Kryptovault AS
Professor Olav Hanssens vei 7A
4021 STAVANGER
NORWAY

Kommunal- og distriktsdepartementet
Postboks 8112 Dep
0032 Oslo

Stavanger, 09 September 2022

HØRINGSSVAR – TILLEGGSHØRING OM DATASENTERREGULERING

1 INNLEDNING

Høringssvar fra Kryptovault AS, Arcane Green Data AS (Arcane Crypto AB), Stokmarknes Datasenter AS (Handelsbygg Holding AS) og Norsk Data AS (Oslofjord Datasenter AS), som gjelder Tilleggshøring om datasenterregulering til forslag til ny lov om elektronisk kommunikasjon (ekomloven) og ny forskrift om elektroniske kommunikasjonsnett og -tjenester (ekomforskriften).

Høringsnotatet innledes med en beskrivelse av reguleringen av datasenternæringen i Norge i dag, og bemerkninger knyttet til viktigheten av en robust digital infrastruktur. Det er åpenbart at noen datasenter spiller en viktig rolle i mange samfunnsviktige- og samfunnskritiske tjenester. Det er ikke urimelig å oppfatte en samfunnsmessig sårbarhet dersom datasentrene ikke har adekvat sikkerhet. Vi oppfatter at høringsnotatet omhandler endringer i ekomloven og ekomforskriften som et tiltak mot en slik aktuell og eller potensiell sårbarhet. Primært legges det til rette for mer omfattende plikter og krav ved drift av visse datasentre. Disse datasentrene innplasserer servere for mobiltjenester, betalingstjenester, helse- og velferdstjenester og mye annet. Vi deler derfor oppfatningen av at det eksisterer et behov for en nærmere regulering av datasentre som bærer samfunnsviktige oppgaver, og vi støtter at det stilles krav til sertifisering og tilsyn å sikre befolkningens adgang til samfunnsviktige- og samfunnskritiske tjenester.

Datasenternæringen er i dag preget av stort mangfold; mange datasentre bærer som nevnt samfunnskritiske oppgaver og systemer, men andre har aktivitet og funksjoner som ikke er av slik karakter. Dette gjelder blant annet skylagringstjenester, drift av serverer for streaming og spill og servere som deltar i blokkjeder, hvor desentraliseringen gjør at ingen enkelt-datasentre er kritiske for tjenestene.

Datasenter er også forskjellige med tanke på eierskap og verdikjede. Av og til eier sluttbruker (gjerne indirekte via konsern) datasenteret, utstyret og serverne. Andre ganger eier sluttkunden servere mens innplassering og infrastruktur kjøpes som en tjeneste av datasenteroperatøren. En annen variant er at datasenteroperatøren også eier serverne og leier ut servere til sluttkunder. Det kan også være tredjeparter som eier serverne.

Verdikjedevariantene må etter vårt syn gjenspeiles i de reguleringer og sikkerhetskrav departementet ønsker å innføre.

I forslaget sidestilles dette med infrastruktur for elektronisk kommunikasjon som følge av at den økende sammensmeltingen av tradisjonell elektronisk kommunikasjon og IT- sky- og datasentertjenester, hvor tredjepartsleverandører blir tettere integrert i ekomtilbydernes løsninger. Ekomlovens formål er å sikre brukerne i hele landet gode, rimelige, og fremtidsrettede elektroniske kommunikasjonstjenester, men også å legge til rette for effektiv bruk av ressurser og bærekraftig konkurranse. Reglene bør balansere disse to formålene.

Vi støtter formålene, men har en rekke kommentarer til forslagsdetaljer.

2 DATASENTER REGULERING

2.1 Om høringsnotatets punkt 5.2: ny bestemmelse om terskelverdi for datasenteroperatør

Departementet har særskilt bedt om kommentar til forslaget om at registreringsplikten skal inntre når man opererer datasentre over terskelverdien på 1 MW allokert kapasitet («**1 MW Terskelen**»). Terskelen er utformet slik at den reiser like mange spørsmål som det svarer.

Definisjonen av «*datasentertjeneste*» i forslagets § 1-5 omfatter langt mer enn bare drift av datasenter. Formodentlig er minimum at datasenteroperatøren tilbyr innplassering og tilgang til infrastruktur, men dette er ikke klart. Dette kompliseres ytterligere ved at verdikjeden kan være sammensatt. Noen aktører har egne datasenter, mens andre har et sammensatt grensesnitt mellom leverandør og kunde. Ordlyden er også utydelig i forbindelse med om det kreves at tjenester må leveres til en uavhengig part, eller om organisasjoner som opererer egne datasenter vil være omfattet.

Det er videre uklart om man i vurderingen av om registreringsplikten utløses, skal se på alle datasenter som datasenteroperatøren yter «datasentertjenester» fra under ett, eller om det er sentre som enkeltvis har fått allokert slik effekt som utløser kravet. Det synes noe tilfeldig hvem som blir registreringspliktig i begge tolkningsalterantiverer. Videre kan co-location datasenter trekke betydelig strømeffekt, men fordele til svært mange kunder.

Formålet med å stille krav og pålegge forpliktelser er knyttet til samfunnets behov for robuste samfunnsviktige- og samfunnskritiske tjenester. Det eksisterer datasentre som har tilgang til svært mye kraft uten at leveranser er samfunnsviktige eller samfunnskritiske av den grunn, slik som beregningstjenester (HPC), drift av serverer for streaming av video og spill og prosesseringstjenester for distribuerte systemer som blokk-kjeder.

Motsatt finnes også datasentre som driver med samfunnskritiske tjenester, men som ikke har et stort kraftforbruk. Disse faller utenfor registreringsplikten. Dette gjelder blant annet datasentre som tilbyr lagringstjenester hvor servere kobles fra nettet. 1 MW Terskelen vil ikke si noe om hvilken aktivitet som skjer på datasentrene.

Etter vårt syn vil det være mer hensiktsmessig at klienter av datasentre bærer ansvaret for hvilke sikkerhetskrav som er nødvendige i forbindelse med den aktivitet som skal knyttes til datasenteret. Det finnes allerede et internasjonalt anerkjent klassifiseringsregime som en slik løsning harmonerer med. En frivillig sertifiseringsordning, hvor datasenteret selv kan velge å registrere seg og dokumentere omfattende sikkerhetstiltak, vil være en mer effektiv måte å oppnå formålet bak forslaget fra departementet.

Et alternativ er at registreringsplikten og sikkerhetskravene blir gjeldende for datasentre som har kunder som tilbyr eller drifter samfunnskritiske tjenester. Det vil imidlertid ikke være enkelt. Ofte vet ikke datasenteret fullt ut kundens prosesser og skal heller ikke vite det. Andre ganger har kunden ivaretatt sikkerheten på annet vis, for eksempel ved redundans.

2.2 Rapporteringsplikt og andre plikter

Høringsnotatet omtaler vesentlige plikter for datasenteroperatørene. Dette notatet vil ikke kommenterer på dem enkeltvis, men for eksempel plikten til å løpende rapportere om kunder og melde endringer framstår som svært uegnet for mange datasenteroperatører. Kundemassen kan endres kjapt. Visse kunder framleier kapasiteten og for visse oppsett har ikke datasenteroperatøren kjennskap til hvem som er kunden. Tvert imot kan slik informasjon være beskyttet av lovpålagt (helse, forsvar med videre) eller avtalebasert taushetsplikt. Det er ofte ikke ønskelig med en generell rapportering av hvilke kunder som bruker hvilke datasenter fra kundens perspektiv. Informasjon til offentlige myndigheter er generelt offentlig etter offentlighetsloven, slik at mange kunder kan oppleve denne plikten som negativ i valget mellom norske datasenter og utenlandske datasenter.

En sluttkunde som yter samfunnsviktige- og samfunnskritiske tjenester i Norge står selvsagt i en annen stilling og må tåle offentlig innsyn. Disse kundene har imidlertid allerede omfattende plikter etter annet regelverk og velger gjennomgående datasenter med svært høyt fokus på sikkerhet og gjerne «Tier 4» eller høyere sertifisering. Et eksempel er Green Mountain, sml. Norske datasenter - bærekraftige, digitale kraftsenter fra august 2021: https://www.regjeringen.no/no/dokumenter/norske-datasenter/id2867155/.

2.3 Om kostnader

Departementet foreslår i høringsnotatet en ny § 3-13 tredje ledd som innebærer en plikt for datasenteroperatører til å sørge for systematisk oppfølging av sikkerhetstiltak og beredskap. Det foreslås også en plikt til å dokumentere sikkerhetstiltak og beredskapsnivå.

Departementet legger til grunn at disse nye kravene ikke vil føre til kostnader av betydning for datasentrene, men påpeker at for de datasentre der det er avvik mellom kravene som stilles og sikkerhetsnivået i dag vil det påløpe kostnader. For disse tilfellende legger departementet til grunn at den ekstra sikkerheten som kravene i så fall vil medføre, vil oppveie eventuelle kostnader.

Selv om noen datasentre allerede har omfattende sikkerhetsrutiner, vil det for flere aktører bety en økt kostnad å oppdatere disse slik at de tilfredsstiller kravene departementet nå foreslår, uten at behovet egentlig er til stede. Datasentrene kan få behov for økt personell for løpende å følge kravene om internkontroll og rapportering til offentlige myndigheter. Uten et behov som følge av kundenes bruk, vil kostnadene vanskelig la seg overføre til kundene i form av økte rater. Rett nok vil like datasenter i Norge ha like rammevilkår, men kundene kan ofte velge andre land som base og terskelen (jf punkt 2.1) kan vel lede til konkurranse om de samme kundene mellom datasenteroperatører som har forskjellige offentlig rettslige krav.

3 DATASENTER MED UTVINNING AV KRYPTO

3.1 Generelt

Utvinning av kryptovaluta er en betegnelse på prosesser der spesialbygde eller ordinære datamaskiner leverer tjenester som prosessering, verifisering og sikring, til et (blokkjede)nettverk og mottar virtuell valuta som motytelse («mining»). Den virtuelle valutaen som mottas stammer typisk fra en kombinasjon av transaksjonsavgifter og nyustedte enheter. Med andre ord hverken skaper man eller finner virtuell valuta når man miner, man får det tildelt som kompensasjon for å levere tjenester som er nødvendige for at nettverket skal fungere.

Den eksakte mekanismen varier fra nettverk til nettverk og det finnes etter hvert mange varianter av mining. Mining er derfor ikke en presist definert aktivitet med klare avgrensninger. Prosessen kan kreve store mengder energi og kapasitet for såkalte Proof of Work-baserte nettverk som Bitcoin.

Vi har etter hvert sett flere datasentre i Norge som har spesialisert seg på å yte tjenester til mining. Disse har flere særpreg. For det første har datasenteret typisk ikke direkte håndtering av selve valutaene som tjenes ved mining. Datakraften leies ut til en tredjepart. Tredjeparten velger formen for mining og betaler et vederlag i ordinær valuta til den norske datasenteroperatøren. For det andre, er maskinvaren ofte robust i seg selv slik at senterne kan være container basert eller annet. Tredje og sist, det godtas større avvik / nedetid mot lavere kost.

Man skal likevel være forsiktig med å generalisere. Mining kommer i flere former. Overskuddskapasitet i datasenter tiltenkte helt andre oppgaver nyttes i mange tilfeller undertiden til mining eller annen blokkkjedeverifikasjon.

Utvinning av kryptovaluta er ikke en samfunnskritisk tjeneste. Forslaget trekker frem at datasenter som utvinner krypto forvalter verdier som er attraktive for kriminelle aktører, og derfor bør underlegges samme sikkerhetsregulering som datasentre med samfunnskritisk aktivitet. Videre skal det kommunikasjonsvernet som ekomloven skal ivareta, sikre konfidensialitet, autensitet og integritet i innholdet av elektronisk kommunikasjon. Forutsetningsvis følger det dermed at datasentrene oppbevarer, deler eller på annen måte forvalter kommunikasjon som krever slik konfidensialitet. Dette hensynet vil etter vårt syn ikke gjelde for datasentre tilpasset mining. Slike datasentre oppbevarer ingen informasjon av verdi. Serverne som brukes til mining kan være utsatt for interesse fra kriminelle aktører, men tyveri av slikt vil kreve teknisk kunnskap og evne til å flytte stor vekt. Datasenter og kunder kan avtale sikkerhetstiltak som involverer fysisk sperring og adgangskontroll, tilpasset verdi og risiko. Dette har vært løsningen til nå. Vi kjenner ikke til at dette har vært problematisk.

Departementet trekker i høringsnotatet til forslag til ny lov om elektronisk kommunikasjon (ekomloven) som skal erstatte gjeldende lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) at de verdiene og funksjonene som ekomnett og -tjenester leverer, er en helt sentral forutsetning for at andre samfunnsfunksjoner skal kunne levere det de skal. Dette er etter vårt syn upresist for datasentre, ettersom datasentre kan drive aktivitet som ikke er en forutsetning for andre samfunnsfunksjoner. Nede-tid i datasenter som utvinner krypto vil ikke føre til konsekvenser for andre samfunnsfunksjoner.

3.2 Anslag over kraftproduksjon som skal anvendes til kryptovaluta.

Det foreslås å innføre en registreringsplikt for datasenteroperatørene. Felles for flere minsteopplysningene som kreves er at de er svært dynamiske og raskt skiftende. Dette gjelder særlig beskrivelse av tjenestene som skal tilbys, liste over kunder hos datasentrene og anslag på prosentvis andel av kraftforbruket som skal anvendes til utvinning av kryptovaluta.

Som nevnt er det vanskelig å anslå dette. Datasenteroperatøren vil ikke alltid vite hva serverne brukes til eller om aktiviteten kan klassifiseres som mining. Det kan tenkes at sluttkunden benytter «ledig tid» på serverne til mining

Flere datasentre leier ut maskinkraft til andre tredjeparter eller innplasserer tredjeparters servere som igjen leies ut til tredjeparter. Det vil derfor være utfordrende å holde en registrering oppdatert. Summen av faktiske forhold og begrepsuklarthetene, samt en dynamisk og ung bransje i utvikling, tyder på at store utfordringer ved operasjonalisere og etterleve denne plikten på en hensiktsmessig måte.

Foruten at det vil være utfordrende å holde det innregistrerte oppdatert, er det også uklart hvordan dette vil stille seg i lys av endringene foreslått i § 15-12 og § 15-13 om overtredelsesgebyr og straff.

Både § 15-12 og § 15-13 hjemler henholdsvis overtredelsesgebyr og straff for så vel forsettlig som uaktsom overtredelse av § 3-13. Departementet skriver i høringsnotatet at det på dette punktet bes om et anslag, nettopp fordi kraftforbruket vil kunne være kraftig skiftende og visse datasenteroperatører i tillegg vil måtte estimere hva kundene bruker serverne til. Dette bør gjenspeile og hensyntas gjennom at terskelen for å ilegge overtredelsesgebyr og straff ved feilregistrering heves.

Vår vurdering er at uaktsomhet synes for hardt for pliktsubjektene og at kravet til subjektiv skyld bør settes slik at kun forsettlig overtredelse rammes.

4 OPPSUMMERING

4.1 Hvilke plikter bør pålegges

Vi støtter en nærmere regulering av datasenternæringen, men bemerker at unødig byrdefulle krav til norske datasenter vil svekke konkurranseevnen vis-a-vis konkurrenter globalt og regionalt. *Norske datasenter - bærekraftige, digitale kraftsenter* la til grunn at Norge hadde et konkurransefortrinn i form av tilgang til rimelig strøm. Det fortrinnet gjelder i dag kun visse deler av landet. Vi ber derfor om at myndighetene i arbeidet videre tar sikte på å finne en god balanse mellom nytteverdi for samfunnet og kostnader for næringen. Høringsnotatet legger til grunn at kostnadene forventes å være begrensede, uten at dette er kvantifisert. Fra vårt ståsted påpekes det at datasenterdrift ikke nødvendigvis gir høye marginger. I tillegg har operatøren ofte langsiktig leiekontrakter og en viss risiko for markedsstyrte kostnader som strøm og finansiering av utstyr.

4.2 Hvem skal reguleres

Vi mener at en kvantitativ grense på 1 MW allokert kapasitet ikke passer med formålet og vil være lite treffsikkert. Det vil være mer hensiktsmessig å skille mellom typer av datasentre basert på tjenestene som kundene til datasentrene yter. Dersom et datasenter har kunder som yter samfunnskritiske tjenester kan det være hensiktsmessig å innføre økte krav til registrering og sikkerhet. Motsatt bør det *ikke* innføres krav på det nivået departementet nå foreslår om et datasenter *ikke* har slike kunder.

Ved en slik terskel skilles det ikke mellom aktivitetene de ulike datasentrene driver med, selv om enkelte datasenter kan ha aktivitet som ikke innebærer en sikkerhetsrisiko og motsatt. Dette er etter vårt syn uheldig. Formålet med de foreslåtte endringene er å legge til rette for en ytterligere styrking av sikkerheten i elektroniske kommunikasjonsnett- og tjenester som følge av at samfunnsutviklingen fordrer økt sikkerhet og beredskap mot nede-tid og trusler.

Det bør i større grad legges vekt på at ekomloven skal stimulere til næringsutvikling og innovasjon. En for streng regulering vil kunne føre til aktuelle at datasenteroperatører og klienter velger å ikke etablere seg i Norge. Dette vil både kunne svekke den nasjonale digitale sikkerheten og undergrave mål knyttet til næringsutvikling og innovasjon.

I høringsnotatet til forslag til ny lov om elektronisk kommunikasjon (ekomloven) som skal erstatte gjeldende lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) legger Departementet opp til at det kan være behov for å treffe vedtak eller inngå avtaler med aktører som tilbyr datasentre som leverer kritiske tjenester, *dersom* det vurderes at det foreligger sårbarheter for sikkerhet i nett og tjenester ved levering av skyplattformer eller dedikert infrastruktur. Dette er i tråd med vårt syn; det fornuftige er å kreve at kunden som skal drive samfunnskritisk aktivitet ved datasenter, selv har ansvar for å velge eller inngå avtaler med datasentre som tilbyr tilstrekkelig sikkerhet. Markedet

vil på denne måten i seg selv sørge for gode rutiner i forhold til sikkerhetsarbeidet. En hjemmel for visse datasenteroperatører til å be om politiattest for visse ansatte ansees imidlertid som positivt.

Hvis man likevel ønsker å sette krav til også datasenteroperatøren, bør det heller defineres hvilke digitale tjenester som er samfunnskritiske eller av spesiell viktighet av andre grunner. Her vil vi tro eksisterende lovkrav allerede setter krav til kunden. For datasenteroperatører som har kunder som yter slike listeførte tjenester kan kravene til registrering, sikkerhet og beredskap gjøres gjeldende.

4.3 Krypto

Vi oppfatter den foreslåtte plikten til å innrapportere anslått strømforbruk som vanskelig å etterleve og ganske urelatert til de hensyn som Ekomloven skal ivareta.

Signaturside

Kryptovault AS

Kjetil Hove Pettersen
CEO

Arcane Green Data AS

Torbjørn Bull Jensen
CEO

Handelsbygg Holding AS

Tore Arntzen
CEO