NORTHERN DATA NOR AS| C/O NÆRINGSPARK, B200 | HEDDALSVEGEN 9 | 3674 NOTODDEN

Notodden, 9. september 2022

Northern Datas uttalelse om tilleggshøring om datasenterregulering til forslag til ny lov om elektronisk kommunikasjon (ekomloven) og ny forskrift om elektronisk kommunikasjonsnett og -tjenester (ekomforskriften)

Til den det måtte gjelde,

Vi er bedt om å komme med innspill til forslagene til endringer i ekomloven og ekomforordningen.

I. I følge høringsnotatet er det foreslåtte lovforslaget ment å oppnå:

a) Få oversikt over datasentre i markedet, inkludert datasentre som henter ut krypto og av kunder som kan være kritiske for samfunnet

b) Stille krav til sikkerhet og beredskap for datasentre, bl.a. pga datasenterets økende integrasjon i den elektroniske kommunikasjonsinfrastrukturen; viktige samfunnsfunksjoner er avhengige av tjenester levert av datasentre og er avgjørende for lagring av data og drift av digitale tjenester, både for privat og offentlig sektor

c) Forebygging av cyberangrep

d) Regulering av datasentre som trekker ut krypto, fordi de forvalter eiendeler attraktive for kriminelle aktører og tilgang til kraftressurser

e) Beskyttelse av tilgjengelighet, integritet, autentisitet og konfidensialitet til datasentre og tjenester

f) Begrensning av interne risikofaktorer (ansatte)

II. Tiltakene for å nå disse målene er bl.a.

a) Nasjonal kommunikasjonsmyndighet (Nkom) som tilsynsmyndighet (finansiert av de regulerte fagene)

b) Registrering av datasenteroperatører, herunder små distribuerte datasentre, inkl lister over enkelte kunder

c) Politiet skal ha tilgang til registreringen for sitt arbeid med kriminalitetsforebygging knyttet til databehandling

d) Ingen differensiering mellom kryptogruvedrift og samlokalisering

e) Angivelse av prosentandel av strømforbruket som skal brukes til kryptogruvedrift

ADRESSE:
Northern Data NOR AS
c/o Næringspark, B200
Heddalsvegen 9
3674 Notodden
Norge

TA KONTAKT MED:
T: +49 69 348 752 25
E-post: info@northerndata.de
Hjemmeside: www.northerndata.de

REGISTRERE:
Registerretten:
Brønnøysundregistrene
Handelsregister: 925207950
mva.: 925 207 950 MVA

BANKINFORMASJON:
IBAN: DE97 5105 0015 0645 0682 14
BIC: NASSDE55XXX
Nassauische Sparkasse

ADMINISTRERENDE DIREKTØR
Monica Larsen
Stefan Sickenberger
Alexander Neumann

f) Datasentre skal få mulighet til å innhente politiattest f.eks. for ansatte og andre personer som har tilgang til datasenteret (f.eks. entreprenører).

g) Risiko- og sårbarhetsanalyser, plikt til å yte grunnleggende sikkerhetsnivå på tjenesten og særskilte krav til sikkerhet i informasjons- og styringssystemer, systematisk overvåking av sikkerhet og beredskap og dens dokumentasjon, beredskapsplanlegging og øvelser, sikkerhetsrevisjon av eksternt revisjonsselskap for operatørens regning.

h) Operatørens plikt til å opprettholde høyest mulig tilgjengelighet, selv ved force majeure hendelser

i) Sanksjoner for brudd

j) Tiltak for å sikre nasjonal sikkerhet, beredskap og funksjonalitetskrav / opprettholde nasjonal autonomi (drift og vedlikehold av personell og tekniske løsninger lokalisert på norsk territorium)

k) Myndigheten skal varsles om vesentlige sikkerhetsbrudd

l) Myndighet kan i konkrete tilfeller kreve at operatør prioriterer viktige samfunnsaktører ved valg av driftssted for å ivareta allmenne interesser.

III. Svar i detalj

1. P. 4 i høringsnotatet lyder: **«Det er viktig å sikre den digitale grunnlinjen. For e-infrastruktur og tjenester er det allerede satt krav av ekom- og sikkerhetslovene. Tilsvarende krav bør også stilles til datasentre i Norge, i første omgang ved å gjøre ekomlovens sikkerhetsbestemmelser gjeldende også for datasentre, slik at det kreves «tilstrekkelig sikkerhet».**

   Til tross for intensjonen om å etablere en digital grunnlinje, omfatter forslaget alle typer datasentre, uten å ta hensyn til betydningen av tjenestene som tilbys.

   Det er imidlertid klart fra høringsnotatet at de foreslåtte endringene ikke tar sikte på et hvilket som helst datasenter, men kun mot de som leverer kritiske tjenester: **«I et digitalisert samfunn som vårt er ekomnett og datasentre hjørnesteinen i vår nasjonale digitale infrastruktur. […]** ***Forsvarsrelatert sikkerhet i komplekse digitale verdener er derfor et prioritert tema, både i Norge og i EU og over hele verden» (se*** s.3 i høringsnotatet).

   Selv om intensjonen er riktig, ser forslaget bort fra at ikke alle digitale tjenester er relevante eller til og med samfunnskritiske. Forslaget ser ut til å være basert på misoppfatningen om at hvert datasenter er en del av kritisk infrastruktur. Det er ikke tilfelle. Flertallet av datasentertjenester er ikke knyttet til styring av strømnett, sykehus, navigasjon, kommunikasjonstjenester eller lignende viktige eller kritiske tjenester, men til spill, videogjengivelse, nettstedshosting og underholdning. Sistnevnte er ikke hjørnesteiner i digital infrastruktur i Norge og bør derfor unntas fra den foreslåtte reguleringen. I stedet bør lovgiver klart bestemme hvilke e-tjenester den anser som vesentlige i den forstand som er angitt ovenfor og begrense reguleringen til disse. Lovgiver har allerede delvis erkjent nødvendigheten av en differensiert regulering ved å fjerne forsvarssektoren og politiet fra utkastets virkeområde.

2. P. 4/5 i høringsnotatet lyder: **«... det er mer hensiktsmessig å stille like sikkerhetskrav for alle datasentre enn å stille sikkerhetskrav som kun gjelder for noen datasentre, fordi skillet mellom de ulike aktivitetene som datasentre**

sentre driver med (co-location og kryptogruvedrift) kan være glidende. Dette gjelder særlig tilfelle fordi også enkelte c o - l o c a t i o n s e n t r e også har kunder som utvinner kryptovaluta.» Spesielt utvinning av kryptovaluta kvalifiserer ikke som materiale for digital infrastruktur (i den grad høringsnotatet antyder at kryptomineringsdatasentre er kilde eller mål for kriminelle aktiviteter, se avsnitt 4 nedenfor)

Enda viktigere, det er absolutt mulig å definere tjenester som bør dra nytte av et høyere nivå av sikkerhet og kontroll og begrense reguleringen til disse. Ikke-kritiske tjenester er selvregulert av markedet og deres kunder, slik høringsnotatet innrømmer: **«mange datasentre har allerede god sikkerhet fordi kundene krever det» (se** s. 3 i høringsnotatet). Bransjen har for lenge siden utviklet standarden for såkalte nivåer (med ulike nivåer av tekniske og sikkerhetsnivåer) og sertifiseringer, og hver kunde kan (og må, se følgende avsnitt) velge det nivået som passer best for sitt formål.

3. Nøkkeldelen av den foreslåtte reguleringene ser ut til å være spørsmålet om "tilstrekkelig sikkerhet" og krav til sikkerhetsstyring, risiko- og sårbarhetsanalyser, beredskapsplanlegging og øvelser som følger av dette.

Vi mener at disse kravene bør ivaretas bedre av kundene til det aktuelle datasenteret som kan vurdere sikkerhetsbehovene til dataene deres bedre enn operatøren eller til og med myndigheten. På grunn av tekniske og databeskyttelsesmessige årsaker kjenner operatøren i mange tilfeller ikke til den spesifikke karakteren av kundenes aktiviteter[1] og vil derfor knapt være i stand til å vurdere det tilstrekkelige sikkerhetsnivået.
I denne sammenheng anser vi også §1-9 annet ledd nr. 8 i forskriften, som pålegger operatøren å gi opplysninger om norske statlige, fylkeskommunale og kommunale myndigheter, organer og virksomheter som er kunder av datasenteret, rettet mot feil adressat.

Byrden må derfor legges på kunden: Kunder som trenger tjenester som er relevante for norsk nasjonal digital infrastruktur bør være tydelig identifisert og forskriftsmessig pålagt å kun bruke slike datasentre som gir tilstrekkelig sikkerhetsnivå.
Ikke-kritiske tjenester bør fortsatt være regulert av markedets/kundenes etterspørsel.

Kritiske tjenester (dvs. de tjenester som myndighetene/lovgivningen bestemmer som relevante for norsk nasjonal digital infrastruktur) bør være klart fastlagt, og kunder som trenger slike tjenester bør være forpliktet til å benytte datasentre som gir sikkerhetsnivå (ved å overholde den etablerte tekniske standarden, f.eks. ISO 27001 opp til C5-sertifisering). Dette vil også unngå feilaktig tolkning av "tilstrekkelig sikkerhet" til operatøren og myndigheten. Henvisning til teknisk standard(er)/sertifisering vil også fjerne nødvendigheten av en ad hoc sikkerhetsrevisjon (i henhold til §9-6 i forskriften) som risiko og sårbarhetstester, beredskapsplanlegging/øvelser, sikkerhetsplaner og vedlikehold av disse og generelt sikkerhetsnivå er en forutsetning for sertifisering.

[1] Selv om operatørene generelt begrenser bruken av tjenestene deres og forbyr all ulovlig bruk i deres Godkjente Bruk Policy, det er teknisk sett ikke mulig å overvåke overholdelse av slike krav

En annen bekymring ser ut til å være spørsmålet om tilgjengelighet. Uptime Institute har for lengst etablert en nivåklassifisering for datasentre som gir enhver kunde en objektiv oversikt over omfanget av tilgjengelighet levert av operatøren. Kunden kan da enkelt velge nivået av tilgjengelighet/redundans som kreves for det spesielle formålet til en tilstrekkelig kostnad. Siden både høyere sikkerhet og tilgjengelighet har en høyere kostnad, kan kundene derfor veie merverdien opp mot kostnadene forbundet med dette.

Å kreve at alle datasentre skal gi samme nivå av sikkerhet og tilgjengelighet selv for kunder som ikke trenger det og ikke er villige til å betale for dem, vil medføre unødvendige kostnader som vil gjøre Norge lite attraktivt for datasenteroperatører.

Utkastet ser også bort fra det faktum at ved å regulere datasenteroperatører dekkes ikke spørsmålet om sikkerhet og tilgjengelighet for digitale tjenester fullt ut. En datasenteroperatør kan bare til en viss grad sørge for fysisk sikkerhet av maskinvare og forhindre sikkerhetsbrudd gjennom eget utstyr. Den har liten eller ingen kontroll over kundens maskinvare som er samlokalisert i datasenteret, og heller ikke over noe virtualiseringslag som maskinvaren kan være underlagt (f.eks. i tilfeller der en kunde har samlokalisert sin maskinvare i datasenteret, men bruker en tredjepart for å tilby skytjenester på grunnlag av slik maskinvare).

Selv om det kan være flere andre aktører, er utkastet unødig tyngende ved kun å regulere operatøren.

4. Den foreslåtte reguleringen vil **«gjelde for datasentre som henter ut krypto, fordi disse forvalter aktiva som er attraktive for kriminelle aktører, både i form av servere og annen infrastruktur, samt tilgang til kraftressurser».** Igjen, det ser ut til å være en misforståelse om karakteren av kryptominering. I den grad høringsnotatet refererer til nettangrep på det aktuelle datasenteret, vil disse bare kunne forstyrre driften av datasenteret, men ville gi svært liten, om noen, direkte fordel for angriperen. Slike angrep vil mer sannsynlig være rettet mot et gruvebasseng, gruvearbeiderens lommebok eller den relevante kryptobørsen hvor kryptovalutaer kan omdirigeres eller fanges opp i større mengder.

I tilfelle notatet refererer til kryptominering eller snarere kryptovalutaer som tilretteleggingsfaktorer for kriminelle aktiviteter, bør det bemerkes at (i) disse ikke administreres av operatøren, men kunden, gruvegruppen og/eller kryptobørsen og (ii) pga. blokkjeden spores transaksjoner i kryptovalutaer enkelt og offentlig. Der en blokkjedebruker ikke er identifiserbar, ligger en slik feil hos den relevante lommebok- eller utvekslingsleverandøren, ikke datasenteroperatøren.

5. På s.6 ber høringsnotatet om **«... høringsinstansenes syn på mulige muligheter for å omgå reguleringen ved for eksempel å etablere flere små datasentre under definert terskel.»** Her kommer en annen misoppfatning til syne – størrelsen er ikke den relevante faktoren når man skal vurdere et datasenters relevans for den nasjonale infrastrukturen. Datasentre kan distribueres, ofte på tvers av land eller kontinenter. Digital arbeidsmengde for ett datasenter kan omfordeles til et annet datasenter på brøkdeler av et sekund. I henhold til paragraf 2 vil det være mer hensiktsmessig å skille mellom gjenstanden for tjenesten i stedet for bare størrelsen på et datasenter.

6. P.5 i høringsnotatet lyder: **«Dersom det skulle stilles ulike sikkerhetskrav, vil dette også kunne føre til ulike konkurransevilkår. Dette er bakgrunnen for departementets forslag om at sikkerhetsforskriften skal gjelde for alle datasentre. Avdelingen ber likevel om høringsdeltakernes syn på om regelverket bør differensieres og eventuelt hvordan.»**

Det er vår oppfatning at forskriften slik den nå er utformet vil ha negativ innvirkning på datasentervirksomheten, konkurransevridning og oppnå det motsatte av det den var tiltenkt:

a) Å bruke de samme sikkerhetsstandardene på alle datasentre vil føre til samme kostnad (spesielt for sikkerhetstiltak, sikkerhetsrevisjon) uavhengig av størrelsen på inntektene til datasenteret. Dette vil uunngåelig være til skade for små datasentre og vil til slutt sette dem ut av drift.

b) Å anvende de samme sikkerhetsstandardene uten å ta hensyn til viktigheten/sensitiviteten til behandlede data vil føre til høyere kostnader selv for prosesser av lav betydning (f.eks. kryptominering, spilling) og vil gjøre slike prosesser dyrere og dermed mindre tilgjengelige. Det er rett og slett ikke nødvendig å **«sikre høyest mulig tilgjengelighet av datasentertjenester også i tilfelle force majeure-hendelser» (s.6** i høringsnotatet) for bare enhver databehandling. For hvorfor byrden bør legges på kunden og hvorfor objektive krav og sertifisering er nødvendig: se avsnitt 3.

c) Selv om vi setter pris på at utkastet krever at tiltak skal være forholdsmessige – et krav **«fra forvaltningsretten som også vil gjelde på dette området. […] Kostnader som langt overstiger tiltakets nytte eller tjenestens betydning må anses som uforholdsmessige.** «(s.7). Tilstrekkelighet av sikkerhetstiltak er imidlertid gjenstand for gransking av myndigheten (som kan vurdere vesentligheten av dataene som behandles ved det aktuelle datasenteret enda mindre enn operatøren (se punkt 3).

d) Slik overregulering vil skade Norges attraktivitet som datasenterplassering og føre til at den aktuelle virksomheten blir allokert andre steder. Dette vil spesielt gjelde datasentre med lav margin som tilbyr tjenester av lav betydning/sensitivitet. Det bør bemerkes at slike datasentre bidrar til stabiliteten i kraftbehovet og dermed strømnettet, ettersom de kan strømmes opp og ned i henhold til etterspørselen, og dermed bidra til å utjevne topper i etterspørselen og unngå nettforstyrrelser.

7. Registreringen i henhold til forskriftens nye §1-9 vil blant annet kreve beskrivelse av tjenestene som tilbys (pkt.nr. 7) og tildeling av prosentandel av strømforbruket som skal brukes til kryptovalutautvinning (pkt.nr. 9). Begge kravene er ikke gjennomførbare.

a) beskrivelse av tjenestene som tilbys: beskrivelsen vil enten være generisk og vil derfor ikke tilføre noen verdi (og vil særlig ikke gjøre det mulig for myndigheten å vurdere tilstrekkeligheten av tiltak) eller kreves i en detalj som operatøren ikke kan levere (se avsnitt 3). Selv om operatøren var i stand til nøyaktig å bestemme hvilke data som behandles i datasenteret av kundene, kan slike data endres når som helst og ofte gradvis. Registreringen ville være i konstant fare for å være feil.

b) tildeling av prosentandel av strømforbruket som skal brukes til utvinning av kryptovaluta:

Siden kryptominering bare er en annen form for databehandling, kan den endres når som helst (som paragraf a) ovenfor). I tillegg kan kunden, dersom maskinvaren tillater det, bytte mellom kryptominering og annen form for databehandling i løpet av sekunder – å allokere hvor mye strøm som forbrukes til kryptominering er derfor rett og slett ikke mulig.

IV. Konklusjon

1. Flertallet av datasentertjenestene er ikke relatert til viktige eller kritiske tjenester – utkastet vil pålegge et unødvendig nivå av sikkerhet/tilgjengelighet og dermed overdrevne kostnader
2. Lovgiver bør identifisere funksjoner som er viktige eller kritiske og definere hvilket nivå av sikkerhet/tilgjengelighet disse funksjonene krever
3. Kunder som trenger datasentertjenester for slike viktige eller kritiske funksjoner, bør være ansvarlig for å velge riktig nivå av sikkerhet/tilgjengelighet, ettersom kun en slik kunde er i stand til å vurdere og kontrollere arten av data som behandles
4. Bruk av samme sikkerhets-/tilgjengelighetsstandarder for alle datasentre vil vri konkurransen, sette mindre bedrifter og de som leverer ikke-kritiske tjenester i fare, påføre mange operatører unødvendige kostnader og ha negativ innvirkning på Norges attraktivitet for leverandører av digitale tjenester.

5. Utkastets krav om "tilstrekkelig sikkerhet" er vagt og unødvendig ettersom industrien allerede har etablert nivåklassifisering (for tilgjengelighet) og sertifisering (for sikkerhet). "Tilstrekkelighet" kan bare vurderes av kunden, ikke operatøren, enda mindre tilsynet
6. Registreringskravene er ikke gjennomførbare

Med vennlig hilsen,

Northern Data NOR AS
Monica Christine Larsen