offentlig tilgjengelig for alle selv om den i utgangspunktet retter seg mot offentlige aktører.

Digdir anbefaler Direktoratet for e-helse å lage en plan for forvaltning av veilederen, inkludert hvordan fremtidige endringer håndteres. Det gjøres mye arbeid innenfor informasjonssikkerhet som f.eks. om Cyber Resilience Act, som regjeringen nylig har laget et [posisjonsnotat](#) om. Det må forventes at vedlikehold av veilederen blir nødvendig.

Avslutning

Digitaliseringsdirektoratet setter stor pris på å få anledning til å gi innspill til produkter som utvikles i den hensikt å gi offentlige virksomheter veiledning knyttet til informasjonssikkerhet. For å sikre en best mulig samordning av den veiledningen brukerne får, er det nyttig for oss å ha kjennskap til hvilke produkter som er tilgjengelige.

Vennlig hilsen
for Digitaliseringsdirektoratet

Katrine Aam Svendsen
fung.seksjonssjef

Dokumentet er elektronisk godkjent og har derfor ingen signatur

Kopi til:
Tuva Føleide Knutsen