Innspill – EUs foreslåtte forordning - CSAR

Dokumentet er signert digitalt av følgende undertegnere:

- Haugland, Knut Michael K (12.07.1989), signert 12.10.2025 med Signicat Sign BANKID

Det signerte dokumentet innholder
• En forside med informasjon om signaturene
• Alle originaldokumenter med signaturer på hver side
• Digitale signaturer

Dokumentet er forseglet av Posten Norge
Signeringen er gjort med digital signering levert av Posten Norge AS. Posten garanterer for autentisiteten og forseglingen av dette dokumentet.

Slik ser du at signaturene er gyldig
Hvis du åpner dette dokumentet i Adobe Reader, skal det stå øverst at dokumentet er sertifisert av Posten Norge AS. Dette garanterer at innholdet i dokumentet ikke er endret etter signering.

Oslo, 10.10.2025

Til:
Justis- og beredskapsdepartementet v/ statsråden

Kopi:
Nærings- og fiskeridepartementet
Datatilsynet
Norges delegasjon til EU, Brussel

Innspill – EUs foreslåtte forordning om bekjempelse av seksuelt overgrepsmateriale (CSAR / «Chatkontroll»): Mulige konsekvenser for norsk næringsliv, datasuverenitet og rettssikkerhet

1 Innledning

WAYSCloud AS er en norsk leverandør av sky- og infrastrukturtjenester med drift og databehandling i Norden.

Vår virksomhet bygger på prinsippet om null innsyn og kundekontrollerte nøkler, slik at data som lagres hos oss ikke kan leses verken av leverandøren selv eller tredjepart – i en tid der kontroll over egne data er blitt en grunnleggende forutsetning for digital sikkerhet og tillit.

Vi ønsker med dette brevet å dele våre faglige vurderinger av de tekniske, rettslige og næringsmessige konsekvensene som etter vår forståelse kan oppstå dersom EUs foreslåtte forordning om bekjempelse av seksuelt overgrepsmateriale (CSAR / «Chatkontroll») innføres i EØS-området uten særskilte tilpasninger.

2 Bakgrunn

Formålet – å beskytte barn mot overgrep – er både legitimt og ekstremt viktig.

Vår bekymring gjelder måten tiltakene foreslås gjennomført på: forslaget åpner for pålegg om skanning («detection orders») og automatisk rapportering av digitalt innhold, også der sterk kryptering er en forutsetning for sikkerhet og tillit.

waysCloud.no no@wayscloud.net 22 25 80 00 Universitetsgata 2 0164 OSLO 833 735 462 MVA

Slik vi forstår forslaget, kan dette i praksis innebære at europeiske leverandører må bygge inn overvåkingsmekanismer i sine produkter. Etter vår vurdering kan slike krav:

– svekke konfidensialitet og tillit,

– øke risikoen for feilbruk og datalekkasje, og

– skape konkurranseulemper for europeiske aktører sammenlignet med leverandører utenfor EU / EØS.

3.1 Konsekvenser for norsk-europeisk næringsliv

Norske skyleverandører og teknologiselskaper er avhengige av tillit og forutsigbare rammevilkår. Dersom skanning pålegges infrastruktur- eller kommunikasjonstjenester, kan det etter vår oppfatning:

– redusere etterspørselen etter nasjonale eller nordiske og europeiske løsninger,

– påføre betydelige etterlevelses- og utviklingskostnader, og

– føre til at data flyttes til jurisdiksjoner som oppleves som mer fortrolige.

Dette kan etter vårt syn svekke Norges mål om digital selvstendighet og nordisk datasuverenitet.

3.2 Teknisk realitet og arkitekturkonsekvenser

Moderne skyløsninger er i praksis kryptert hele veien – under transport, i lagring og i intern tjenestekommunikasjon. WAYSCloud benytter anerkjente sikkerhetsstandarder for data i ro og i bevegelse og tilbyr kundestyrte nøkler for virksomheter som krever full kontroll.

Når kunden legger på egne krypteringslag – som full diskkryptering, applikasjonsnøkler eller egne sertifikater – har vi ikke teknisk mulighet til å inspisere innholdet uten å bryte sikkerheten og kundens rett til konfidensialitet.

Å gjennomføre slik skanning vil etter vår oppfatning kreve inngrep i grunnleggende sikkerhetsprinsipper og undergrave tilliten til norsk skytjenesteindustri.

3.3 Forholdet til GDPR og innovasjon

Etter vår forståelse står forslaget også i spenn til GDPR. Mange av våre kunder bruker plattformen til å utvikle egne produkter som omfattes av regelverket, og de er selv behandlingsansvarlige for personopplysninger.

Dersom infrastrukturleverandører pålegges å installere skannings- eller overvåkingsprogramvare i kundenes miljøer, vil kundene miste kontroll over egen databehandling og komme i konflikt med sine plikter etter GDPR.

Etter GDPR artikkel 32 skal virksomheter iverksette «egnede tekniske og organisatoriske tiltak» for å sikre behandlingen, herunder bruk av kryptering. Et pålegg om å svekke slike tiltak vil stå i motstrid til databehandleransvarets kjerneforpliktelser.

Dette kan skape en uløselig dobbeltrolle, der aktørene skal sikre konfidensialitet og samtykke – samtidig som de pålegges uautorisert innsyn.

4.1 Ansvarsavklaringer

Slik vi oppfatter det, retter forslaget pliktene mot tjenestetilbydere i bred forstand. Etter vår forståelse vil en hosting- og infrastrukturtilbyder som WAYSCloud kunne omfattes av krav om risikovurdering og rapportering, samt i visse tilfeller pålegg om deteksjon eller fjerning av offentlig tilgjengelig materiale.

Våre B2B-kunder, som utvikler egne applikasjoner – for eksempel meldings- eller kommunikasjonstjenester – vil samtidig være selvstendige tilbydere med direkte plikter etter forordningen, herunder eventuelle deteksjonspålegg for såkalt grooming-innhold.

Vi ønsker å peke på at norsk posisjon bør tydeliggjøre at ansvaret bør følge faktisk tilgang og kontroll:

– Nøytrale infrastrukturtjenester uten innsyn bør ikke pålegges politi- eller etterforskningsroller.

– Applikasjonstilbydere med reell kontroll over innholdet bør bære ansvaret der tiltak anses forholdsmessige og rettslig hjemlet.

En slik ansvarsdeling samsvarer etter vår vurdering med GDPRs prinsipper og bidrar til å bevare et klart skille mellom teknologi, forvaltning og rettshåndhevelse.

4.2 Praktisk håndtering og etiske grenser

Slik vi forstår forslaget, vil eventuelle pålegg i praksis måtte håndteres innenfor det ansvarsområdet hver tjenestetilbyder dekker. For en infrastrukturleverandør som WAYSCloud er handlingsrommet begrenset til tiltak som:

– stenging eller midlertidig isolering av konto, node eller lagringsenhet, og

– bevaring av data slik de foreligger («as is») i tråd med pålegg fra myndighetene.

Vi har derimot verken teknisk forutsetning, juridisk hjemmel eller etisk mandat til å undersøke eller tolke innholdet i kundedata. Å analysere eller klassifisere innhold vil være å opptre som etterforskningsmyndighet – noe vi som nøytral tilbyder verken kan eller bør gjøre.

I praksis innebærer det at vi kan etterkomme pålegg om nedstenging og sikring, men ikke gå aktivt inn i kundedata. Etter vår oppfatning er dette den eneste modellen som ivaretar rettssikkerhet, personvern og tillit mellom leverandør og kunde.

5 Konkurransemessige og geopolitiske betraktninger

Europa står i en tid med økende geopolitisk uro og et forsterket behov for digital selvstendighet. Tillit til datasikkerhet og personvern er i dag en strategisk ressurs – på linje med energi og forsvar.

Kryptering er ikke et hinder for sikkerhet, men en forutsetning for trygg digital kommunikasjon, næringsliv, bank, helse og offentlig forvaltning. Den beskytter samfunnets kritiske data mot misbruk og utgjør grunnlaget for at både borgere, virksomheter og myndigheter kan bruke digitale tjenester med tillit.

Dersom EU pålegger egne leverandører tekniske bakdører eller skanningsplikt, kan dette gi konkurranseulemper sammenlignet med aktører i tredjeland som viderefører sterk kryptering og null-innsyn-arkitektur. Konsekvensen kan bli at data, kunder og investeringer flyttes ut av EØS, noe som i realiteten svekker både verdiskaping, innovasjon og cybersikkerhet.

Et regelverk som undergraver kryptering vil derfor ikke bare ramme enkeltleverandører – det kan på sikt svekke Europas digitale motstandskraft i møte med både statlige og kriminelle trusler.

6 Rettssikkerhet og EØS-forhold

Forslaget omfatter generalisert innholdsskanning, noe som etter vår forståelse utfordrer Grunnloven § 102 og EMK artikkel 8 om retten til privatliv og fortrolig kommunikasjon. Grunnloven § 113 understreker at inngrep i borgeres eller virksomheters råderett krever klar lovhjemmel og forholdsmessighet.

Vi noterer oss at Tyskland nylig har varslet at landet ikke vil støtte forordningen i sin nåværende form. Dette endrer dynamikken i EU-forhandlingene og viser at bekymringene om rettssikkerhet og forholdsmessighet deles av flere medlemsstater.

Selv om prosessen nå er usikker, står våre faglige vurderinger fast: Norge bør uansett legge til grunn en teknisk og etisk forsvarlig linje som ivaretar både personvern, sikkerhet og næringslivets behov for forutsigbarhet.

7 Et balansert alternativ

WAYSCloud støtter arbeidet mot ulovlig innhold, men ønsker å understreke viktigheten av at tiltak ikke svekker kryptering eller rettssikkerhet. Vi mener det bør vurderes en modell basert på følgende prinsipper:

1. Målrettet hashing av bilder, video og lenker mot offentlig eid og reviderbar database, begrenset til offentlig tilgjengelig innhold – ikke privat eller kryptert datalagring.
2. Myndighetsdriftet matching-infrastruktur, der EU-senteret eller nasjonal enhet håndterer matchingen. Dette sikrer at nøytrale infrastrukturtilbydere ikke må implementere innsyns- eller overvåkingsmekanismer, mens applikasjonstilbydere kan pålegges forholdsmessige tiltak nær brukeren.
3. Uavhengig revisjon, transparens og klageadgang, inkludert forbud mot krav om forhåndsskanning av ende-til-ende-kryptert kommunikasjon.

waysCloud.no no@waysCloud.net 22 25 80 00 Universitetsgata 2 0164 OSLO 833 735 462 MVA

4. Klart definert «umulighets-unntak», slik at pålegg som ikke kan gjennomføres uten å bryte sikkerhets- eller personvernprinsipper, kan modifiseres eller frafalles etter dokumentert prosess.

Etter vår oppfatning kan en slik tilnærming ivareta både barns sikkerhet og samfunnets behov for tillit til digital infrastruktur.

8 Avslutning

WAYSCloud AS ønsker med dette innspillet å uttrykke bekymring for de tekniske, rettslige og næringsmessige konsekvensene forordningen kan få dersom den innføres uten nasjonale tilpasninger.

Vi mener det er avgjørende at arbeidet mot ulovlig innhold skjer på en måte som ikke svekker kryptering, rettssikkerhet eller innovasjon. Regelverket må følge den teknologiske utviklingen – ikke henge etter den.

Et trygt digitalt Europa bygges best gjennom samarbeid mellom myndigheter, næringsliv og samfunn, der personvern, sikkerhet og etisk teknologiutvikling går hånd i hånd.

Med hilsen,

Knut Michael Haugland
Daglig leder, WAYSCloud AS