Høringsnotat

Avdeling for digitaliseringspolitikk
Dato: 29. januar 2025
Saksnr: 24/2069-7
Høringsfrist: 28. mars 2025

Forslag til endringer i datasenterforskriften (nasjonal sikkerhet og kriminalitetsbekjempelse i datasentre)

Innhold

1 Hovedinnholdet i høringsnotatet

Digitaliserings- og forvaltningsdepartementet sender med dette på høring forslag til endringer i forskrift av 18. desember 2024 nr. 3313 om datasenter. Høringsnotatet er utformet i samarbeid med Justis- og beredskapsdepartementet. Omtalen som gjelder politiet og Nasjonal sikkerhetsmyndighet (NSM) med tilhørende regelverk, og omtalen av konstitusjonelle og menneskerettslige skranker for forslaget er basert på innspill fra Justis- og beredskapsdepartementet.

For å sikre myndighetenes mulighet til å kunne forebygge, avverge, stanse og etterforske kriminalitet og håndtere bortfall av datasentertjenester som er av betydning for samfunnet, vil departementet i dette høringsnotatet foreslå enkelte endringer i datasenterforskriften slik at justis- og ekommyndighetene får tilgang til nødvendig informasjon og bedre mulighet til å iverksette nødvendige tiltak.

Formålet med endringsforslagene er å legge til rette for kriminalitetsbekjempelse og ivaretakelse av nasjonal sikkerhet i datasentre. Samtidig skal næringens behov for hensiktsmessige og forutsigbare rammevilkår ivaretas. Datasentre er viktige for å sikre en robust nasjonal infrastruktur, og det er i samfunnets interesse at det stimuleres til utvikling og investeringer fra både norske og utenlandske aktører. Det vises i denne sammenhengen også til Stortingets behandling av lov av 13. desember 2024 nr. 76 om elektronisk kommunikasjon (ekomloven), jf. Innst. 28 L (2024–2025) side 8, hvor flertallet i Transport- og kommunikasjonskomiteen er positive til at det stilles krav til sikkerhet og transparens, men mener at kravene må være forholdsmessige og ubyråkratiske.

Forslagene til endringer i datasenterforskriften som foreslås i dette høringsnotatet, er kort oppsummert som følger:

For det første foreslås det å pålegge datasenteroperatører å ha oppdatert informasjon om egne kunders navn og kontaktopplysninger tilgjengelig og, der det er relevant, informasjon om hvor i senteret de ulike kundenes fysiske utstyr er plassert.

For det andre foreslås det regler om utlevering av denne informasjonen til henholdsvis Nasjonal kommunikasjonsmyndighet (Nkom), NSM, Politiets sikkerhetstjenesten (PST) og politi og påtalemyndighet for øvrig. Adgangen til å pålegge utlevering av kundeopplysninger skal blant annet styrke arbeidet med forebygging, avverging og stansing av lovbrudd med tilknytning til et datasenter, samt ivareta forebyggende sikkerhet, robusthet og hendelseshåndtering.

Datasenteroperatører driver virksomhet som er helt nødvendig for alle sektorer i samfunnet. Samtidig kan infrastrukturen i datasentre misbrukes til kriminalitet og virksomhet som truer nasjonal sikkerhet. Derfor er det i likhet med banknæringen behov for en særskilt regulering av datasentre. Det vises i denne sammenhengen til flertallets uttalelser i Innst. 28 L (2024–2025) side 8:

> «F l e r t a l l e t viser til at et stadig større omfang av private og offentlige tjenester er digitale, de baseres på data og leveres via skyløsninger. Datasentrene som lagrer og prosesserer dataene, er dermed en helt sentral del av den digitale grunnmuren og den kritiske infrastrukturen i Norge. Sentrale funksjoner i det offentlige og private må sikres mot dataangrep, slik at man ivaretar kritiske samfunnsfunksjoner. I den digitale verdikjeden etablerer utenlandske og kommersielle aktører seg, og i et sikkerhetsperspektiv er det viktig å ivareta norske interesser. De siste årene har

> cyberangrep mot viktige institusjoner og bedrifter økt. Datasentre er kritisk infrastruktur, og kommunikasjonsstrukturen er en del av sikkerhetsutfordringen.»

På denne bakgrunnen er det særlig viktig at NSM, Nkom, PST og politiet og påtalemyndigheten for øvrig har tilstrekkelig informasjonstilgang når det oppstår hendelser med tilknytning til datasentre.

Det foreslås derfor at *politi og påtalemyndighet* skal gis adgang til å pålegge utlevering av opplysninger om én eller enkelte angitte kunders navn og kontaktinformasjon og, der det er relevant, opplysninger om plassering av kundens fysiske utstyr i senteret når og i det omfang det er nødvendig for å stanse eller avverge et lovbrudd.

Dersom politiet griper inn for å avverge eller stanse lovbrudd *utenfor etterforskning*, jf. politiloven § 7 første ledd nummer 3, har de etter gjeldende rett ikke hjemler til å pålegge utlevering av kundeinformasjon.

I etterforskning vil politiet og påtalemyndigheten etter gjeldende rett kunne bruke beslag eller utleveringspålegg for å få tilgang til kundeopplysninger forutsatt at vilkårene for disse tvangsmidlene er oppfylt. Begge tvangsmidler krever skjellig grunn til mistanke om en straffbar handling og at det som beslaglegges eller kreves utlevert, antas å ha betydning som bevis. Utleveringspålegg anses som det mest praktiske virkemiddelet for å få utlevert kundeinformasjon, og forutsetter, i motsetning til beslag, beslutning fra retten. Beslag og utleveringspålegg for *å avverge* et straffbart forhold kan imidlertid bare benyttes når det er rimelig grunn til å tro at noen kommer til å begå et begrenset antall svært alvorlige handlinger (terrorhandlinger, terrortrusler og drap, samt grove narkotikaovertredelser og grovt ran, forutsatt at de to sistnevnte lovbruddene utøves som ledd i aktivitetene til en organisert kriminell gruppe).

Forslaget til forskriftsendring om ny utleveringsbestemmelse til politi og påtalemyndighet er ment å gjelde både *i og utenfor etterforskning*. Forslaget vil dermed sikre at politiet også får en hjemmel til å pålegge utlevering av kundeopplysninger ved *hendelseshåndtering utenfor etterforskning*.

I etterforskning vil forslaget medføre at det oppstilles lempeligere vilkår enn i dag. For det første vil slike opplysninger kunne utleveres til avverging i flere tilfeller. Dette er viktig fordi kundeopplysninger i dag som nevnt bare kan kreves utlevert for å avverge et svært begrenset knippe alvorlige handlinger. For det andre oppstilles det også lempeligere vilkår ved stans av pågående handlinger i etterforskning, blant annet ved at man ikke trenger å gå veien om utleveringspålegg og beslutning fra retten. Slike lempeligere vilkår vil sikre at politiet har lik informasjonstilgang i og utenfor etterforskning ved håndtering av akutte hendelser. Vilkårene vil også sikre at tiltakene kan iverksettes raskt og hjemmelen vil kunne være ressursbesparende for aktørene og domstolene. De lempeligere vilkårene må videre ses i sammenheng med hvilken informasjon det gis tilgang til, det vil si opplysninger om enkelte kunders navn, kontaktinformasjon og informasjon om plasseringen av kundens eventuelle fysiske utstyr.

Videre foreslås det at *PST* skal gis tilgang til kundeopplysninger i forebyggende øyemed. Kundeopplysninger kan være en forutsetning for at PST kan innhente ytterligere informasjon fra andre kilder for å vurdere om det bør settes i verk forebyggende tiltak. Etter dagens regler vil PST bare kunne innhente slike

opplysninger i forebyggende øyemed dersom vilkårene for skjult tvangsmiddelbruk etter politiloven er oppfylt. PST har behov for kundeinformasjon også for å forebygge andre straffbare handlinger enn de som kan begrunne skjult tvangsmiddelbruk. I tillegg kan sakene ha et betydelig hasteaspekt der tjenesten kan ha behov for rask tilgang til informasjonen. Det foreslås derfor at PST gis tilgang til kundeopplysninger når det er grunn til å undersøke om noen forbereder en handling som nevnt i politiloven § 17 b og det er grunn til å tro at informasjonen er av betydning for å forebygge handlingen.

NSM har i dag ikke hjemmel til å pålegge utlevering av kundeopplysninger, men har behov for slike opplysninger i sitt arbeid med å drive den nasjonale responsfunksjonen ved alvorlige digitale angrep og det nasjonale varslingssystemet for digital infrastruktur etter sikkerhetsloven § 2-4. Formålet med utleveringshjemmelen er at NSM skal kunne kartlegge omfanget av et cyberangrep og den risikoen angrepet utgjør for øvrige kunder i et datasenter.

Informasjon om datasenteroperatørens kunder vil også bidra til *Nkoms* arbeid med kartlegging av hvilke datasentre som har vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser, jf. sikkerhetslovens §§ 1-3 og 2-1, samt for øvrig bidra til at Nkom kan ivareta sine oppgaver etter sikkerhetsloven.

For det tredje foreslås det å presisere kravene til datasenteroperatørens fysiske representant i Norge. I ny datasenterforskrift, som trådte i kraft 1. januar 2025, er det allerede stilt krav om at datasenteroperatøren skal ha en representant som er fysisk tilgjengelig med fullmakt og kunnskap til å følge opp myndighetenes henvendelser, men etter departementets syn er det behov for å presisere kravene til representanten. Dette vil bidra til å sikre at alle aktører i datasenternæringen kan bistå myndighetene med gjennomføring av tiltak med hjemmel i gjeldende regelverk.

For det fjerde foreslås det å regulere hvor raskt datasenteroperatøren skal etterkomme pålegg om utlevering av kundeinformasjon og bistå Nkom, NSM, PST og politiet og påtalemyndigheten med gjennomføring av tiltak som har hjemmel i lov eller forskrift gitt i medhold av lov. Forslaget inneholder regler om responstid både innenfor og utenfor arbeidstid.

For det femte foreslås det at forsettlige eller uaktsomme overtredelser av plikten til å ha oppdatert kundeinformasjon tilgjengelig, plikten til å utlevere kundeinformasjonen, plikten til å ha en representant og plikten til å respondere innen en bestemt frist kan møtes med overtredelsesgebyr.

Endelig foreslås det at datasenteroperatører skal oppgi navn på eier av bygning der datasenteret er lokalisert når operatøren registrerer seg hos Nkom etter datasenterforskriften § 1-3.

Ny ekomlov § 3-7 femte ledd åpner som nevnt for regulering av datasentre for å ivareta samfunnsoppdraget til politiet og EOS-tjenestene, samt Nkom som har et sektoransvar for nasjonal sikkerhet i datasentre. Dette høringsnotatet tar særlig for seg regulering av informasjonstilgang for politiet og påtalemyndigheten, PST, NSM og Nkom og innebærer at datasenterforskriften vil bidra til å løse samfunnsoppdraget til disse etatene slik det fremgår av politiloven, straffeprosessloven og sikkerhetsloven. For enkelhets skyld benyttes «politiet» som en fellesbetegnelse for både politiet og PST. Det vil si at for de delene av

dokumentet som gjelder «politiet», er også PST inkludert. Dersom det derimot er særskilte regler som kun gjelder PST, vil betegnelsen «PST» benyttes.

2 Nærmere om bakgrunnen for forslagene

Ekomloven trådte i kraft 1. januar 2025. Loven inneholder den første reguleringen spesielt rettet mot datasenterbransjen i norsk rett. I medhold av ekomloven § 3-7 er det gitt en ny forskrift om datasenter, som trådte i kraft samtidig med loven.

Et datasenter er en infrastruktur som lagrer og bærer digitale tjenester og data. I et digitalisert samfunn er elektroniske kommunikasjonsnett og datasentre grunnmuren i vår nasjonale digitale infrastruktur, jf. Prop. 93 LS (2023–2024) side 198. Datasentre er kritisk infrastruktur for den stadig økende bruken av internett- og skybaserte tjenester i samfunnet. Mange kritiske tjenester leveres i dag fra datasentre, og avhengigheten til datasentrene kan utgjøre en stor samfunnsmessig sårbarhet. Noen eksempler på tjenester som datasentre bærer er mobiltjenester, som tale og data, betalingstjenester, helse- og velferdstjenester, kritiske kommunikasjonstjenester, TV- og radiodistribusjon (DAB), Forsvarets kommunikasjonstjenester og nød- og beredskapskommunikasjon. Datasentre er moderne industribygging og datasentre lokalisert i Norge legger til rette for at kritiske digitale tjenester kan produseres nasjonalt fremfor i utlandet, hvilket styrker den nasjonale kontrollen og sikrer muligheter for nasjonal autonomi. Norge er blitt et attraktivt land for etablering av datasentre, og datasenternæringen har vokst kraftig det siste tiåret. Departementet viser til at næringen spiller en viktig rolle for ivaretakelsen av norske interesser, og departementet er derfor opptatt av at kravene som stilles til datasenteroperatører skal være forholdsmessige og ivareta hensynet til gode markedsvilkår.

Datasenteroperatører driver virksomhet som er helt nødvendig for alle sektorer i samfunnet, både offentlige og private. Samtidig kan infrastrukturen i datasentre misbrukes til kriminalitet og virksomhet som truer nasjonal sikkerhet. Kripos har gjennom flere hendelser erfart evne og vilje hos datakriminelle og andre trusselaktører til å gjennomføre digital kriminalitet mot virksomheter, infrastruktur og tjenester knyttet til datasentre i Norge, og at datasentre i Norge benyttes til straffbare handlinger både i Norge og mot andre land. Den sikkerhetspolitiske utviklingen, økningen i digitale angrep og en hurtig digital transformasjon har også endret rammebetingelsene for arbeidet med nasjonal sikkerhet.

På denne bakgrunnen er det behov for en særskilt regulering av datasentre. Det må stilles krav til datasenteroperatørene, slik at myndighetene kan ivareta sine oppgaver knyttet til kriminalitetsbekjempelse og ivaretakelse av nasjonal sikkerhet. Kunnskap om hvem som er kunder i et datasenter, hvor i senteret kundene har sin virksomhet når de har fysisk utstyr plassert i senteret og rask tilgang til slik informasjon kan være avgjørende for at politiet og NSM skal kunne oppfylle sine samfunnsoppdrag, jf. uttalelsene i Prop. 93 LS (2023–2024) side 204.

Det er viktig at myndighetene kan komme i kontakt med datasenteroperatørene, at operatørene har en representant som er fysisk tilgjengelig når det er behov for det, at de kjenner sine kunder og at de kan gi informasjon om kundeforholdene når myndighetene har hjemmel til å innhente slik informasjon. I ny datasenterforskrift som trådte i kraft 1. januar 2025 er det allerede stilt krav om en representant for datasenteroperatøren som er fysisk tilgjengelig med fullmakt og kunnskap til å

følge opp myndighetenes henvendelser, men det er behov for å presisere kravene til denne.

Ekomloven § 3-7 femte ledd gir departementet adgang til å gi forskrift om ivaretakelse av hensynene til nasjonal sikkerhet og kriminalitetsbekjempelse i datasentre. Forskriftshjemmelen åpner blant annet for at det kan oppstilles krav om at datasenteroperatøren skal ha en tilgjengelig representant som har nødvendig kunnskap om senteret til å kunne bistå politiet eller EOS-tjenestene slik at den tilgangen disse skal ha til datasentre i eller i medhold av ekomloven eller annet regelverk, blir reell. Videre kan det gis krav om separasjon av kunder eller kundegrupper samt krav om at datasenteroperatøren skal føre oppdaterte lister over egne kunder og hvor deres fysiske utstyr er plassert i datasenteret. Etter samme bestemmelse gis departementet adgang til å oppstille krav om at politiet og EOS-tjenestene gis rask tilgang til informasjon fra kundelistene på nærmere vilkår. Det følger av Prop. 93 LS (2023–2024) side 204 og side 281 at vilkårene skal balansere hensynet til kriminalitetsbekjempelse og nasjonal sikkerhet og hensynet til hensiktsmessige rammevilkår for datasenternæringen.

Det følger som nevnt av § 3-7 femte ledd at departementet kan gi forskrift om nasjonal sikkerhet og kriminalitetsbekjempelse i datasenter. Dette innebærer at bestemmelsen også gir hjemmel til å forskriftsfeste at Nkom, som ansvarlig myndighet for nasjonal sikkerhet i datasenter, kan innhente kundeinformasjon for å oppfylle sitt sektoransvar etter sikkerhetsloven, jf. nærmere redegjørelse i punkt 9 nedenfor. Denne informasjonsinnhentingen kommer i tillegg til Nkoms hjemmel for informasjonsinnhenting etter ekomloven § 15-2.

Bruken av forskriftshjemler i ny ekomlov er kommentert flere steder i Innst. 28 L (2024–2025) om ny ekomlov. Komiteens flertall (medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Sosialistisk Venstreparti og Venstre), har på side 3 i innstillingen uttalt at departementet i det videre arbeidet skal etterstrebe en bred dialog og transparent prosess når forskrifter skal utformes og endres.

Et annet flertall bestående av medlemmene fra Arbeiderpartiet, Senterpartiet, Sosialistisk Venstreparti og Venstre uttaler på side 4 i innstillingen at bruken av forskriftshjemler er godt begrunnet, og at det er hensiktsmessig med en fleksibel regulering som raskt kan tilpasses den teknologiske utviklingen og økte krav til sikkerhet og beredskap.

Endelig viser et flertall bestående av medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti på side 4 til at de har merket seg høringsinnspill fra datasenteraktører om nye forskriftskrav knyttet til registrering av kunder og deres fysiske plassering i datasenteret, og uttaler at det må være praktisk gjennomførbart å etterleve slike krav, og at for eksempel logisk separasjon vil kunne være tilstrekkelig til å oppfylle plikten.

Samlet sett mener departementet at presiseringene i proposisjonen nevnt ovenfor, Stortingets behandling av forskriftshjemlene og den foreliggende høringen sikrer at det foreligger et tilstrekkelig grunnlag for forslaget til endringer i datasenterforskriften som fremsettes i dette høringsnotatet, herunder forslaget om hjemmel for pålegg om utlevering av kundeinformasjon.

Det har vært nedsatt en arbeidsgruppe bestående av Digitaliserings- og forvaltningsdepartementet og Justis- og beredskapsdepartementet, samt deltakere fra Nkom, Politidirektoratet (POD), Kripos, PST og NSM med mandat til å

utarbeide forslag til endringer i datasenterforskriften. Representanter fra datasenternæringen har også deltatt i enkelte arbeidsgruppemøter.

3 Konstitusjonelle og menneskerettslige skranker for forslaget

3.1 Legalitetsprinsippet og det strafferettslige lovkravet

Beslutninger som fattes av offentlige myndigheter, for eksempel pålegg overfor private om utlevering av informasjon, vil kunne gripe inn i privates rettssfære og berøre rettigheter som er vernet etter både Grunnloven og menneskerettslige konvensjoner. Ved utformingen av forskriftsreguleringen må staten holde seg innenfor de rettslige skrankene som følger av disse forpliktelsene.

I Grunnloven § 113 er det oppstilt et generelt krav om at «[m]yndighetens inngrep overfor den enkelte må ha grunnlag i lov».

Både Stortingets lovgivning og forskrift gitt med hjemmel i lov regnes som et tilstrekkelig formelt rettsgrunnlag etter bestemmelsen, jf. Dokument 16 (2011–2012) side 246–247. Lovkravet etter Grunnloven § 113 medfører også kvalitative krav til rettsgrunnlaget – det må være tilgjengelig og så presist som forholdene tillater, jf. HR-2020-1967-A avsnitt 35. I samme avgjørelse tilføyer førstvoterende at kravet til presisjon er relativt og avhenger av arten av inngrepet og hvor hardt det rammer, jf. avsnitt 36.

Reaksjoner som regnes som straff etter Den europeiske menneskerettighetskonvensjonen (EMK), slik som overtredelsesgebyr, må videre oppfylle de kravene til hjemmel som er nedfelt i artikkel 7 nr. 1 i konvensjonen, i tillegg til at prosessen må oppfylle kravene til en rettferdig rettergang etter EMK artikkel 6. Tilsvarende krav fremgår av FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 14 og 15 nr. 1. Konvensjonene er gjennomført i norsk rett ved lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven), jf. § 2 og går ved motstrid foran bestemmelser i annen lovgivning, jf. § 3.

EMK artikkel 7 nr. 1 fastsetter som nevnt at det må foreligge hjemmel for å ilegge straff. I tillegg må hjemmelen oppfylle visse kvalitative minstekrav. De kvalitative kravene omfatter både gjerningsbeskrivelsen og straffetrusselen, se *Del Río Prada mot Spania*, saksnr. 42750/09, 21. oktober 2013 avsnitt 91. Straffebestemmelsen må være tilgjengelig for allmennheten og så klart utformet at borgerne ut fra lovteksten – og om nødvendig med rettslig bistand eller rettsavklaringer fra domstolene – forstår hvilke handlinger og unnlatelser som kan møtes med straff, jf. *Cantoni mot Frankrike*, saksnr. 17862/91, 15. november 1996 avsnitt 29. For å oppfylle kravet til presisjon må lovteksten – eventuelt sett i sammenheng med andre rettskilder – gi rimelig veiledning om hva som er straffbart, jf. også uttalelsene i HR-2016-2228-A avsnitt 30.

3.2 Retten til respekt for privatliv og korrespondanse

3.2.1 Rettighetsvernets anvendelsesområde

Grunnloven § 102 første ledd første punktum verner blant annet om retten til respekt for privatliv, hjem og kommunikasjon. En rett til respekt for privatliv, hjem og korrespondanse følger også av EMK artikkel 8 og SP artikkel 17. Grunnloven § 102 ble tilføyd ved grunnlovsrevisjonen i 2014, og det er lagt til grunn i høyesterettspraksis at § 102 første ledd første punktum skal tolkes i lys av de nevnte konvensjonsbestemmelsene, jf. Rt. 2015 side 93 avsnitt 57. Departementet legger til grunn at innholdet i retten til respekt for privatliv og hjem i all hovedsak er sammenfallende etter Grunnloven § 102 første ledd første punktum og EMK artikkel 8, og at det heller ikke er holdepunkter for at vernet er mer omfattende etter SP artikkel 17. I det videre tas det derfor utgangspunkt i rettighetsvernet etter EMK artikkel 8.

Uttrykket «privatliv» i EMK artikkel 8 nummer 1 er autonomt og blir tolket vidt av Den europeiske menneskerettsdomstolen (EMD). Derfor kan det ikke oppstilles en klar eller uttømmende definisjon av uttrykket. Retten til respekt for privatliv inneholder blant annet et vern om personopplysninger, jf. *L.B. mot Ungarn*, saksnr. 36345/16, 9. mars 2023 avsnitt 103.

EMD tolker «privatliv» i lys av definisjonen av personopplysninger i Europarådskonvensjon nummer 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger, jf. for eksempel *Satakunnan Markkinapörssi Oy and Satamedia Oy mot Finland*, saksnr. 931/13, 27. juni 2017 avsnitt 133. I konvensjon nummer 108 artikkel 2 bokstav a heter det at «personopplysninger» omfatter informasjon om en identifisert eller identifiserbar enkeltperson. Det fremgår videre av den forklarende rapporten til endringsprotokollen at konvensjon nummer 108 er begrenset til behandling av opplysninger om fysiske personer, se side 6. På bakgrunn av dette legger departementet til grunn at personopplysningsvernet etter EMK artikkel 8 nummer 1 vil aktualiseres overfor de kundene til datasenteroperatøren som er fysiske personer.

Blant opplysningene som vil kunne angå privatlivet etter EMK artikkel 8 nummer 1, er en persons navn og adresse, jf. henholdsvis *L.B. mot Ungarn*, saksnr. 36345/16, 9. mars 2023 avsnitt 104 og *Alkaya mot Tyrkia*, saksnr. 42811/06, 9. oktober 2012 avsnitt 30. Fødselsnummer og telefonnummer er andre eksempler på opplysninger med tilknytning til privatlivet, jf. *Breyer mot Tyskland*, saksnr. 50001/12, 30. januar 2020 avsnitt 81 jf. avsnitt 27.

Behandling av personopplysninger vil kunne være et inngrep i retten til respekt for privatliv etter EMK artikkel 8 nummer 1. Domstolen har lagt til grunn at offentlige myndigheters lagring av personopplysninger som knytter seg til privatlivet etter konvensjonsbestemmelsen utgjør et inngrep i privatlivsvernet, jf. blant annet *Leander mot Sverige*, saksnr. 9248/81, 26. mars 1987 avsnitt 48 og *Amann mot Sveits*, saksnr. 27798/95, 16. februar 2000 avsnitt 65. Privates behandling av personopplysninger vil kunne være et inngrep dersom inngrepet kan tilskrives offentlige myndigheter, jf. *Vukota-Bojić mot Sveits*, saksnr. 61838/10, 18. oktober 2016 avsnitt 46–47. Myndighetenes krav om utlevering og etterfølgende bruk av opplysninger som angår privatlivet, vil også kunne være et inngrep, jf. blant annet *Benedik mot Slovenia*, saksnr. 62357/14, 24. april 2018 avsnitt 120.

EMK artikkel 8 nr. 1 gir også enhver rett til respekt for sin «korrespondanse». Konvensjonsbestemmelsen oppstiller et vern for konfidensialiteten til privat kommunikasjon, uavhengig av form og innhold, jf. *Klaus Müller mot Tyskland*, saksnr. 24173/18, 19. november 2020 avsnitt 38. Om innholdet i korrespondansebegrepet uttaler EMD følgende i samme avsnitt:

> «[…] what Article 8 protects is the confidentiality of all the exchanges in which individuals may engage for the purposes of communication […]»

Vernet er teknologinøytralt, og så vel fysiske som juridiske personer kan være rettighetssubjekter. Kjerneområdet for bestemmelsen synes å være den direkte dialogen mellom én eller flere avsendere og mottakere. I avgjørelser om advokatkorrespondanse har EMD uttrykkelig lagt til grunn at korrespondansevernet også får anvendelse for nedtegnelser av opplysninger som har fremkommet gjennom en slik direkte dialog, jf. *Roemen og Schmit mot Luxembourg*, saksnr. 51772/99, 25. februar 2003 avsnitt 65. I hvilken utstrekning dette har overføringsverdi til andre tilfeller, fremstår noe usikkert.

Informasjon om kunders identitet og deres kontaktopplysninger tilkommer datasenteroperatøren gjennom dialog og kommunikasjon med kundene. I lys av EMDs praksis kan det ikke utelukkes at operatørens nedtegnelse av kundeopplysninger er å regne som korrespondanse etter EMK artikkel 8 nummer 1, men vernets utstrekning er som nevnt noe uklart. Det er imidlertid ikke nødvendig å ta endelig stilling til rekkevidden av korrespondansebegrepet, ettersom forslagene i høringsnotatet etter departementets syn uansett vil oppfylle inngrepsvilkårene i EMK artikkel 8 nummer 2.

3.2.2 Begrensninger i rettighetsvernet

Inngrep i privatlivs- og korrespondansevernet må skje på de vilkårene som er oppstilt i EMK artikkel 8 nummer 2. Det innebærer at inngrepet må være i samsvar med lov og være nødvendig i et demokratisk samfunn av hensyn til ett eller flere av de nærmere angitte legitime formålene i konvensjonsbestemmelsen. Hensynet til nasjonal sikkerhet og kriminalitetsbekjempelse er begge legitime formål etter artikkel 8 nummer 2.

Kravet om at inngrepet må være i samsvar med lov innebærer for det første at det må kunne forankres i et nasjonalt rettsgrunnlag, men det oppstilles ikke noen formelle krav til rettsgrunnlaget, jf. eksempelvis *Libert mot Frankrike*, saksnr. 588/13, 22. februar 2018 avsnitt 44. Det oppstilles derimot kvalitative krav. Rettsgrunnlaget må være tilgjengelig og forutsigbart, hvilket blant annet innebærer at rettsgrunnlaget må utformes på tilstrekkelig presist vis slik at den enkelte kan forutberegne sin rettsstilling og tilpasse sin atferd – om nødvendig etter å ha søkt passende råd, jf. *Rotaru mot Romania*, saksnr. 28341/95, 4. mai 2000 avsnitt 55.

Det nasjonale rettsgrunnlaget må også inneholde tilstrekkelige garantier mot vilkårlighet, jf. *S. og Marper mot Storbritannia*, saksnr. 30562/04 og 30566/04, 4. desember 2008 avsnitt 95. Dette innebærer blant annet muligheter for effektiv kontroll med det aktuelle tiltaket, jf. *M.N. mfl. mot San Marino*, saksnr. 28005/12, 7. juli 2015 avsnitt 63.

Slike rettssikkerhetsgarantier er for eksempel viktige når personopplysninger behandles til politimessige formål, jf. *S. og Marper mot Storbritannia*, saksnr. 30562/04 og 30566/04, 4. desember 2008 avsnitt 103. Aktuelle

rettssikkerhetsgarantier ved behandling av personopplysninger kan blant annet være regler om lagringstid og sletting, tilgang til opplysningene og prosedyrer for å sikre opplysningenes integritet og konfidensialitet, jf. *Breyer mot Tyskland*, saksnr. 50001/12, 30. januar 2020 avsnitt 83. Det samme gjelder regler som bidrar til at personopplysningene er relevante og begrenset til det som er nødvendig sett opp mot formålet opplysningene er lagret for, jf. *S. og Marper mot Storbritannia*, saksnr. 30562/04 og 30566/04, 4. desember 2008 avsnitt 103.

Inngrepets art og styrke vil være styrende for hvor presist det aktuelle rettsgrunnlaget må være og hvilke garantier mot vilkårlighet – herunder krav til tilsyn og kontroll – som er påkrevd, jf. *S. og Marper mot Storbritannia*, saksnr. 30562/04 og 30566/04, 4. desember 2008 avsnitt 103 og *Breyer mot Tyskland*, saksnr. 50001/12, 30. januar 2020 avsnitt 103 flg.

Spørsmålet om det foreligger tilstrekkelige garantier mot vilkårlighet henger nært sammen med vilkåret om at inngrepet må være «nødvendig i et demokratisk samfunn», jf. eksempelvis *Sommer mot Tyskland*, saksnr. 73607/13, 27. april 2017 avsnitt 53.

Vilkåret om at inngrepet må være «nødvendig i et demokratisk samfunn» innebærer at det må foreligge et presserende samfunnsmessig behov, jf. *L.B. mot Ungarn*, saksnr. 36345/16, 9. mars 2023 avsnitt 115, og at inngrepet må være forholdsmessig hensett til formålet med inngrepet, jf. *Breyer mot Tyskland*, saksnr. 50001/12, 30. januar 2020 avsnitt 91. I dette ligger et krav om at det må søkes å treffe en rimelig balanse mellom konvensjonsrettigheten det gripes inn og de legitime samfunnsbehovene som begrunner inngrepet, jf. *Breyer mot Tyskland*, saksnr. 50001/12, 30. januar 2020. Ved vurderingen av forholdsmessigheten av et inngrep må en plikt til å oppbevare eller lagre personopplysninger ses i sammenheng med tilgangen til og den mulige bruken av opplysningene, jf. avsnitt 97 i samme avgjørelse.

Staten har en viss skjønnsmargin ved vurderingen av om et inngrep er «nødvendig i et demokratisk samfunn». Rekkevidden av skjønnsmarginen påvirkes blant annet av arten og viktigheten av interessene som berøres og hvor alvorlig inngrepet er. Utlevering og lagring av store mengder informasjon vil kunne gjøre skjønnsmarginen snevrere, jf. Naumenko og Sia Rix Shipping mot Latvia, saksnr. 50805/14, 23. juni 2022 avsnitt 51. Samtidig vil marginen være videre med hensyn til inngrep som berører juridiske personer sammenlignet med inngrep som rammer fysiske personer, se *Bernh Larsen Holding AS mfl. mot Norge*, saksnr. 24117/08, 14. mars 2013 avsnitt 159.

Departementet har etter dette vurdert hvor inngripende en plikt til å ha tilgjengelig informasjon om kundenes navn, kontaktinformasjon og plasseringen av deres fysiske utstyr – samt en plikt til å utlevere denne informasjonen – vil være etter EMK artikkel 8. Isolert sett vil opplysningene ikke være sensitive personopplysninger. Departementet viser i denne sammenhengen til avgjørelsen *Breyer mot Tyskland*, saksnr. 50001/12, 30. januar 2020, hvor den tyske telekommunikasjonslovgivningen påla ekomtilbydere å registrere informasjon som identifiserte kunder med forhåndsbetalte SIM-kort. Opplysningene som måtte registreres omfattet kundens telefonnummer, navn og adresse, fødselsdato og dato for avtaleinngåelsen. EMD konkluderte med at inngrepet var nokså begrenset, jf. avsnitt 95, blant annet med henvisning til at

> «[…] only a limited data set was stored. These data did not include any highly personal information or allow the creation of personality profiles or the tracking of the movements of mobile-telephone subscribers. Moreover, no data concerning individual communication events were stored» (avsnitt 92).

Opplysningstypene som operatøren må oppbevare og etter omstendighetene utlevere er som nevnt begrenset til navn og kontaktinformasjon om kundene, samt informasjon om kundenes plassering av sitt fysiske utstyr i datasenteret. Disse opplysningene vil etter departementets oppfatning alltid være relevante for formålet som begrunner inngrepet. Det er dermed ikke tale om å få tilgang til store datamengder som datasenteroperatøren har lagret i sine systemer, hvor myndighetene også får tilgang til store mengder informasjon som ikke er relevant for inngrepsformålet, slik tilfellet var i *Bernh Holding AS mfl. mot Norge*, saksnr. 24117/08, 14. mars 2013. I motsetning til det som har vært tilfellet i en rekke avgjørelser for EMD om rettighetene til juridiske personer etter EMK artikkel 8, åpner heller ikke forslaget for at myndighetene kan søke på, og ta meg seg informasjon fra, datasenteroperatørenes kontorer.

En plikt til å oppbevare og utlevere slike opplysninger kan derfor ikke betegnes som et alvorlig inngrep i privatlivs- eller korrespondansevernet. Inngrepets intensitet vil naturligvis kunne øke dersom opplysningene gjelder et stort antall eller samtlige av datasenteroperatørens kunder.

Like fullt vil manglende etterlevelse av de foreslåtte bestemmelsene om plikt til å ha tilgjengelig oppdatert kundeinformasjon, utlevere kundeinformasjonen, ha en representant som er tilgjengelig i Norge og respondere innenfor nærmere angitte frister etter forslaget kunne møtes med overtredelsesgebyr. Handlingsnormene og bestemmelsen om overtredelsesgebyr må derfor i alle tilfeller utformes i tråd med lovkravet i Grunnloven § 113, EMK artikkel 7 nr. 1 og SP artikkel 15 nr. 1.

I tillegg nevner departementet at opplysninger om datasenteroperatørerenes kunder og deres kontaktinformasjon vil kunne være underlagt kontraktsfestet taushetsplikt. Departementet ser derfor at operatøren ofte vil ha en interesse i å bevare konfidensialitet omkring slike opplysninger. Departementet har vektlagt disse hensynene i vurderingen av hvilke krav som bør oppstilles for oppbevaring av kundeinformasjonen og for at myndighetene skal kunne få utlevert informasjonen.

Etter departementets oppfatning er forslagene om å ha tilgjengelig kundeinformasjon og å utlevere denne informasjonen utformet på tilstrekkelig presist vis og innebærer et forholdsmessig inngrep i privatlivs- og korrespondansevernet av hensyn til kriminalitetsbekjempelsen og nasjonale sikkerhetsinteresser. Dette har en sammenheng med at inngrepet ikke kan anses å være særlig alvorlig, samtidig som begrensningen i retten til respekt for privatliv og korrespondanse er begrunnet i tungtveiende samfunnsmessige hensyn.

Når det gjelder utformingen av rettsgrunnlaget, viser departementet til at forslaget i § 1-5 eksplisitt angir hvilke offentlige myndigheter som kan kreve informasjon utlevert og hvilke formål eller oppgaver som kan begrunne et pålegg om utlevering fra den enkelte myndigheten. Dette vil bidra til forutsigbarhet om hvilke myndigheter som har kompetanse til å kreve informasjonen utlevert og i hvilke tilfeller utlevering kan kreves. For det andre er plikten til å ha tilgjengelig og

utlevere kundeinformasjon begrenset til å omfatte opplysninger som er nødvendige for å kjenne kundens identitet og for å komme i kontakt med vedkommende kunde.

Det er også foreslått et vilkår om at informasjonen enten må være nødvendig i lys av – eller kunne være av betydning for – formålet med utleveringen. Hvilken informasjon som utleveres, vil dermed begrenses ytterligere. I tillegg er det foreslått visse formalkrav til pålegget, nærmere bestemt at det må fremsettes et skriftlig pålegg overfor datasenteroperatører som både informerer om hva saken gjelder, formålet, hva det omfatter og at vilkårene i utleveringshjemmelen er vurdert. Disse kravene vil også kunne være mekanismer som bidrar til at det ikke samles inn irrelevante eller et større antall opplysninger enn det er grunn til.

Departementet viser også til at det er gitt regler om politiet og påtalemyndighetens behandling av opplysninger i politiregisterloven og -forskriften som blant annet skal ivareta personvernet, mens regler for Nkom og NSM sin behandling av personopplysninger følger av personopplysningsloven og personvernforordningen. Den foreslåtte regelen om utlevering av kundeinformasjon i § 1-5 og andre regler i sikkerhetsloven om oppgaver og myndighet som er lagt til Nkom og NSM utgjør et supplerende rettsgrunnlag etter personvernforordningen artikkel 6 nummer 3 bokstav b. I sikkerhetsloven § 2-4 andre til fjerde ledd er det også gitt mer presise regler om NSMs behandling av personopplysninger i forbindelse med driften av den nasjonale responsfunksjonen for alvorlige digitale angrep og det nasjonale varslingssystemet for digital infrastruktur.

Videre kan det nevnes at Datatilsynet fører tilsyn med overholdelsen av politiregisterloven og -forskriften, med unntak for PSTs behandling av opplysninger, jf. politiregisterloven § 58. Datatilsynet fører også tilsyn med overholdelsen av personvernforordningen, jf. personopplysningsloven § 20 første ledd jf. personvernforordningen artikkel 51. Vedtak fra tilsynet kan påklages til Personvernnemnda, jf. politiregisterloven § 60 tredje ledd og personopplysningsloven § 22 andre ledd. For PSTs del fører Stortingets kontrollutvalg for etterretnings- og overvåkings- og sikkerhetstjenesten blant annet tilsyn med om opplysninger behandles i samsvar med politiregisterloven, jf. § 68. Endelig viser departementet til punkt 10.3 om overprøvingsmuligheter ved pålegg om utlevering av kundeinformasjon etter forslaget her.

4 Datasenteroperatørens plikt til å ha tilgjengelig oppdatert kundeinformasjon

4.1 Bakgrunn

Som beskrevet i punkt 2 i dette høringsnotatet, tilsier hensynet til nasjonal sikkerhet og kriminalitetsbekjempelse at det må stilles krav om at datasenteroperatørene kjenner sine kunder. Det er behov for at operatørene har en oppdatert kundeoversikt, slik at det kan gis informasjon om kundeforhold når myndighetene har hjemmel til å gi pålegg om utlevering av slike opplysninger. Kunnskap om hvem som er kunder i et datasenter, hvor i senteret kundene har sin virksomhet når de har fysisk utstyr i senteret og rask tilgang til slik informasjon kan som nevnt være avgjørende for at politiet og NSM skal kunne oppfylle sine samfunnsoppdrag, jf. Prop. 93 LS (2023–2024) side 204. I proposisjonen vises det til at det er viktig både å kunne identifisere kunden og kunne lokalisere dennes datastrøm.

4.2 Gjeldende rett

Etter ekomloven § 3-7 femte ledd tredje punktum kan departementet gi forskrift med krav om at datasenteroperatører skal føre oppdaterte lister over egne kunder og deres plassering i datasenteret. Det er per i dag ikke gitt slike forskriftsregler.

Det følger av datasenterforskriften § 1-3 andre ledd nummer 8 at datasenteroperatøren ved registrering hos Nkom skal opplyse om norske statlige, fylkeskommunale og kommunale myndigheter, organer og virksomheter som er kunder. Det er derimot ingen krav om at datasenteroperatøren skal oversende lister over alle sine kunder ved registrering. Datasenteroperatøren har heller ingen plikt til å føre oppdaterte kundelister hos seg.

4.3 Departementets vurderinger og forslag

Det er etter departementets syn behov for at datasenteroperatørene pålegges en plikt til å ha en oppdatert oversikt over visse opplysninger om sine kunder, slik at nødvendige opplysninger om kundeforhold er tilgjengelige når myndighetene har hjemmel for å pålegge utlevering av slik informasjon.

Informasjon om hvem som er kunde i et datasenter, deres kontaktinformasjon og, der det er relevant, hvor i senteret kunden driver sin virksomhet fra er viktig i flere sammenhenger. Departementet viser til redegjørelsen for behovet for tilgang til informasjon om kundeforhold i punkt 2 i dette høringsnotatet. At datasenteroperatørene har informasjonen tilgjengelig er særlig viktig i dagens geopolitiske sikkerhetssituasjon, og i håndteringen av dagens trussel- og risikobilde hvor kriminalitet i større grad enn tidligere foregår i det digitale rom. Dersom det er nødvendig å benytte tvangsmidler etter straffeprosessloven som ledd i etterforskningen av en straffesak, som for eksempel ransaking, beslag, kommunikasjonskontroll eller dataavlesning, er politiet blant annet avhengig av å lokalisere den aktuelle kunden i datasenteret for å sette i verk tiltakene. Tilgang til kundeinformasjon kan også være avgjørende for å sikre nasjonale sikkerhetsinteresser og ivaretakelsen av forsvarlig sikkerhet, i tillegg til en god håndtering av digitale trusler og hendelser.

Departementet antar at et krav om å ha oppdatert informasjon om hvem som er kunder i et datasenter, er lite kontroversielt. Datasentrene har behov for en slik oversikt for å ivareta sin egen virksomhet. Politiets og NSMs erfaring er imidlertid at informasjonen ikke alltid er tilgjengelig. En forskriftsregulering som oppstiller plikt til å ha informasjon om kundene tilgjengelig for myndighetene vil sikre at oversikten over kundeforhold foreligger, og hva den som minimum skal inneholde.

Departementets vurdering er at plikten til å melde inn opplysninger om kunder til Nkom i henhold til de gjeldende kravene i datasenterforskriften § 1-3, som kun omfatter norske statlige, fylkeskommunale og kommunale myndigheter, organer og virksomheter, ikke er tilstrekkelig for å ivareta hensynene til kriminalitetsbekjempelse og nasjonal sikkerhet.

På denne bakgrunnen foreslår departementet at datasenterforskriften oppstiller krav i ny § 1-4 om at datasenteroperatører skal ha oppdatert kundeinformasjon tilgjengelig. Departementet foreslår at denne plikten påhviler alle datasenteroperatører, jf. ny ekomlov § 1-5 nummer 38 bokstav a og b. Dette innebærer at både aktører som tilbyr andre tilgang til datasentertjenester mot vederlag og aktører som driver datasenter med en abonnert elektrisk effekt over

den forskriftsfastsatte terskelverdien, vil pålegges å ha en oversikt over egne kunder. Plikten til å ha oversikt over egne kunder, gjelder de kundene datasenteroperatøren har et direkte kundeforhold til i datasenteret, det vil si kunder som datasenteroperatører normalt inngår avtaler med. Datasenteroperatører som driver datasentre for drift av egne digitale tjenester (for eksempel hyperscale-datasenter) skal dermed ha oppdatert kundeinformasjon tilgjengelig, mens rene virksomhetsinterne datasentre, der operatøren ikke tilbyr digitale tjenester til andre, ikke vil pålegges en slik plikt da disse operatørene ikke har kunder i datasenteret. Ved at enhver datasenteroperatør plikter å ha oversikt over kundeinformasjon, vil informasjon om kundeforhold være tilgjengelig for myndighetene når de har hjemmel for tilgang til informasjonen.

Departementet mener at det vil være tilstrekkelig at den spesifikke kundeinformasjonen finnes tilgjengelig digitalt i datasenteroperatørens systemer, at informasjonen kan sammenstilles relativt raskt og at den er oppdatert til enhver tid. Det pålegges derfor ikke en plikt til å ha oppdaterte utskrifter av lister med kundeinformasjon. Det forventes imidlertid at en datasenteroperatør eller dennes representant på forespørsel fra myndighetene sørger for en hensiktsmessig utlevering av etterspurt informasjon, enten i form av utskrift eller ved elektronisk overføring av informasjonen.

Plikten til å føre oversikt over egne kunder må ses i sammenheng med de foreslåtte reglene om utlevering av kundeinformasjon, jf. punkt 5 - 10 samt kravet om en stedlig representant og kravet til kunnskap og fullmakter representanten skal ha for å kunne bistå Nkom, politiet og NSM, jf. punkt 11.

Et særlig spørsmål er hvilken informasjon datasenteroperatøren skal ha om kundene. Departementet foreslår at oversikten skal omfatte informasjon som er nødvendig for at kunden på en enkel måte kan identifiseres og kontaktes av myndighetene når vilkårene for utlevering er oppfylt.

Departementet viser til at enhver som har regnskapsplikt etter regnskapsloven har bokføringsplikt etter bokføringsloven, jf. bokføringsloven § 2 første ledd. Etter regnskapsloven § 1-1 første ledd gjelder loven regnskapspliktige som nevnt i § 1-2 første ledd nummer 1 til 12 som er hjemmehørende i Norge, samt regnskapspliktige som nevnt i § 1-2 første ledd nummer 13. Det omfatter blant annet aksjeselskap etter § 1-2 første ledd nummer 1.

Bokføringsforskriften § 5-1-1 første ledd nummer 1 til 7 stiller minstekrav til innholdet i dokumentasjonen av salg av varer og tjenester. Etter nummer 2 skal angivelse av partene opplyses. Etter bokføringsforskriften § 5-1-2 første ledd skal angivelse av kjøper minst inneholde kjøpers navn, og adresse eller organisasjonsnummer som er tildelt i henhold til enhetsregisterloven § 23. Dersom kjøper er registrert i Merverdiavgiftsregisteret, skal organisasjonsnummer etterfølges av bokstavene MVA, jf. tredje punktum.

Departementet antar at de fleste datasenteroperatører vil være underlagt bokføringsregelverket og derfor må ivareta kravene til hvilke opplysninger salgsdokumentasjon skal inneholde. Departementet legger derfor til grunn at datasenteroperatørene har tilgang til kundens navn, adresse og organisasjonsnummer, og departementet foreslår at kundeinformasjonen som et minimum skal omfatte disse opplysningene.

Departementet antar videre at datasenteroperatørene også har opplysninger om kundenes telefonnummer, e-postadresse og kundens eventuelle nettadresse, eller at disse opplysningene er enkelt å skaffe til veie. Departementet foreslår at også disse opplysningene skal medtas i informasjonen som skal være tilgjengelig, slik at det er mulig å komme i kontakt med kundene på en enkel måte.

Departementet foreslår videre at aktørene som omfattes av ny ekomlov § 1-5 nummer 38 bokstav a, også skal føre oversikt over hvor i senteret de ulike kundene driver sin virksomhet fra. På denne måten vil myndighetene, når de har hjemmel for tilgang til slik informasjon, raskt kunne få oversikt over hvilke kunder som fysisk befinner seg i slike datasentre og hvor utstyret deres er plassert. At slik informasjon er tilgjengelig vil blant annet være avgjørende når politiet i henhold til straffeprosessloven skal iverksette tvangsmidler mot enkeltkunder.

At denne plikten kun påhviler de datasenteroperatørene som omfattes av ny ekomlov § 1-5 nummer 38 bokstav a innebærer at bestemmelsen kun omfatter de operatørene som tilrettelegger for at kunder kan innplassere eget utstyr i datasenteret (i hovedsak såkalte co-location aktører).

Operatører som kun omfattes av ekomloven § 1-5 nummer 38 bokstav b, det vil si operatører som driver datasenter med en abonnert elektrisk effekt over den forskriftsfastsatte terskelverdien, uten at andre tilbys tilgang til datasentertjenester slik dette er definert i ekomloven § 1-5 nummer 37, vil dermed ikke pålegges å ha oversikt over hvor i senteret ulike kunder er plassert. Slike datasenteroperatører vil ikke ha fysisk, men logisk adskilte kunder. Dette innebærer at kundene deler fysisk infrastruktur med andre kunder, og at et krav om å føre oversikt over hvor de enkelte kundenes utstyr fysisk befinner seg ikke er relevant eller mulig på samme måte som for fysisk adskilte kunder. Det vises i denne sammenheng også til Innst. 28 L (2024–2025) side 4, hvor komiteens flertall (medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti) merker seg flere høringsinnspill fra datasenteraktører som omhandler nye forskriftskrav knyttet til registrering av kunder og deres fysiske plassering i datasenteret. Dette flertallet legger blant annet til grunn at det må være praktisk gjennomførbart å etterleve slike krav.

5 Overordnet om forslaget om plikt for datasenteroperatøren til å utlevere informasjon om egne kunder

Det følger som tidligere nevnt av ekomloven § 3-7 femte ledd tredje punktum at departementet kan fastsette krav om at blant annet politiet og EOS-tjenestene på nærmere vilkår gis rask tilgang til informasjon om datasenteroperatørenes kunder og deres plassering i senteret. Departementet vises også til at ekomloven § 3-7 femte ledd tredje punktum gir hjemmel for å gi forskrifter om nasjonal sikkerhet, noe som innebærer at bestemmelsen også hjemler forskriftsregler om Nkoms behov for å få utlevert kundeinformasjon for å kartlegge hvilke datasentre som har vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser, jf. sikkerhetsloven §§ 1-3 og 2-1, eller for øvrig for å ivareta sine sektoroppgaver etter sikkerhetsloven.

I Prop. 93 LS (2023–2024) side 281 utdyper departementet innholdet i forskriftshjemmelen. Der heter det blant annet at forskriftshjemmelen gir rettslig grunnlag for å fastsette at politiet og EOS-tjenestene kan gis tilgang til

informasjonen på nærmere vilkår. Det fremgår også at vilkårene skal balansere hensynet til kriminalitetsbekjempelse og nasjonal sikkerhet og hensynet til hensiktsmessige rammevilkår for datasenternæringen. Departementet la videre til grunn at krav om tilgang til informasjonen skal gjøres skriftlig, for eksempel av leder for politidistriktene eller EOS-tjenestene eller den disse bemyndiger. Formålet med kravet om at avgjørelsen skal være formell, er ifølge proposisjonen at beslutningen om å kreve tilgang til informasjon fra datasenteroperatøren har notoritet og at beslutningen kan påklages.

På side 204 i proposisjonen fremgår det at forskriftshjemmelen også skal kunne gi hjemmel for at politiet og EOS-tjenestene på nærmere vilkår skal kunne innhente denne informasjonen i *forebyggende øyemed*.

Informasjonen som kan utleveres i medhold av forskriftshjemmelen, er begrenset til informasjon om datasenteroperatørens kundeforhold og plasseringen av kundenes fysiske utstyr i datasenteret. Forskriftshjemmelen åpner ikke for tilgang til andre opplysninger hos datasenteroperatøren. Tilgang til annen informasjon enn nevnte kundeinformasjon må følge annet regelverk, for eksempel reglene om tvangsmidler i straffeprosessloven og politiloven.

NSM har etter *gjeldende rett* ikke noen egen hjemmel for å kreve utlevert kundeinformasjon fra datasenteroperatører, jf. redegjørelsen i punkt 8.2. Politiet kan derimot få tilgang til slik informasjon i medhold av tvangsmidlene i straffeprosessloven når vilkårene for disse er oppfylt – se punkt 6. PST kan i tillegg få tilgang til kundeinformasjon ved bruk av tvangsmidler i forebyggende øyemed i medhold av politiloven når vilkårene for dette er oppfylt. Det er redegjort for disse reglene i punkt 7 nedenfor.

Nkom vil med hjemmel i ekomloven § 15-2 kunne kreve utlevert kundeinformasjon fra datasenteroperatør. Formålet med en slik utlevering vil imidlertid være å ivareta myndighetens oppgaver etter ekomloven. Nkom har etter gjeldende rett ikke noen egen hjemmel til å kreve kundeinformasjon for å ivareta sine oppgaver etter sikkerhetsloven.

Departementet foreslår i dette høringsnotatet en *ny bestemmelse i datasenterforskriften § 1-5* som gir datasenteroperatør som nevnt i ekomloven § 1-5 nummer 38 bokstav a plikt til å utlevere kundeinformasjon til Nkom, NSM, PST, politiet og påtalemyndigheten når nærmere vilkår er oppfylt. I tillegg foreslår departementet at datasenteroperatør som nevnt i ekomloven § 1-5 nummer 38 bokstav b får plikt til å utlevere kundeinformasjon til Nkom og NSM.

At plikten til å levere ut kundeinformasjon til politiet og PST etter § 1-5 første og andre ledd kun skal gjelde for datasenteroperatør som tilbyr andre tilgang til datasentertjeneste mot vederlag, jf. ny ekomlov § 1-5 nummer 38 bokstav a, innebærer at datasenteroperatører som driver datasenter med en abonnert elektrisk effekt over den forskriftsfastsatte terskelverdien uten at andre tilbys tilgang til datasentertjeneste mot vederlag, ikke omfattes av forslaget til § 1-5 første og andre ledd. Datasenteroperatører som driver datasentre for drift av egne digitale tjenester (for eksempel hyperscale-datasenter), omfattes med andre ord ikke av plikten til å utlevere informasjon om kundeforhold til politiet og PST.

Bakgrunnen for dette skillet er at det er en vesensforskjell mellom å tilby fysisk innplassering av servere og det å tilby for eksempel skytjenester. Når det gjelder aktører som faller inn under ekomloven § 1-5 nummer 38 bokstav b, for eksempel

skytjenesteleverandører, antar departementet at det i hovedsak vil være tilstrekkelig for politi og påtalemyndighet å identifisere og komme i kontakt med operatøren av datasenteret. Dersom man har behov for å avverge eller stanse lovbrudd innad i et datasenter som leverer skytjenester, der kundenes data er logisk adskilt, antar departementet videre at det vil være behov for informasjon om et større antall kunder. Et slikt pålegg om utlevering vil kunne innebære at forretningshemmeligheter kreves utlevert, som i etterforskning er underlagt et særskilt vern etter straffeprosessloven § 124. Etter straffeprosessloven er det retten som må pålegge utlevering av informasjon som utgjør en forretningshemmelighet, jf. punkt 6.2.2.3 nedenfor. På bakgrunn av dette foreslås det ikke å gi en utleveringshjemmel etter datasenterforskriften som åpner for at politiet eller påtalemyndigheten kan gi pålegg om utlevering av kundeinformasjon fra datasenteroperatører som nevnt i ekomloven § 1-5 nummer 38 bokstav b.

Informasjonen som kan være gjenstand for utlevering til politiet og PST etter forslaget til ny § 1-5 første og andre ledd, vil dermed være begrenset til opplysninger om navn og kontaktinformasjon for kunder som har leiet plass og innplassert fysisk utstyr i et datasenter og informasjon om hvor i datasenteret utstyret deres er lokalisert. En nærmere angivelse av hvilke opplysninger som kan pålegges utlevert vil følge av datasenterforskriften § 1-4, jf. høringsnotatet punkt 4.3.

I det følgende drøfter departementet behovet for en utleveringshjemmel til politiet og påtalemyndigheten i punkt 6, mens en hjemmel for PST, NSM og Nkom behandles i henholdsvis punkt 7, 8 og 9.

6 Nærmere om utlevering av kundeinformasjon til politiet og påtalemyndigheten

6.1 Bakgrunn

6.1.1 Politiets rolle og oppgaver

De overordnede oppgavene som er tillagt politiet kommer til uttrykk i politiloven § 2. I § 2 nummer 2 fremgår det at politiet skal forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet, mens det følger av nummer 3 at politiet skal avdekke og stanse (herunder avverge) kriminell virksomhet og forfølge straffbare forhold. I tillegg er det lagt til politiet å beskytte person og eiendom og verne om all lovlig virksomhet samt yte borgerne hjelp og tjenester i faresituasjoner, jf. nummer 1 og 4.

Ansvaret og oppgavene politiet er tillagt er de samme i den fysiske og den digitale verden, og det er forventet at politiet skal kunne utføre sine lovpålagte oppgaver også i det digitale rom. Disse forventningene er tilkjennegitt fra flere hold, blant annet i Justis- og beredskapsdepartementets strategi mot IKT-kriminalitet fra 2015. Der fremhever departementet at det er en klar visjon og målsetning at det digitale rommet skal være like trygt som det fysiske, og at blant annet politiet skal skape trygghet, forebygge, avverge, oppklare og straffeforfølge IKT-kriminalitet, jf. side 5. Departementet viser også til Nasjonal strategi for digital sikkerhet fra 2019 side 21 og Innst. 187 S (2017–2018) side 12. Riksadvokaten har også i flere år fremhevet alvorlig IKT-kriminalitet, blant annet straffbare handlinger rettet mot

datasystemer og nettverk samt kriminalitet der teknologi og datasystemer utgjør en vesentlig eller sentral komponent, som en sakstype som skal prioriteres, jf. senest rundskriv nummer 1/2024 del III punkt 2 side 8.

Selv om forventningene til hvordan politiet løser sitt samfunnsoppdrag er de samme med hensyn til digitale og fysiske hendelser, kan digitale hendelser fortone seg annerledes enn fysiske hendelser og aktualisere andre spørsmål og behov. Den teknologiske utviklingen vil stadig utfordre og stille nye krav til politiets oppgaveløsning, jf. også Meld. St. 38 (2016–2017) side 31.

6.1.2 Særlig om kriminalitet i og fra datasentre

Politiet kan motta informasjon om mulige avsluttede, pågående eller nært forestående straffbare handlinger med tilknytning til datasentre på flere måter. Politiet kan for eksempel motta opplysninger fra samarbeidende myndigheter om at en virksomhet i et datasenter er utsatt for et løsepengevirus eller datainnbrudd, bli bedt av internasjonale samarbeidspartnere om å følge opp datainnbrudd som er gjennomført eller gjennomføres fra en IP-adresse sporet til en norsk datasenterkunde eller motta informasjon om at en virksomhet i et datasenter er utsatt for kriminalitet og brukes som utgangspunkt for ny kriminalitet. Ved pågående eller nært forestående hendelser er det en forventning om at politiet reagerer raskt på informasjonen og iverksetter egnede tiltak for å stanse eller avverge den straffbare handlingen. Målsetningen er å unngå skadevirkninger ved at kriminell virksomhet får starte eller fortsette, og det vil kunne være et betydelig hasteaspekt i slike situasjoner.

Dersom politiet mottar opplysninger om akutte hendelser i det fysiske rom, vil politiet i kraft av sin alminnelige handlefrihet – og i en politioperativ sammenheng – kunne undersøke stedet, gjøre passive observasjoner og ha frivillige samtaler med personer som enten er på stedet eller i umiddelbar nærhet av gjerningsstedet og gjøre andre enkle undersøkelser, for på den måten å raskt opparbeide en situasjonsforståelse eller avklare hendelsesforløpet.

Når politiet ankommer et datasenter, vil situasjonen være noe annerledes. Politiloven § 7 kan etter omstendighetene hjemle at politiet tar seg inn i et datasenter for å stanse et dataangrep fra en server i senteret. Det som møter politiet, vil i stor grad være servere og tilhørende utstyr. Visuelt vil politiet se rader med serverstativer, kabler til nettverksforbindelser, kjølesystemer og sikkerhetssystemer som beskytter infrastrukturen. I noen sentre vil ulike kunder være fysisk adskilte i forskjellige rom eller bygninger. Kundene er ikke fysisk til stede og ofte vil det ikke være mulig for politiet å vite hvem som er kunder i datasenteret og hvilket utstyr som tilhører den enkelte kunde kun ved å se seg om i datasenteret. I motsetning til i den fysiske verden kan politiet med andre ord vanskelig orientere seg gjennom passiv observasjon, og det er ikke alltid personer til stede som muliggjør frivillige samtaler med personer på stedet. Politiet vil dermed regelmessig ikke komme i kontakt med de forskjellige kundene eller vite hvor i senteret de er lokalisert uten bistand fra datasenteroperatøren, som ofte vil ha en avtalefestet taushetsplikt om kundeforholdene sine.

Politiets tilgang til informasjon er med andre ord mer begrenset når gjerningsstedet er et datasenter enn når de rykker ut til en hendelse i samfunnet ellers. Virkningen av informasjonsmangelen kan illustreres ved et eksempel. Man kunne tenkt seg at det var hensiktsmessig å kutte strømmen til serveren et angrep

skjer fra, men dette lar seg ikke gjøre dersom man ikke har informasjon om hvilken kunde som driver virksomhet fra de ulike serverne. Man kunne som alternativ kuttet strømmen til hele eller deler av datasenteret, men all den tid man ikke vet hvilke andre kunder som befinner seg der, risikerer man å kutte strømmen til kunder som ivaretar viktige samfunnsoppgaver. Avhengig av hvilke reserveløsninger for strøm den enkelte datasenteroperatøren benytter, vil kutting av strømmen dessuten kunne være teknisk komplisert og kunne ha uklare virkninger for hendelsen myndighetene ønsker å håndtere. Å kutte strømmen til hele eller deler av senteret vil dessuten måtte anses å være et svært inngripende tiltak, som i mange situasjoner vil være uforholdsmessig.

For å kunne vurdere hvilke tiltak som bør settes i verk for å stanse eller avverge et lovbrudd som begås mot eller av kunder i et datasenter, er politiet altså avhengig av å ha nok informasjon til å kunne etablere en tilstrekkelig situasjonsforståelse. For å få den nødvendige informasjonen om kundenes identitet, kontaktinformasjon og deres plassering i senteret, er politiet avhengig av bistand fra datasenteroperatøren. Tilgang til informasjon om kundene vil medføre at politiet kan sette i verk spissede avvergende eller stansende tiltak mot dem som er berørte av eller begår et lovbrudd. Politiet vil kunne komme i kontakt med virksomheter med sikte på å varsle berørte kunder eller gjennomføre en frivillig samtale for å opparbeide en situasjonsforståelse eller avklare hendelsesforløpet. Tilgangen til kundens kontaktinformasjon vil også kunne forhindre at eksempelvis et dataangrep sprer seg, ved at politiet kan stanse angrepet eller advare kundene om at systemene deres kan være kompromitterte og anbefale at sikkerhetstiltak iverksettes. Hvis opplysningene tilgjengeliggjøres for politiet, kan det dessuten vurderes om andre myndigheter – særlig Nkom og NSM – skal varsles og involveres, om virksomheten skal stanses eller andre tiltak settes i verk og – dersom etterforskning ikke allerede er igangsatt – om etterforskning skal iverksettes og i så fall hvilke etterforskningsskritt som skal foretas.

6.2 Gjeldende rett

6.2.1 Politiets hendelseshåndtering utenfor etterforskning

Det følger av politiloven § 7 første ledd nummer 3 at politiet kan gripe inn for å avverge og stanse lovbrudd. Etter samme bestemmelse nummer 2 kan politiet gripe inn for å ivareta enkeltpersoners eller allmennhetens sikkerhet, uavhengig av om trusselen skyldes et straffbart forhold.

Tiltak etter § 7 første ledd nummer 2 og 3 kan gjennomføres ved metoder som ligger innenfor den alminnelige handlefriheten eller metoder som følger av politiloven § 7 andre ledd. I medhold av sistnevnte bestemmelse kan politiet blant annet regulere ferdsel, forby opphold i bestemte områder, visitere person eller kjøretøy, uskadeliggjøre eller ta farlige gjenstander i forvaring, avvise, bortvise, fjerne eller anholde personer, påby virksomhet stanset eller endret og ta seg inn på privat eiendom eller påby områder evakuert. Opplistingen er ikke uttømmende, men de inngrepsmåtene som benyttes, må ligne på de som er positivt angitt og ikke være mer inngripende enn disse. Selv om virkemidlene som nevnes i politiloven § 7 andre ledd er utformet primært med tanke på inngripen mot trusler og straffbare handlinger i det fysiske rom, må de samme tiltakene også kunne brukes der handlingen skjer digitalt.

Departementet viser for øvrig til at politiloven § 7 andre ledd ikke hjemler pålegg om utlevering av informasjon om datasenteroperatørens kunder.

6.2.2 Utlevering av kundeinformasjon til politiet og påtalemyndigheten i etterforskning

6.2.2.1 *Oversikt*

I etterforskning kan politiet og påtalemyndigheten innhente informasjon fra datasenteroperatører om kundeforhold i medhold *av reglene om beslag og utleveringspålegg* i straffeprosessloven.

Det følger av straffeprosessloven § 224 at etterforskning foretas når det er *rimelig grunn til å undersøke* om det *foreligger et straffbart forhold*. Riksadvokaten har i rundskriv nummer 3/1999 angitt tre sentrale momenter til denne skjønnsmessige vurderingen, nærmere bestemt sannsynlighet, proporsjonalitet og saklighet. Hvilken sannsynlighet som bør kreves for at det foreligger et straffbart forhold, vil særlig variere med hvor alvorlig det mulige lovbruddet er. For en nærmere redegjørelse for etterforskningsbegrepet viser departementet til Riksadvokatens rundskriv nummer 3/1999 samt Prop. 68 L (2015–2016) side 176–177 og Ot.prp. nr. 60 (2004–2005) side 42–43.

Utover at det må være igangsatt etterforskning, må det alltid være tilstrekkelig grunn til å beslutte beslag eller utleveringspålegg, og tvangsmiddelbruken må i tillegg være forholdsmessig, jf. straffeprosessloven § 170 a.

6.2.2.2 *Nærmere om beslag*

Det kan tas beslag i ting som antas å ha betydning som bevis, jf. straffeprosessloven § 203 første ledd første punktum. Ved beslag overtar politiet og påtalemyndigheten rådigheten over det beslaglagte. For å kunne ta beslag må politiet kunne sette seg i besittelse av tingen.

Av ordlyden i § 203 første ledd første punktum fremgår det at gjenstanden for beslag er «ting». Uttrykket forstås vidt, og det omfatter blant annet både fysiske dokumenter og elektronisk lagret informasjon, jf. eksempelvis Rt. 2011 side 296 avsnitt 24 for så vidt gjelder elektronisk informasjon.

Selv om det ikke fremgår av ordlyden i § 203, er det lagt til grunn at det må være skjellig grunn til mistanke om et straffbart forhold for å ta beslag, jf. Rt. 1999 side 1414 på side 1415. Det kreves imidlertid ikke mistanke rettet mot en enkeltperson.

Hvis besitteren av en ting ikke ønsker å overlevere tingen frivillig, beslutter påtalemyndigheten beslag av tingen, jf. straffeprosessloven § 205 første ledd. Påtalemyndigheten kan – dersom det foreligger særlige grunner – bringe spørsmålet om beslag inn for retten, jf. § 205 andre ledd. Hvis det er fare ved opphold, kan politimann ta beslag, og tilsvarende gjelder blant annet når politimann iverksetter beslutning om ransakelse, jf. straffeprosessloven § 206 første ledd.

Straffeprosessloven oppstiller enkelte formkrav til beslutninger om beslag. Beslutningen skal så vidt mulig være skriftlig, opplyse om hva saken gjelder, hva formålet med beslaget er og hva beslaget omfatter, og muntlige beslutninger skal snarest mulig nedtegnes, jf. § 205 første ledd annet punktum.

Den som blir rammet av et beslag, har en rett til å få spørsmålet om opprettholdelse av beslaget avgjort av retten ved kjennelse, jf. straffeprosessloven § 208 første ledd jf. tredje ledd. Den som frivillig overleverer tingen, kan kreve spørsmålet om tilbakelevering av tingen prøvd av retten, jf. § 208 andre ledd.

6.2.2.3 *Nærmere om utleveringspålegg*

I medhold av straffeprosessloven § 210 første ledd kan besitteren av en ting pålegges å utlevere den. Utleveringspålegg kan besluttes i alle sakstyper, men bare overfor dem som plikter å vitne i saken, jf. § 210 første ledd første punktum. Utleveringspålegg sammenfaller altså med vitneplikten i straffesaker, jf. bestemmelsene om vitneplikt i straffeprosessloven kapittel 10.

I motsetning til det som er tilfellet ved beslag, må besitteren av tingen aktivt medvirke til at politiet får hånd om tingen. Reglene om utleveringspålegg er et alternativ til – og supplerer – reglene om beslag. Utleveringspålegg kan utstedes der politiet selv ikke er i posisjon til å overta besittelsen av en ting.

Som for beslag er det et vilkår at tingen kan antas å ha betydning som bevis.

I motsetning til kompetansereglene for beslutning om beslag er primærkompetansen til å beslutte utleveringspålegg lagt til retten, jf. straffeprosessloven § 210 første ledd. Ved fare for opphold kan likevel påtalemyndigheten beslutte utleveringspålegg, men slik beslutning skal snarest mulig forelegges retten, jf. § 210 andre ledd. Slike beslutninger fra påtalemyndigheten skal så vidt mulig være skriftlig, hvor det opplyses hva saken gjelder, formålet med pålegget og hva det skal omfatte, jf. § 210 fjerde ledd jf. straffeprosessloven § 197 tredje ledd. Muntlige beslutninger skal snarest mulig nedtegnes.

6.2.2.4 *Begrensninger i adgangen til beslag og utleveringspålegg – nærmere om forretningshemmeligheter*

Begrensninger i adgangen til å ta *beslag* følger av straffeprosessloven § 204 første ledd. I utgangspunktet kan det ikke tas beslag i ting som inneholder opplysninger som et vitne etter reglene om vitneforklaringer i straffeprosessloven §§ 117 til 121 og 124 til 125 har rett eller plikt til ikke å forklare seg om, og som besittes av den som kan nekte å forklare seg eller som har rettslig interesse i hemmelighold. I den utstrekning det etter de nevnte bestemmelser kan pålegges vitneplikt i visse tilfelle, gjelder dette tilsvarende for adgangen til beslag.

Av straffeprosessloven § 205 tredje ledd første punktum fremgår det at påtalemyndigheten må ha rettens kjennelse for å ta beslag i ting som inneholder opplysninger som besitteren ikke plikter å forklare seg om uten etter særskilt pålegg fra retten. Dersom politiet vil ta med dokumenter til retten for avgjørelse av om beslag kan tas, skal dokumentene forsegles i lukket konvolutt i nærvær av en representant for besitteren, jf. tredje ledd annet punktum. Tilsvarende begrensninger gjelder for *utleveringspålegg*, jf. straffeprosessloven § 210 første ledd, da utleveringspålegg som nevnt bare kan besluttes overfor dem som plikter å vitne i saken.

Det følger av det ovenstående at én mulig begrensning i adgangen til å benytte utleveringspålegg og beslag for å få tilgang til informasjon om datasenteroperatørers kundeforhold, er reglene om forretningshemmeligheter i straffeprosessloven § 124. Etter straffeprosessloven § 124 har et vitne rett til å

nekte å svare på spørsmål som kan åpenbare en *forretningshemmelighet*. Retten kan likevel pålegge vitnet å forklare seg når den «etter en avveining av de stridende interesser finner det påkrevd». I så fall skal retten pålegge de tilstedeværende taushetsplikt og forbud mot bruk av forretningshemmeligheten som kan utledes av forklaringen. I tillegg har retten adgang til å lukke dørene når den mottar forklaringen, jf. andre ledd annet punktum.

Pålegg om utlevering av dokumenter som inneholder forretningshemmeligheter må dermed gis av retten, og retten må være av den oppfatning at tilgangen til forretningshemmeligheten er påkrevd. Også beslag av slike dokumenter må besluttes av retten, jf. straffeprosessloven § 205. For å avgjøre om retten må involveres ved utferdigelse av beslag eller utleveringspålegg som omfatter informasjon om kundeforhold, må innholdet i forretningshemmelighetsbegrepet etter straffeprosessloven § 124 fastlegges.

Ordlyden i straffeprosessloven § 124 ble endret ved innføringen av lov 27. mars 2020 nummer 15 om vern av forretningshemmeligheter (forretningshemmelighetsloven). Tvisteloven inneholder en lignende regel om bevisfritak i § 22-10, som også ble endret gjennom forretningshemmelighetsloven. Formålet med endringen av både straffeprosessloven og tvisteloven var å modernisere ordlyden, uten at dette skulle endre gjeldende rett, jf. Prop. 5 LS (2019–2020) side 129 jf. side 128.

Spørsmålet om – og i hvilken utstrekning – informasjon om virksomheters kunder skal regnes som en forretningshemmelighet, er ikke drøftet i forarbeidene eller rettspraksis om straffeprosessloven § 124. I kommentaren til straffeprosessloven § 124 er det riktignok uttalt at «kundeforhold» kan være å regne som en forretningshemmelighet, jf. Erik Keiserud mfl. Lovkommentar til straffeprosessloven § 124, Universitetsforlaget, note 2 (à jour 1. januar 2024). Uttalelsen er imidlertid helt generell og er ikke begrunnet nærmere.

Ved tolkningen av straffeprosessloven § 124 vil blant annet uttalelser om tvisteloven § 22-10 være relevante. Det vil også være relevant å se hen til legaldefinisjonen i forretningshemmelighetsloven, ettersom definisjonen i forretningshemmelighetsloven i all hovedsak omfatter samme opplysninger som etter blant annet bevisfritaksreglene i tvisteloven § 22-10 og straffeprosessloven § 124, jf. Prop. 5 LS (2019–2020) side 24. I tillegg vil uttalelser om straffeloven § 207 og markedsføringsloven § 28 forut for ikrafttredelsen av forretningshemmelighetsloven fremdeles ha betydning for tolkningen av straffeprosessloven § 124, jf. side 17 i samme proposisjon.

Forretningshemmelighetsloven § 2 første ledd oppstiller tre kumulative vilkår for at en opplysning skal anses som en forretningshemmelighet. Opplysningene må for det første være *hemmelige* – det vil si at de ikke som helhet, eller slik de er satt sammen eller ordnet, er allment kjent eller lett tilgjengelig. Dette vilkåret ble tidligere omtalt som et krav om at informasjonen er foretaksspesifikk, jf. Prop. 5 LS (2019–2020) side 119. Kriteriet er ment å avgrense mot allmenn viten. Selv om enkelte kundeforhold ikke anses å være hemmelige, vil en oversikt over en virksomhets samlede kundemasse, for eksempel i form av et kunderegister eller en kundeliste, likevel kunne være noe som ikke er enkelt tilgjengelig for andre og som dermed kan anses som hemmelig, jf. side 21 i proposisjonen.

Innehaveren må for det andre *ha truffet rimelige tiltak for å holde opplysningene hemmelige*. Slike tiltak kan være organisatoriske, rettslige eller tekniske. Det sentrale vurderingstemaet er om innehaveren av en forretningshemmelighet har en berettiget interesse i hemmelighold, jf. Prop. 5 LS (2019–2020) side 119.

Endelig må opplysningene *ha kommersiell verdi fordi de er hemmelige*. Dette innebærer at opplysningene må ha en faktisk eller potensiell verdi for virksomheten eller markedet, jf. Prop. 5 LS (2019–2020) side 119. Kriteriet vil være oppfylt hvor inngrep kan skade innehaveren av opplysningene ved for eksempel å undergrave dennes forretningsmessige eller finansielle interesser, eller evne til å konkurrere. Det må derfor avgrenses mot ubetydelige opplysninger. Vilkåret om kommersiell verdi vil kunne være oppfylt når «markedet er villig til å gi innehaveren vederlag eller andre økonomisk målbare fordeler for tilgang til de aktuelle opplysningene, eller opplysningene gir innehaveren konkurransefortrinn ved bruk i egen virksomhet», jf. Prop. 5 LS (2019–2020) side 24.

I relasjon til tvisteloven § 22-10 og forvaltningsloven § 13 første ledd nummer 2 er det på lignende vis avgrenset mot ubetydelige opplysninger. Etter disse bestemmelsene må opplysningen være av en viss betydning, og offentlighet omkring opplysningen må kunne føre til økonomisk tap eller redusert gevinst for virksomheten, jf. HR-2022-2386-F avsnitt 12. Forvaltningsloven § 13 nr. 2 omfatter dessuten ikke enhver opplysning om forretningsforhold som kan medføre et økonomisk tap for virksomhet dersom opplysningen blir kjent. De mindre sensitive næringsopplysningene faller utenfor, og skadevirkningene for virksomhetens konkurranseevne må være ikke uvesentlige, jf. G-2009-418 side 86.

Opplysninger om sikkerhetsrutiner og lignende er ikke omfattet av definisjonen i forretningshemmelighetsloven fordi beskyttelsen av opplysningene ikke er ansett å være begrunnet i den konkurransemessige betydningen av hemmelighold, jf. Prop. 5 LS (2019–2020) side 25. Slike opplysninger kan likevel etter omstendighetene være omfattet av vernet om forretningshemmeligheter i tvisteloven og straffeprosessloven, jf. Rt. 1998 side 1624. Avgjørelsen gjaldt opplysninger om Norsk Folkemuseums vaktrutiner, alarmsystemer og sikkerhetsopplegg, og opplysningene var av vesentlig betydning for å beskytte en samling på mer enn 250 000 gjenstander av stor nasjonal, kulturhistorisk og økonomisk verdi. Avgjørelsen viser at det ikke kan utelukkes at opplysninger som vil kunne utsette en virksomhet for en betydelig sikkerhetsrisiko i helt spesielle tilfeller kan være omfattet av vernet etter straffeprosessloven § 124.

På bakgrunn av redegjørelsen over må det antakelig legges til grunn at *hele kundelister* vil kunne utgjøre forretningshemmeligheter etter straffeprosessloven § 124. Etter departementets syn fremstår det imidlertid mer tvilsomt om *enkeltstående kunders navn, kontaktinformasjon og opplysninger om deres plassering av fysiske utstyr i datasenteret* kan regnes som forretningshemmeligheter i straffeprosesslovens forstand. Departementet har derfor gjort en vurdering av om opplysninger om enkeltstående kunders navn, kontaktopplysninger og plassering av fysisk utstyr i datasenteret er omfattet av vernet etter straffeprosessloven § 124.

Departementet har vurdert om opplysninger om identiteten til enkeltstående kunder oppfyller vilkåret om kommersiell verdi som følge av hemmelighold eller at hemmelighold har konkurransemessig betydning. Oversikter over en samlet kundemasse vil klart nok kunne ha en verdi for konkurrerende virksomheter ved at

informasjonen om kundene er satt sammen og systematisert, slik at konkurrerende virksomheter får rask og enkel tilgang til opplysninger om mange relevante kunder. En slik oversikt over et marked kan innebære en betydelig ressurs og arbeidsbesparelse. Det er imidlertid vanskeligere å se hvordan opplysninger om én kundes navn og kontaktinformasjon kan gi konkurrenter et konkurransefortrinn.

Videre er det en sentral og uttalt begrunnelse for vernet om forretningshemmeligheter at man søker å forhindre at næringsaktører skaffer seg urettmessige konkurransefordeler gjennom tilgang til resultater av andres innsats, investeringer, prøving og feiling, jf. Prop. 5 LS (2019–2020) side 26. Etter departementets syn treffer ikke denne begrunnelsen normalt på informasjon om enkeltstående kunders identitet og kontaktopplysninger, i motsetning til hva som kan være tilfellet for hele eller større deler av kundelister.

Endelig stiller departementet spørsmål om opplysninger om enkeltstående kunders navn og kontaktopplysninger er omfattet av vilkåret om at opplysningene er spesifikke for den enkelte virksomheten, jf. tilsvarende uttalelser i Irgens-Jensen. Bedriftens hemmelighet – og rettighet? Universitetsforlaget, 2010, side 200–201. Det kan også vises til spesialmerknaden til straffeloven § 207, jf. Ot.prp. nr. 22 (2008–2009), hvor departementet i tilknytning til omtalen av kravet om at opplysningene er foretaksspesifikke uttaler følgende:

> «Det er klart nok at en ansatt ikke kan kopiere over på en minnepinne eller lignende hele eller store deler av sin tidligere arbeidsgivers kunderegister, for å benytte seg av dette hos sin nye arbeidsgiver. Men det vil på den annen side ikke være straffbart å kontakte kunder man husker fra tidligere, og drive markedsføring overfor disse.»

Etter departementets syn vil kunnskap om at noen kjøper en datasentertjeneste i mange tilfeller kunne ligge tett opp mot allmenn viten, eller vil være informasjon som er lett tilgjengelig, all den tid datasentertjenester er en del av den digitale grunnmuren til svært mange bedrifter.

Spørsmålet om opplysninger om kunders navn og kontaktinformasjon utgjør en forretningshemmelig må antakelig vurderes konkret, og det vil være relevant hvor mange kunder det er snakk om. Som tidligere nevnt avgrenses det mot mer ubetydelige opplysninger, og opplysningene må ha en faktisk eller potensiell verdi for virksomheten eller markedet.

Informasjon om identiteten til enkeltkunder kan riktignok oppfattes som sensitiv av datasenteroperatøren og som nevnt være underlagt en avtalebasert taushetsplikt. Eksistensen av en slik avtaleregulering er imidlertid ikke i seg selv avgjørende for hva som regnes som en forretningshemmelighet etter straffeprosessloven § 124, men klausuler om konfidensialitet vil kunne oppfylle kravet om at det er truffet rimelige tiltak for å holde opplysningene hemmelige, jf. Prop. 5 LS (2019–2020) side 120.

6.2.2.5 *Beslag og utleveringspålegg i avvergende øyemed*

Det er en snever adgang til å beslutte beslag eller utleveringspålegg for å avverge enkelte alvorlige straffbare handlinger etter straffeprosessloven § 222 d.

Avvergende tvangsmiddelbruk etter § 222 d må skje «som ledd i etterforskning». Dette innebærer at etterforskning etter straffeprosessloven § 224 må være

besluttet, i tillegg til at det må det være rimelig grunn til å tro at noen kommer til å begå en av de straffbare handlingene som er nevnt i § 222 d.

De straffbare handlingene som kan kvalifisere til beslag eller utleveringspålegg i avvergende øyemed er begrenset til et knippe alvorlige handlinger, herunder terrorhandlinger, terrortrusler og drap. I tillegg kan grove narkotikaovertredelser som omfatter en betydelig mengde og grovt ran begrunne avvergende tvangsmiddelbruk, forutsatt at handlingene utøves som ledd i aktivitetene til en organisert kriminell gruppe. PST er etter straffeprosessloven § 222 d andre ledd gitt en videre adgang til å benytte tvangsmidler i avvergende øyemed enn politiet for øvrig, jf. punkt 7.2 i dette notatet.

Når beslag og utleveringspålegg benyttes for å avverge en straffbar handling, kreves det i tillegg at tvangsmiddelbruken vil gi opplysninger av vesentlig betydning for å kunne avverge handlingen, og at avverging ellers i vesentlig grad ville ha blitt vanskeliggjort, jf. § 222 d tredje ledd første punktum. Avgjørelse om avvergende tvangsmiddelbruk fattes av retten ved kjennelse, men påtalemyndigheten er gitt hastekompetanse dersom det er fare ved opphold, jf. § 222 d fjerde ledd første punktum. Det stilles formkrav til påtalemyndighetens ordre, og slik ordre skal snarest mulig – og senest innen 24 timer – bringes inn for retten for godkjennelse.

6.2.3 Andre hjemler for utlevering av informasjon til politiet og påtalemyndigheten

Lovverket inneholder også enkelte andre regler om utlevering av informasjon om kunder til politiet eller påtalemyndigheten. Ingen av disse hjemlene omfatter krav om utlevering av opplysninger om en datasenteroperatørs kunder. Departementet vil likevel redegjøre for enkelte utleveringsregler rettet mot andre bransjer som eksempler på særlige løsninger som er valgt ved behov for utlevering av kundeinformasjon.

Ekomloven § 3-10 tredje og fjerde ledd er et eksempel på en regel som gir politiet og påtalemyndigheten adgang til å kreve utlevering av informasjon om kunder både i og utenfor etterforskning. Bestemmelsen gir tilgang til abonnementsinformasjon fra tilbyder eller installatør av elektronisk kommunikasjonsnett eller -tjeneste, og utgjør en selvstendig hjemmel for utlevering av abonnementsopplysninger og IP-data som er lagret til tilbyderens drifts- og faktureringsformål. Det er her tale om utlevering av «identifikasjonsopplysninger/abonnementsopplysninger», jf. Prop. 49 L (2010–2011) punkt 17.3, og bestemmelsen er dermed avgrenset mot opplysninger som sier noe om innholdet eller andres bruk av elektronisk kommunikasjon. For identifikasjonsopplysninger er det for politiet ikke nødvendig å få rettens tillatelse eller fritak fra taushetsplikten fra Nasjonal kommunikasjonsmyndighet etter straffeprosessloven § 118.

Et annet eksempel på en bestemmelse som hjemler utlevering av kundeopplysninger er straffeprosessloven § 210 tredje ledd. I medhold av denne bestemmelsen kan påtalemyndigheten pålegge vitner som har taushetsplikt etter finansforetaksloven § 9-6 eller § 9-7, verdipapirhandelloven § 10-5 eller verdipapirsentralloven § 8-1 å utlevere dokumenter eller andre ting som antas å ha betydning som bevis og som omfattes av taushetsplikten eller taushetsplikt etter avtale. Det er ikke krav om foregående eller etterfølgende beslutning fra

domstolen. Begrunnelsen for innføringen av regelen var dels prosessøkonomiske betraktninger og dels at regelen ville tilrettelegge for raskere informasjonsinnhenting i saker hvor det kan være avgjørende å få innhentet informasjonen (for eksempel om bruken av et bankkort) hurtig, jf. Ot.prp. nr. 59 (2003–2004) side 51. Dersom sterke allmenne hensyn tilsier at forklaring gis, gjelder forklaringsplikten etter straffeprosessloven § 210 tredje ledd uten hensyn til om det er åpnet etterforskning i straffesak. Dette siste alternativet tar særlig sikte på forsvinningssaker «hvor det kan være grunn til å frykte at noe har tilstøtt den savnede», jf. Ot.prp. nr. 59 (2003–2004) side 53 og 59.

6.3 Departementets vurderinger og forslag

Dersom datasenteroperatøren får en plikt til å ha tilgjengelig oppdatert kundeinformasjon, jf. forslagene i høringsnotatet punkt 4.3, vil reglene i straffeprosessloven om beslag og utleveringspålegg kunne benyttes for å innhente denne kundeinformasjonen.

Som det fremgår av redegjørelsen for gjeldende rett ovenfor, forutsetter bruken av beslag og utleveringspålegg at betingelsene for å iverksette etterforskning etter straffeprosessloven § 224 foreligger, samt at de respektive vilkårene for tvangsmidlene er oppfylt. For at beslag i disse tilfellene skal være et anvendelig tiltak, må politiet ha fysisk tilgang til kundeinformasjonen og vite hvor den befinner seg. Fysisk tilgang til kundeinformasjonen kan forutsette tredjemannsransaking, og uansett være utfordrende dersom politiet ikke vet hvor kundeinformasjonen befinner seg eller den ligger lagret på en databærer som er beskyttet med passord. Utleveringspålegg synes derfor å være et egnet tiltak dersom kundeinformasjonen ikke utleveres frivillig. Påtalemyndigheten har som nevnt hastekompetanse til å utferdige utleveringspålegg, men et slikt pålegg forutsetter uansett beslutning fra retten, enten før tiltaket settes i verk eller snarest mulig etterpå forutsatt at det ved opphold er fare for at etterforskningen vil lide.

Dersom formålet med utleveringspålegget eller beslaget er å avverge en straffbar handling, må tiltaket hjemles i straffeprosessloven § 222 d. De straffbare handlingene som kan begrunne beslag eller utleveringspålegg i avvergende øyemed er imidlertid begrenset til et knippe svært alvorlige handlinger, herunder drap og terrorhandlinger. Departementet antar at det er andre typer kriminalitet som primært ønskes avverget gjennom tilgang til kundeinformasjon i datasentre enn de som kan begrunne anvendelse av straffeprosessloven § 222 d.

Dersom politiet derimot griper inn for å avverge eller stanse lovbrudd *utenfor etterforskning*, jf. politiloven § 7 første ledd nummer 3, har de som tidligere nevnt ikke hjemler til å pålegge utlevering av kundeinformasjon i dag.

Etter departementets vurdering synes det på bakgrunn av det ovenstående å være behov for en hjemmel for at politiet og påtalemyndigheten kan få utlevert kundeinformasjon fra en datasenteroperatør når det er nødvendig for å stanse eller avverge et lovbrudd. Det synes å være i disse situasjonene at behovet for rask informasjonstilgang er størst. Departementet foreslår derfor at politiet og påtalemyndighet gis tilgang til kundeinformasjonen når det er nødvendig for å stanse eller avverge et lovbrudd rettet mot eller ved bruk av servere eller lignende utstyr i et datasenter.

Departementet foreslår at bestemmelsen skal kunne brukes både i og utenfor etterforskning. I etterforskning vil en slik hjemmel oppstille noe lempeligere vilkår enn for utleveringspålegg og beslag. Det er ikke krav til skjellig grunn til mistanke om en straffbar handling, og det kreves ikke forutgående eller etterfølgende beslutning fra retten, slik det gjør for utleveringspålegg. I tillegg vil både påtalemyndigheten og politiet ha kompetanse til å pålegge utlevering av kundeinformasjonen. Hvem i politiet og påtalemyndigheten som bør ha slik kompetanse, drøftes nærmere i punkt 10.2 nedenfor. Videre vil en slik hjemmel gi tilgang til kundeinformasjon også i tilfeller der det er rimelig grunn til å tro at noen kommer til å begå en handling og kriminalitetskravene i straffeprosessloven § 222 d ikke er oppfylt. Utenfor etterforskning kan bestemmelsen anvendes når politiet utfører sine oppgaver etter politiloven § 7 første ledd nummer 3. Departementet viser til redegjørelsen i punkt 6.2.3 for andre hjemler som gir politi og påtalemyndighet tilgang til kundeinformasjon i og utenfor etterforskning og med lempeligere vilkår enn beslag og utleveringspålegg.

Departementet understreker at den foreslåtte bestemmelsen ikke er ment å påvirke vurderingen av om innhentingen av kundeinformasjonen fra datasenteroperatøren er å regne som etterforskning. Politiet og påtalemyndigheten må i det konkrete tilfellet vurdere om innhenting av informasjon med hjemmel i den foreslåtte bestemmelsen er å regne som etterforskning, med utgangspunkt i begrepet om etterforskning slik det er kommet til uttrykk i riksadvokatens rundskriv nummer 3/1999 samt Prop. 68 L (2015-2016) side 176–177 og Ot.prp. nr. 60 (2004–2005) side 42–43.

Utlevering av kundeinformasjon kan som tidligere nevnt tenkes å omfatte *forretningshemmeligheter*. I og med at den foreslåtte plikten til å utlevere informasjon kun gjelder datasentre som tilrettelegger for at kunder innplasserer fysisk utstyr, jf. punkt 4.3 ovenfor, antar departementet at det i de fleste tilfeller kun vil være behov for utlevering av opplysninger om én eller et svært begrenset antall enkeltkunder. Det vil eksempelvis være liten risiko for «smitte» til andre kunder i et slikt datasenter dersom én kunde er rammet av et angrep, og det vil derfor som regel ikke være behov for informasjon om andre kunder i en slik situasjon. Departementet legger på bakgrunn av dette til grunn at det ikke vil være aktuelt å be om informasjon om et større antall eller alle kundene til en datasenteroperatør i medhold av utkastet til § 1-5 første ledd.

Departementet går videre ut fra at informasjon om navn, kontaktopplysninger og fysisk plassering vedrørende én eller et par enkeltkunder som den klare hovedregel ikke vil aktualisere vernet av forretningshemmeligheter etter straffeprosessloven § 124, jf. redegjørelsen i punkt 6.2.2.4 ovenfor, men ber særlig om høringsinstansenes syn på dette. Etter departementets syn kan forslaget til utleveringshjemmel i § 1-5 uansett ikke brukes til å innhente forretningshemmeligheter i strid med vernet i straffeprosessloven § 124. Dette innebærer at det vil ligge begrensninger på adgangen til å benytte regelen for å innhente opplysninger om et større antall kunder. Dette kommer til uttrykk i forslaget til tilgangshjemmel, som for politiet og påtalemyndigheten er begrenset til informasjon *om én eller enkelte angitte kunder* når og i det omfang det er nødvendig for å stanse eller avverge et lovbrudd.

Politiets videre behandling av opplysningene som hentes inn i medhold av forslaget til § 1-5 første ledd, vil reguleres av politiregisterloven og

politiregisterforskriften, som gjennomfører direktiv (EU) 2016/680 om fysiske personers vern i forbindelse med kompetente myndigheters behandling av personopplysninger med sikte på å forebygge, etterforske, avsløre eller rettsforfølge straffbare handlinger eller fullbyrde strafferettslige sanksjoner. Direktivets regler er på en del punkter sammenfallende med personvernforordningen, men med tilpasninger på grunn av særlige behov ved kriminalitetsbekjempelse. Politiregisterloven stiller blant annet krav til informasjonssikkerhet, internkontroll og sporbarhet for bruk av opplysninger, jf. lovens §§ 15, 16 og 17 og nærmere regler i forskriften. I tillegg stilles det krav om tjenestemessig behov for tilgang til opplysninger, jf. § 21, og krav om at opplysninger ikke skal oppbevares lenger enn nødvendig for formålet, jf. § 50.

7 Utlevering av kundeinformasjon til PST

7.1 Bakgrunn

PST skal etter politiloven § 17 b forebygge og etterforske nærmere angitte straffbare handlinger. Som for politiet for øvrig er ansvaret og oppgavene PST er tillagt de samme i det fysiske og det digitale rom, og det er forventet at PST skal kunne utføre sine lovpålagte oppgaver også i det digitale rom. Som følge av de svært alvorlige straffbare handlingene tjenesten har i oppgave å forebygge, og at den overveiende delen av PSTs arbeid skjer i det forebyggende sporet, gjør det seg gjeldende særskilte behov for denne tjenesten.

PST kan motta informasjon om at noen forbereder straffbare handlinger med tilknytning til datasentre på flere måter. PST kan for eksempel få opplysninger fra samarbeidende tjenester om at en virksomhet eller en server i et datasenter brukes av personer som samarbeider med fremmed etterretningstjeneste eller som planlegger sabotasjehandlinger eller terrorvirksomhet.

I slike tilfeller vil informasjon om hvorvidt en aktør er kunde hos et datasenter kunne være en nødvendig forutsetning for tjenestens ytterligere informasjonsinnhenting for å avklare informasjonens troverdighet og vurdere om det bør settes i verk tiltak. Uten kundeinformasjon fra datasenteroperatøren, vil PST ikke kunne berike opplysningene de har fått med informasjon fra andre kilder, som åpent tilgjengelig informasjon, registersøk og forespørsler til andre samarbeidende tjenester om informasjon.

7.2 Gjeldende rett

Politiloven § 17 b angir hvilke straffbare handlinger PST skal forebygge og etterforske. Dette er blant annet overtredelser av straffeloven kapittel 17 om vern av Norges selvstendighet og andre grunnleggende nasjonale interesser, ulovlig etterretningsvirksomhet, spredning av masseødeleggelsesvåpen, sabotasje og terrorisme. Reglene om beslag og utlevering i straffeprosessloven som det er redegjort for i punkt 6.2 ovenfor gjelder også når PST etterforsker straffbare handlinger som nevnt i politiloven § 17 b.

Som eneste politiorgan er PST i medhold av politiloven § 17 d gitt anledning til å benytte skjulte tvangsmidler, herunder skjult ransaking, skjult beslag og skjult utleveringspålegg, jf. straffeprosessloven §§ 200 a, 208 a og 210 a, i forebyggende

øyemed. PST kan av retten få tillatelse til å benytte skjulte tvangsmidler dersom det er grunn til å undersøke om noen forbereder en handling som rammes av:

a. straffeloven §§ 131, 133 og 134, [terrorhandlinger, terrorforbund og terrortrusler]
b. straffeloven §§ 121 til 126 eller § 130 a, [etterretningsvirksomhet, avsløring av statshemmeligheter og grov påvirkning fra fremmed etterretning]
c. straffeloven § 142, [ulovlig befatning med farlig materiale]
d. straffeloven §§ 251, 254, 256, 263, 273 eller 275 [tvang, frihetsberøvelse, forbund om grov frihetsberøvelse, trusler, kroppsskade og drap] og som retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater.

Dersom det er grunn til å undersøke om noen forbereder disse straffbare handlingene, kan PST dermed få utlevert kundeinformasjon fra datasentrene dersom retten gir tillatelse til skjult beslag eller skjult utleveringspålegg. Kravet om at det må være «grunn til å undersøke» om noen forbereder en handling som nevnt i bestemmelsen innebærer både et saklighetskrav, et krav om en viss sannsynlighet for at noe er under oppseiling og et krav til forholdsmessighet, jf. Innst. O nr. 113 (2004–2005) side 35.

Tillatelse til forebyggende tvangsmiddelbruk kan bare gis dersom det er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen, at forebygging ellers i vesentlig grad vil bli vanskeliggjort og inngrepet etter sakens art og forholdene ellers ikke fremstår som uforholdsmessig, jf. § 17 d andre ledd. Sjefen for PST er gitt hastekompetanse til å beslutte tvangsmiddelbruk, med unntak av romavlytting, dersom det ved opphold er stor fare for at muligheten til å forebygge et forhold som nevnt i første ledd bokstav a eller d vil gå tapt, jf. tredje ledd. Det stilles – som for avvergende tvangsmiddelbruk etter straffeprosessloven § 222 d – formkrav til beslutningen og krav om etterfølgende fremleggelse for retten. For handlinger som nevnt i politiloven § 17 d første ledd bokstav b og c har sjefen for PST ikke slik hastekompetanse, og det kreves alltid forutgående kjennelse fra retten.

Opplistingen av hvilke straffebud som kan begrunne tvangsmidler i det forebyggende sporet er snevrere enn de straffebudene som PST er satt til å forebygge. Begrunnelsen for dette er at politiloven § 17 d åpner for at svært inngripende tvangsmidler kan benyttes på et tidspunkt der det ikke foreligger holdepunkter for at den som inngrepet retter seg mot, har begått eller er i ferd med å begå noe straffbart.

PST kan benytte tvangsmidler i avvergende øyemed etter straffeprosessloven § 222 d andre ledd i langt flere tilfeller enn i det forebyggende sporet, for eksempel for å avverge sabotasjehandlinger og brudd på en rekke bestemmelser i straffeloven kapittel 17. PST er gitt videre adgang til avvergende tvangsmiddelbruk enn det alminnelige politiet. Opplistingen av straffebud i straffeprosessloven § 222 d andre ledd er likevel avgrenset til de mest alvorlige straffbare handlingene som omfattes av politiloven § 17 b første ledd, jf. Ot.prp. nr. 60 (2004–2005) side 128–131.

7.3 Departementets vurderinger og forslag

Forslaget om hjemler for utlevering av kundeinformasjon til politiet for å avverge eller stanse straffbare handlinger i forrige punkt vil også omfatte utlevering til PST. Dersom datasenteroperatøren får en plikt til å ha tilgjengelig oppdatert

kundeinformasjon, jf. forslagene i høringsnotatet punkt 4.3, vil PST også kunne benytte tvangsmidler etter politiloven § 17 d for å innhente denne kundeinformasjonen i forebyggende øyemed, dersom vilkårene for dette er oppfylt.

For de straffebud der PST har hjemmel til å bruke forebyggende tvangsmidler, kan det være et betydelig hasteelement i saken. I slike tilfeller vil en eventuell hjemmel for uthenting av kundeinformasjon, med lempeligere vilkår, innebære en tidsbesparelse som kan være av stor betydning for muligheten til å forebygge lovbruddet. Dette gjelder særlig ved forebygging av ulovlig etterretning eller spredning av masseødeleggelsesvåpen, jf. politiloven § 17 d første ledd bokstav b og c, der sjefen for PST ikke har hastekompetanse til å beslutte tvangsmiddelbruk. I disse sakene må PST få rettens forutgående godkjenning til tvangsmiddelbruken, selv om det er stor fare for at muligheten til å forebygge lovbruddet går tapt.

Videre er adgangen til å benytte skjulte tvangsmidler i det forebyggende sporet som omtalt i punkt 7.2 snever. En rekke straffebud der kundeinformasjon fra en datasenteroperatør kan være nødvendig for å forebygge den straffbare handlingen vil falle utenfor opplistingen i politiloven § 17 d. Noen eksempler på svært alvorlige straffebud innenfor PSTs mandat som ikke er nevnt i politiloven § 17 d er angrep på de høyeste statsorganenes virksomhet, inngrep overfor viktige samfunnsinstitusjoner, anslag mot infrastrukturen og fremkalling av fare for allmennheten, jf. straffeloven §§ 115, 117, 192 og 355. Dette er handlinger som kan begås med digitale virkemidler, og dermed begås både mot og fra et datasenter. Etter dagens regelverk har PST ikke mulighet til å få tilgang til kundeinformasjon fra en datasenteroperatør selv om det er grunn til å undersøke om noen forbereder slike handlinger.

Samlet sett foreslås det derfor en hjemmel for at PST kan innhente kundeinformasjon fra datasenteroperatører i forebyggende øyemed, og slik innhenting vil kunne være nødvendig til forebygging innenfor hele PSTs ansvarsområde. Det synes ikke hensiktsmessig å skille ut spesifikke straffebud fra politiloven § 17 b som kan begrunne utlevering av kundeinformasjon. Det legges vekt på graden av sensitivitet i informasjonen og at utleveringsplikten begrenses til datasenteroperatører som tilbyr datasentertjenester mot vederlag og til informasjon om en eller flere bestemte kunder. Det innebærer at PST ikke vil kunne få utlevert informasjon om alle datasenteroperatørens kunder etter bestemmelsen. På samme måte som etter forslaget til ny forskriftsbestemmelse § 1-5 første ledd, vil det heller ikke for PST etter andre ledd være adgang til å benytte den foreslåtte regelen om utleveringsplikt til å innhente informasjon som anses som forretningshemmeligheter etter straffeprosessloven § 124.

Det er behov for – og forutsatt i forskriftshjemmelen i ekomloven § 3-7 femte ledd – at utleveringen rammes inn. Det foreslås derfor ikke å åpne for at PST kan få utlevert informasjon kun fordi det er nødvendig for forebygging generelt. Dette ville legge terskelen for lavt. Forebygging er et vidt begrep som kan romme en rekke ulike situasjoner og handlinger, slik at det ikke nødvendigvis egner seg som et utløsende vilkår. I stedet foreslås det at PST kan få utlevert informasjon dersom det er «grunn til å undersøke» om noen forbereder en handling som nevnt i politiloven § 17 b. Kravet skal forstås på samme måte som i politiloven § 17 d første ledd. Det innebærer som nevnt i punkt 7.2 både et saklighetskrav, et krav om en viss sannsynlighet for at noe er under oppseiling, og et krav til

forholdsmessighet. Det må være konkrete objektive omstendigheter som tilsier at noen forbereder en handling som angitt. Det er ikke tilstrekkelig å vise til informasjon, erfaringer og vurderinger mer generelt. Vilkåret er relativt i forhold til handlingens alvor, slik at det skal mindre til for at kravet er oppfylt dersom det dreier seg om svært alvorlige handlinger (som terror og drap) enn handlinger av lavere alvorlighetsgrad (som trusler mot myndighetspersoner).

I tillegg til terskelen for utlevering vil de nærmere kravene til påleggets innhold, avgrensning av informasjon som skal utleveres og til beslutningskompetanse, jf. punkt 10, også gjelde for PSTs pålegg om utlevering av opplysninger.

PSTs videre behandling av de utleverte opplysningene reguleres av politiregisterloven kapittel 11 og politiregisterforskriften del 6. Ettersom opplysninger som behandles i PSTs forebyggende virksomhet i det alt vesentlige er sikkerhetsgraderte, vil også sikkerhetsloven gjelde.

Foruten internkontroll og departementets overordnede styring fører Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) kontroll med PST. Utvalgets kontroll av PST skal sikre at virksomheten holdes innenfor rammen av tjenestens fastlagte oppgaver og føre kontroll med tjenestens behandling av forebyggende saker og etterforskningssaker, dens bruk av skjulte tvangsmidler og andre skjulte metoder for informasjonsinnhenting, jf. EOS-kontrolloven § 6 fjerde ledd nummer 1. PSTs innhenting av kundeinformasjon fra datasenteroperatører vil dermed bli kontrollert av EOS-utvalget som ledd i utvalgets alminnelige kontroll med PST.

8 Utlevering av kundeinformasjon til NSM

8.1 Bakgrunn

NSM har som hovedoppgave å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. NSM har blant annet ansvar for å drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur, jf. sikkerhetsloven § 2-4 første ledd. Det nasjonale varslingssystem (VDI) skal avdekke og varsle om cyberoperasjoner mot digital infrastruktur. Nasjonalt cybersikkerhetssenter (NCSC) er den nasjonale responsfunksjonen for alvorlige digitale angrep og Norges nasjonale CERT (Computer Emergency Response Team).

I forbindelse med utførelsen av sine oppgaver etter sikkerhetsloven § 2-4 har NSM behov for tilgang til kundeinformasjon for blant annet å kartlegge omfanget av et angrep og skaffe en oppdatert situasjonsforståelse. I tillegg kan det være viktig med slik informasjon i et skadebegrensende øyemed ved at andre kunder kan varsles om angrepet og settes i stand til å gjøre sikkerhetstiltak. Videre kan informasjon om kunder være viktig for å sikre at en mulig konsentrasjon av samfunnskritiske kunder i samme eller et fåtall datasentre håndteres riktig.

8.2 Gjeldende rett

NSM har etter gjeldende rett ikke hjemmel til å pålegge en datasenteroperatør å utlevere informasjon om hvem som er kunder i et datasenter.

Etter sikkerhetsloven § 2-2 andre ledd bokstav c skal NSM blant annet *innhente* og vurdere informasjon som har betydning for forebyggende sikkerhetsarbeid. NSM er avhengig av å få tilgang til et bredt informasjonsgrunnlag om trusselbildet og hendelser fra de ulike virksomhetene og sektorene for å kunne vurdere og analysere sikkerhetstilstanden innenfor lovens virkeområde, jf. Prop. 153 L (2016–2017) side 53. Bestemmelsen gir imidlertid ikke hjemmel for NSM til å *pålegge utlevering* av informasjon.

Sikkerhetsloven § 2-2 fjerde ledd bestemmer at NSM skal, så langt det er nødvendig for å gjennomføre oppgavene i eller i medhold av loven, gis *uhindret adgang* til skjermingsverdig informasjon, informasjonssystem, objekt eller infrastruktur. Bestemmelsen er begrenset til å gjelde i forebyggende sikkerhetsarbeid og kun for informasjon som er skjermingsverdig etter sikkerhetsloven § 5-1, skjermingsverdige informasjonssystemer etter § 6-1 eller skjermingsverdige objekter og infrastruktur etter § 7-1.

Som nevnt har NSM ansvar for å drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur, jf. sikkerhetsloven § 2-4. I forskrift 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften) kapittel 11 er det gitt nærmere bestemmelser om det nasjonale varslingssystemet.

Det følger av forarbeidene at både responsfunksjonen og varslingssystemet har et bredere nedslagsfelt enn sikkerhetslovens virkeområde, jf. Prop. 153 L (2016–2017) side 168. I forbindelse med denne oppgaven skal informasjon om digitale angrep *innhentes*, analyseres og deles, jf. virksomhetsikkerhetsforskriften § 63. Hva som ligger i innhentingsbegrepet er ikke angitt i forskriften.

Departementet viser til at en rekke andre forvaltningsorganer i spesiallovgivningen er gitt kompetanse til å pålegge private å gi opplysninger til myndighetene. Dette er for eksempel tilfellet for skattemyndighetene etter skatteforvaltningsloven § 10-2 første ledd, Datatilsynet etter personopplysningsloven § 23 første ledd, tollmyndighetene etter tolloven § 10-1 første ledd, Arbeidstilsynet etter arbeidsmiljøloven § 18-5 første ledd og Finanstilsynet etter finanstilsynsloven § 3 andre ledd. Etter ekomloven § 15-2 første ledd kan departementet kreve opplysninger fra enhver – inkludert personopplysninger – når det er nødvendig for å gjennomføre bestemmelsene i ekomloven, vedtak gitt i medhold av ekomloven eller forpliktelser som følger av internasjonale avtaler. En lignende regulering av utleveringsplikt er inntatt i konkurranseloven § 24 første ledd.

Utleveringspliktene i annen lovgivning overfor andre myndigheter er gjennomgående knyttet til opplysninger som er nødvendige eller av betydning for at det aktuelle organet kan utøve sin myndighet eller sine oppgaver etter loven. Ut over den rammen er det imidlertid få andre begrensninger med hensyn til arten av opplysningene eller hvem som plikter å gi opplysninger. Flere av hjemlene om utleveringsplikt åpner dessuten for unntak fra lovbestemt taushetsplikt.

8.3 Departementets vurderinger og forslag

En rekke virksomheter er avhengige av datasentre. Bortfall eller forringelse av datasentertjenester vil kunne skape store utfordringer, herunder for grunnleggende nasjonale funksjoner og virksomheter som understøtter dette. I et datasenter vil

nivået på risikoen bestemmes av verdien av den produksjonen som utføres og de konsekvensene som oppstår om en hendelse skulle inntreffe.

Et helt sentralt element i NSMs utøvelse av responsfunksjonen etter sikkerhetsloven § 2-4 er innhenting, verifisering, analyse og videreformidling av informasjon om sårbarheter, potensielle risikoer, angrepsmetoder og ondsinnet kode. Dette skjer dels gjennom Nasjonalt varslingssystem for digital infrastruktur (VDI), men også gjennom mottak av informasjon fra nasjonale og internasjonale samarbeidspartnere.

Under en hendelseshåndtering av et digitalt angrep vil tilgang til kundeinformasjon ha betydning for at NSM skal få kartlagt omfanget av angrepet samt skaffe seg en oppdatert situasjonsforståelse. I tillegg vil en tilgang til kundeinformasjon være viktig i et skadebegrensende øyemed ved at det blir mulig å kartlegge risiko for øvrige kunder i et datasenter. I det siste ligger at kundeinformasjon vil kunne bidra til å avdekke og identifisere om det forekommer lateral (sideveis) bevegelse fra en kompromittert kunde til andre kunder. I tilfeller hvor flere kunder deler internettleveranse eller har annet felles nettverksutstyr, for eksempel som en del av datasenterets styrings- og kontrollsystem, kan angrep mot en kunde få en smitteeffekt mot andre kunder. Oversikt over kunder er også viktig for tilfeller der det vil være nødvendig å varsle en eller flere kunder om angrepet. Kundeinformasjon kan også være nødvendig for å finne årsaken til et digitalt angrep, samt hvilke aktører som står bak.

Det er også nødvendig for NSM å kunne få oppdaterte oversikter over hvem som er kunder i et datasenter under en hendelse for å kunne sikre at en mulig konsentrasjon av samfunnskritiske kunder i samme eller et fåtall datasentre håndteres på en god måte. Konsentrasjonsrisikoen kan være stor, avhengig av hvilke kunder som befinner seg i datasenteret, og om kunden er en samfunnskritisk virksomhet. Særlig de samfunnskritiske virksomhetene må settes i stand til å gjøre egne vurderinger av sikkerheten.

Det er etter departementets oppfatning behov for en bestemmelse som gir NSM tilgang til kundeinformasjon når og i det omfang det er nødvendig for å drive den nasjonale responsfunksjonen ved alvorlige digitale angrep og det nasjonale varslingssystemet for digital infrastruktur etter sikkerhetsloven § 2-4.

For at NSM skal kunne ivareta sitt ansvar etter sikkerhetsloven § 2-4, foreslår departementet som nevnt i punkt 5 at NSM skal kunne gi pålegg om utlevering av informasjon fra både datasenteroperatør nevnt i ekomloven § 1-5 nummer 38 bokstav a og bokstav b. Dette har sammenheng med at digitale angrep kan ramme begge disse kategoriene av datasenteroperatører, og at NSMs behov for tilgang til kundeinformasjon derfor gjør seg gjeldende uavhengig av hvordan datasenteroperatøren driver sin virksomhet. Videre har ikke NSM hjemmel til å få tilgang til kundeinformasjon fra datasenteroperatør på samme måte som politiet og PST gjennom bruk av straffeprosessuelle tvangsmidler. Vernet av forretningshemmeligheter etter straffeprosessloven § 124 gjelder ikke ved utlevering til NSM, se punkt 6.2.2.4 og 6.3. Departementet viser for øvrig til redegjørelsen for andre forvaltningsorganers hjemler for å pålegge utlevering av informasjon i punkt 8.2.

Den foreslåtte utleveringshjemmelen for NSM angir både arten av informasjonen som skal gis til NSM: kundeinformasjon, jf. nærmere om hvilken informasjon

dette vil være i utkastet § 1-4, samt at formålet med informasjonsinnhentingen konkretiseres til å være å drive den nasjonale responsfunksjonen ved alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur etter sikkerhetsloven § 2-4 for å kunne kartlegge omfanget av et cyberangrep.

Departementet viser til at kundeinformasjon som NSM får tilgang til, vil behandles i tråd med reglene i forvaltningsloven. Det innebærer blant annet at tjenestepersoner som får kjennskap til kundeinformasjonen kan bli underlagt taushetsplikt etter forvaltningsloven § 13 første ledd nummer 2 dersom de utleverte opplysningene er omfattet av denne bestemmelsen. For behandling av personopplysninger viser departementet til omtalen i punkt 3.

9 Utlevering av kundeinformasjon til Nkom

9.1 Bakgrunn

Datasentre representerer kjernen i den digitale infrastrukturen i Norge, og er en integrert del av vår kritiske digitale infrastruktur på lik linje med ekomnett og -tjenester. Gjennom ny ekomlov og datasenterforskrift stilles det nå krav til forsvarlig sikkerhet i datasentre.

Med hjemmel i sikkerhetsloven, fører NSM tilsyn med virksomheter som er omfattet av sikkerhetsloven, jf. sikkerhetsloven § 3-1 første ledd. Etter andre ledd kan departementet bestemme at myndigheter med sektoransvar skal føre tilsyn med virksomheter som er omfattet av loven. Det er Nkom som er sektortilsynsmyndighet for datasentre. NSM og Nkom har flere samarbeidsarenaer og utfører også enkelte tilsyn sammen. For Nkom som tilsynsmyndighet for datasentre vil det være viktig å ha informasjon om datasenteroperatørenes kunder som et ledd i vurderingen av datasenterets betydning og kritikalitet, for således å kunne tilpasse kravene til forsvarlig sikkerhet. Dette gjelder både i relasjon til ekomloven og sikkerhetsloven.

Det vises også til omtalen under punkt 8 ovenfor om NSMs behov for kundeinformasjon i hendelseshåndteringsøyemed. De samme begrunnelser gjør seg gjeldende for Nkoms håndtering av hendelser i datasentersektoren.

9.2 Gjeldende rett

Etter sikkerhetsloven § 1-3 skal ansvarlig departementet innenfor sitt ansvarsområde fatte vedtak om at sikkerhetsloven skal gjelde for virksomheter som oppfyller vilkårene i bokstav a til c. Etter bokstav a er det virksomheter som behandler sikkerhetsgradert informasjon. Bokstav b gjelder for virksomheter som råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller som har avgjørende betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon. Etter bokstav c omfattes virksomheter som driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller som har avgjørende betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon.

Digitaliserings- og forvaltningsdepartementet kan innenfor sitt ansvarsområde fatte vedtak om at sikkerhetsloven kapittel 10 om eierskapskontroll skal gjelde for

virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner, eller virksomheter som har vesentlig betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon.

For datasentre er Digitalisering- og forvaltningsdepartementet ansvarlig departement i tilknytning til sikkerhetsloven § 1-3. I tillegg er Digitaliserings- og forvaltningsdepartementet etter sikkerhetsloven § 2-1 ansvarlig for forebyggende sikkerhetsarbeid innenfor sitt ansvarsområde, herunder datasentre, og skal blant annet identifisere og holde oversikt over grunnleggende nasjonale funksjoner, jf. bokstav a. Etter bokstav b skal også Digitaliserings- og forvaltningsdepartementet identifisere og holde oversikt over virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser.

Digitaliserings- og forvaltningsdepartementet skal blant annet melde inn oversikter til sikkerhetsmyndigheten etter bokstav a og b og vedtak etter bokstav c, jf. sikkerhetsloven § 2-1 første ledd bokstav d.

Nkom bistår departementet i å ivareta sektoransvaret etter sikkerhetsloven, og Nkom er derfor avhengig av en rekke informasjonskilder for å kunne ivareta dette ansvaret.

9.3 Departementets vurderinger

Ny ekomlov stiller krav til sikkerhet og beredskap i datasenter, jf. ekomloven § 3-7 med tilhørende datasenterforskrift som trådte i kraft 1. januar 2025. Nkom er sektormyndighet med tilsynsansvar etter ekomloven for elektroniske kommunikasjonsnett og -tjenester. Med den nye ekomloven har Nkom også fått delegert det samme ansvaret for datasentersektoren.

Digitaliserings- og forvaltningsdepartementet har i dag hjemmel i ekomloven § 15-2 til å kunne kreve utlevert de opplysningene de trenger for å gjennomføre sine oppgaver etter ekomloven. Nkom har fått delegert samme hjemmel til å kreve utlevert nødvendige opplysninger fra datasenteroperatør.

Sikkerhetsloven stiller ytterligere krav til sikkerhet og vil gjøres gjeldende for datasentre som har avgjørende betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 1-3. For å kunne avgjøre om et datasenter har slik avgjørende betydning, vil det kunne være viktig å ha kjennskap til hvem som er kunder hos datasenteroperatøren da dette vil kunne vektlegges i vurderingen av om datasenteret er av avgjørende betydning eller ikke.

Det samme behovet for kundeinformasjon gjør seg gjeldende i vurderingen av om datasenteret er av «vesentlig betydning» etter sikkerhetsloven § 1-3 andre ledd.

Det fremgår av ny ekomlov § 15-2 første ledd at Digitaliserings- og forvaltningsdepartementet kan kreve opplysninger fra enhver når det er nødvendig for å sikre effektiv gjennomføringen av ekomloven, forskrifter og enkeltvedtak. Siden bestemmelsen er begrenset til utlevering av informasjon når det er nødvendig for å gjennomføre bestemmelsene i ekomloven, er departementets vurdering at bestemmelsen ikke kan benyttes til å pålegge utlevering av kundeinformasjon for å identifisere virksomheter som vurderes underlagt sikkerhetsloven. Ekomloven § 15-2 kan dermed ikke anvendes for informasjonsinnhenting når departementet skal fatte vedtak om hvilke private virksomheter som bør omfattes av reguleringen i sikkerhetsloven, jf.

sikkerhetsloven § 1-3. I den grad departementet eller Nkom trenger kundeinformasjon for å vurdere de ulike datasentrenes viktighet eller kritikalitet i sikkerhetslovsammenheng, kan ekomloven § 3-7 femte ledd benyttes som hjemmel for å oppstille en plikt i forskrift til utlevering av kundeinformasjon til departementet eller Nkom, jf. femte ledd siste punktum om at departementet «kan gi forskrift om nasjonal sikkerhet og kriminalitetsbekjempelse i datasenter, herunder [..]».

For å være i stand til å identifisere om et datasenter har den betydningen at den bør omfattes av sikkerhetsloven, vil det etter vårt syn derfor være vesentlig å få tilgang til informasjon om kunder i et datasenter. For eksempel kan det tenkes at flere virksomheter som er underlagt sikkerhetsloven er lokalisert i samme datasenter, og at bortfall av tjenesten vil kunne få store konsekvenser. Selv om datasenteroperatør etter datasenterforskriften § 1-3 andre ledd nummer 8 skal registrere en oversikt over kommunale, fylkeskommunale og statlige kunder, er det etter vår mening ikke tilstrekkelig til å vurdere om et datasenter skal underlegges sikkerhetsloven. Tilgang til kundelister kan derfor få betydning for at Digitaliserings- og forvaltningsdepartementet og Nkom skal kunne oppfylle sitt ansvar etter sikkerhetsloven.

Som en del av en hendelseshåndtering i et datasenter kan det være nødvendig å kreve utlevering av kundeinformasjon om kunder som er plassert fysisk nært hverandre. Hendelseshåndtering i sektoren forvaltes av Nkom, og for hendelser knyttet til cyber er det EkomCERT som koordinerer og følger utviklingen. EkomCERT jobber tett med blant annet Nasjonalt cybersikkerhetssenter (NSM NCSC) og andre sektor-responsmiljøer i Norge.

Kundens fysiske plassering i et datasenter kan være avgjørende ved fysiske innbrudd, uautorisert adgang og kompromittering av adgangskontrollsystemer. Videre kan det være nødvendig å avklare eventuell kundekonsekvens av strømutfall og manglende kjøling. Dersom flere kunder deler internettleveranse eller har annet felles nettverksutstyr kan angrep mot en kunde få en smitteeffekt mot andre, og det kan være nødvendig å kontakte denne eller disse kunden(e) for å avgjøre eventuell konsekvens.

EkomCERT har spisskompetanse på sårbarhets- og trusselbildet generelt, og sektorspesifikke utfordringer spesielt. EkomCERT følger det generelle trussel- og sårbarhetsbildet gjennom innhenting av data fra åpne og lukkede kilder og samarbeidspartnere. Her kan kundeinformasjon ha en betydelig verdi.

Fordi det er en manglende hjemmel i eksisterende regelverk, jf. redegjørelsen ovenfor, er det departementets vurdering at det er behov for å foreslå en bestemmelse som gir Nkom tilgang til kundeinformasjon for å ivareta sitt ansvar etter sikkerhetsloven, samt for at EkomCERT skal kunne ivareta sitt ansvar ved en hendelseshåndtering i et datasenter. Ved alvorlige digitale hendelser yter EkomCERT bistand i form av informasjonsinnhenting, rådgivning og koordinering.

10 Nærmere om utformingen av hjemlene for utlevering av kundeinformasjon

10.1 Ytterligere vilkår for utlevering av informasjon

Det er kundeinformasjon som på nærmere vilkår skal utleveres til politiet eller påtalemyndigheten, PST, NSM eller Nkom i henhold til forslaget til ny § 1-5 i datasenterforskriften. Rammene for hvilke typer opplysninger som kan være gjenstand for utlevering, fremgår av forslaget til § 1-4.

Etter departementets oppfatning bør det oppstilles ytterligere vilkår for utleveringsplikten. Etter departementets syn bør det for politiet og påtalemyndigheten, NSM og Nkom oppstilles et vilkår om at tilgang til kundeinformasjon i det enkelte tilfelle må være «nødvendig» for å oppnå det aktuelle formålet beskrevet i § 1-5. Vilkåret er skjønnsmessig, og vil kreve at myndigheten som gir pålegget gjør konkrete vurderinger i det enkelte tilfellet. Videre foreslås det at utlevering kun kan kreves «i det omfang» det er nødvendig for å oppnå formålene. På denne måten begrenses også mengden informasjon som skal utleveres i det enkelte tilfellet. Vilkårene er nærmere beskrevet i merknadene til de enkelte bestemmelsene i høringsnotatet kapittel 15.

Også PSTs informasjonsinnhenting etter forslaget til § 1-5 andre ledd bør rammes inn gjennom ytterligere vilkår. For PSTs del foreslår departementet imidlertid å legge listen noe lavere enn et krav om nødvendighet, slik at det kreves at det er grunn til å tro at informasjonen er av betydning for å forebygge en handling som nevnt i bestemmelsen. Kravet innebærer at PST må ha konkrete holdepunkter for at kundeinformasjonen vil være av betydning for å forebygge handlingen, men det kreves ikke sannsynlighetsovervekt. At opplysningene må være av betydning, innebærer at det ikke kan innhentes opplysninger som er mer perifere eller mindre viktige for å forebygge handlingen. Det foreslås ikke et tilsvarende vilkår om at tilgang kun skal gis «i det omfang» det er behov for opplysningene. Dette innebærer imidlertid ikke at det åpnes for at PST kan pålegge utlevering av informasjon om flere kunder enn det er grunn til ut fra formålet. Departementet ber særskilt om høringsinstansenes syn på dette punktet.

10.2 Kompetansen til å pålegge utlevering av informasjonen

Etter departementets oppfatning er det grunn til å angi hvilket nivå i det enkelte myndighetsorganet som skal kunne gi pålegg om utlevering av kundeinformasjon. På den ene siden vil det sikre kontroll med myndighetsutøvelsen dersom kompetansen ligger på et høyt nivå i organet. Ved pågående hendelser, for eksempel pågående digitale angrep eller andre straffbare handlinger fra eller i et datasenter, vil imidlertid hasteelementet ofte være fremtredende. Det vil derfor være nødvendig at beslutninger kan treffes raskt. Departementet mener at disse hensynene best kan ivaretas ved at lederen av det aktuelle myndighetsorganet eller den denne bemyndiger kan beslutte krav om utlevering av kundeinformasjon. En slik løsning er også skissert i Prop. 93 LS (2023–2024) side 281. Der heter det blant annet at krav om tilgang «skal gjøres skriftlig for eksempel av leder for politidistriktene eller EOS-tjenestene eller den disse bemyndiger».

På bakgrunn av vurderingen ovenfor vil det være politimester, leder av det aktuelle særorganet i politiet, sjef PST, direktøren av NSM og direktøren av Nkom som kan

gi pålegg om utlevering. Deres myndighet til å pålegge utlevering av kundeinformasjon vil som nevnt kunne delegeres til andre i organisasjonen. En slik løsning sikrer at beslutningen om å pålegge utlevering av opplysninger treffes på et tilstrekkelig høyt nivå, samtidig som det sikres en viss fleksibilitet ved at kompetansen kan delegeres. Ved at lederen for det aktuelle organet gis mulighet til å delegere sin kompetanse, vil de foreslåtte reglene sikre at myndighetene raskt gis tilgang til den aktuelle informasjonen. Når kompetansen må delegeres, bidrar dette like fullt til at vurderinger av hvem som skal kunne kreve utlevering av informasjonen er forankret høyt i organisasjonen.

10.3 Krav til påleggets form og innhold

Etter departementets oppfatning bør det oppstilles krav til formen og innholdet i pålegget om utlevering av kundeinformasjon. Slike krav vil sikre at pålegget i tilstrekkelig grad blir individualisert, og at datasenteroperatøren får muligheter til å sette seg inn i og rette seg etter pålegget. Krav til påleggets innhold bidrar videre til å sikre at det ikke gis unødvendige pålegg og at vilkårene for utlevering blir tilstrekkelig vurdert. I tillegg vil krav til påleggets innhold også kunne understøtte mekanismene for tilsyn og kontroll med behandlingen av opplysningene i etterkant.

Departementet har sett hen til kravene som stilles til anmodninger om utlevering av IP-informasjon etter ekomloven § 3-14, og foreslår at pålegg om utlevering av kundeinformasjon skal være skriftlig og så vidt mulig opplyse om hva saken gjelder, formålet med pålegget og hva det omfatter. I tillegg må det fremgå av pålegget at vilkårene for utlevering er vurdert. Det kreves ikke at det gis noen nærmere redegjørelse i pålegget for hvorfor vilkårene er oppfylt, kun at det fremgår at vilkårene er vurdert.

Angivelsen av hva pålegget omfatter, vil opplyse datasenteroperatøren konkret om hvilke opplysninger som etterspørres og sikre at det ikke utleveres flere opplysninger enn det som er nødvendig.

Det kan være behov for å begrense informasjonen som blir gitt til datasenteroperatøren av hensyn til etterforskningen av en straffesak eller fordi opplysningene er graderte etter sikkerhetsloven. Det foreslås derfor at kravet *så vidt mulig* skal opplyse om hva saken gjelder. For PSTs del vil det ofte ikke være mulig å utgi informasjon om bakgrunnen for pålegget, da informasjonen vil være gradert. Begrunnelsen vil i disse tilfellene måtte gis på et overordnet nivå, for eksempel at informasjonen er nødvendig fordi det er grunn til å undersøke om noen forbereder en handling nevnt i politiloven § 17 b.

Myndighetene som fremsetter pålegget om utlevering, vil være best egnet til å vurdere hvilken informasjon om saken som kan gis til datasenteroperatøren.

10.4 Adgangen til å overprøve et pålegg om utlevering av informasjon

Forvaltningsloven § 14 gjelder pålegg om å gi opplysninger, og inneholder særlige regler om begrunnelse, klage og iverksettelse. Slike avgjørelser blir trolig regnet som enkeltvedtak når det treffes uavhengig av en forvaltningssak som allerede pågår, jf. NOU 2019: 5 *Ny forvaltningslov* punkt 26.2. Forvaltningsloven § 14 regulerer klageadgangen for beslutningen om krav om utlevering fra NSM og Nkom, men også politiet og PST når beslutningen treffes utenfor etterforskning.

Dersom pålegg om å utlevere informasjon gis av NSM, vil Justis- og beredskapsdepartementet være klageinstans, jf. forvaltningsloven § 28 første ledd. Det samme gjelder der pålegget gis av PST. For å unngå at Justis- og beredskapsdepartementet blir klageinstans i nye sakstyper, vil Justis- og beredskapsdepartementet arbeide videre med spørsmålet om rollen som klageinstans kan ivaretas av et annet organ. Når politiet innhenter informasjon utenfor etterforskning, vil Politidirektoratet være klageinstans. For klage på pålegg gitt av Nkom vil det være Digitaliserings- og forvaltningsdepartementet som er klageinstans.

Det følger av forvaltningsloven § 14 andre punktum at et pålegg om å gi opplysninger kan påklages dersom man mener at man ikke har plikt eller lovlig adgang til å etterkomme pålegget. Denne klageretten gjelder uavhengig av om pålegget anses som et enkeltvedtak eller ikke, jf. Marius Stub, Karnov lovkommentar til forvaltningsloven § 14 note 4 i Lovdata Pro (2023) hentet 16. oktober 2024. Det skal videre opplyses om klageadgangen i forbindelse med pålegget. Klagen fremsettes for det forvaltningsorganet som har truffet vedtaket, jf. forvaltningsloven § 32 første ledd bokstav a jf. § 14 i.f. Departementet kan ikke se at det er behov for å gi særregler om klageadgangen for pålegg etter den foreslåtte regelen i datasenterforskriften § 1-5.

Etter forvaltningsloven § 14 femte punktum har en klage i utgangspunktet oppsettende virkning. Den pålegget retter seg mot, kan i så fall vente med å etterkomme pålegget om å gi opplysninger til klagen er avgjort. Hvis forvaltningsorganet som har pålagt å gi opplysninger «finner det påtrengende nødvendig for å gjennomføre sine oppgaver etter loven», kan forvaltningsorganet kreve at opplysningene utgis før klagesaken er avgjort. Det er altså det forvaltningsorganet som krever opplysningene som avgjør spørsmålet om klagen skal gis oppsettende virkning, jf. Ot.prp. nr. 38 (1964–65) *Om lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)* side 55. Forvaltningskomiteen uttalte at en klage ikke vil ha oppsettende virkning «dersom det fremstiller seg som nødvendig å få opplysningene straks for å sikre at bevis ikke forspilles eller fordi opplysningene trengs til uoppsettelige tiltak», jf. NUT 1958: 3 *Innstilling fra Komiteen til å utrede spørsmålet om mer betryggende former for den offentlige forvaltning* side 172. Det er derfor «ikke nok at kontrollen i og for seg ville bli mer effektiv eller at myndighetene ville bli spart for bry og kostnader om tiltaket kunne settes i verk straks», jf. Ot.prp. nr. 38 (1964–65) side 56.

For andre vedtak er utgangspunktet motsatt: Underinstansen, klageinstansen eller annet overordnet organ kan beslutte at vedtaket ikke skal iverksettes før klagefristen er ute eller klagen er avgjort, jf. forvaltningsloven § 42 første ledd. Det kan derfor spørres om det er grunn til å regulere oppsettende virkning særskilt i datasenterforskriften, slik at pålegget kan iverksettes også når det er gjenstand for klage. En tilsvarende løsning er gitt i skatteforvaltningsloven § 10-13. Formålet med utleveringen av opplysningene fra en datasenteroperatør er imidlertid å forhindre eller begrense skadene av en nært forestående eller pågående digital hendelse. Departementet antar derfor at myndighetene som oftest vil kunne finne det «påtrengende nødvendig» at opplysningene gis før en klagesak er avgjort. Ellers vil hovedregelen om oppsettende virkning i stor grad kunne forspille formålet med pålegget.

Når det gjelder utlevering til PST fordi det er grunn til å undersøke om noen forbereder en straffbar handling, vil det antakeligvis være noen flere tilfeller der klagen gis oppsettende virkning. Imidlertid vil det også på det forebyggende feltet kunne være situasjoner der formålet vil kunne forspilles dersom klagen gis slik virkning. På bakgrunn av dette antar departementet at regelen om oppsettende virkning i forvaltningsloven § 14 ikke vil føre til betydelige forsinkelser, eller at formålet med pålegget forspilles i tilfeller hvor det er et hasteaspekt ved hendelsen i datasenteret. Departementet foreslår derfor ikke en særregel om oppsettende virkning i datasenterforskriften.

Når politiet og påtalemyndigheten treffer beslutninger under etterforskning, følger overprøvingsmulighetene av straffeprosessloven. Ved beslag og utleveringspålegg i medhold av reglene i straffeprosessloven vil domstolen på ulike vis kunne bringes inn til enten forhånds- eller etterkontroll av bruken av tvangsmiddelet, jf. punkt 6.2.1.

For utlevering av informasjon til politiet eller påtalemyndighet under etterforskning etter den foreslåtte regelen i § 1-5 første ledd, foreslås det ingen adgang til domstolskontroll. Dette har en sammenheng med at formålet med den foreslåtte regelen er at blant annet politiet og påtalemyndigheten raskt og på noe lempeligere vilkår skal gis tilgang til kundeinformasjonen. Hvilke rettssikkerhetsgarantier som er nødvendig, har en sammenheng med arten og intensiteten av inngrepet. Departementet viser i denne forbindelse til vurderingene i punkt 3 og 6.3 av blant annet inngrepets omfang, behovet for rask informasjonstilgang samt prosessøkonomiske hensyn.

Retten til å klage på påtalevedtak er lovregulert i straffeprosessloven § 59 a. Et krav om utlevering av informasjon vil ikke være omfattet av noen av vedtakene som er positivt listet opp i første ledd i bestemmelsen. Utenfor vedtakstypene som er nevnt i § 59 a første ledd, har riksadvokaten i rundskriv bestemt at enkelte påtaleavgjørelser alltid skal tas til behandling ved klage i kraft av overordningsforholdet, jf. rundskriv, jf. RA-2020-2 punkt 9.2, RA-2002-4 punkt X og RA-1996-2 punkt IV. Krav om utlevering av informasjon i medhold av den foreslåtte forskriftshjemmelen vil heller ikke være omfattet av retningslinjene fra riksadvokaten. I kraft av overordnet påtalemyndighets omgjørings- og instruksjonsadgang vil overordnet påtalemyndighet uansett ha en adgang til å ta til behandling en avgjørelse fra underordnet påtalemyndighet, jf. RA-1996-2 punkt VI 1. Overordnet påtalemyndighet kan eksempelvis bli gjort oppmerksom på påtaleavgjørelsen gjennom en henvendelse fra private. Klager har ikke oppsettende virkning, med mindre dette er uttrykkelig fastsatt av enten underordnet påtalemyndighet eller klageinstansen, jf. RA-1996-2 punkt V. Klagen bør fremsettes overfor den myndigheten som har truffet det påklagede vedtaket, jf. punkt IV i samme rundskriv.

Etter departementets oppfatning bør det tas utgangspunkt i reglene om og systematikken for overprøving av påtalevedtak som følger av straffeprosessloven. Av den grunn foreslås det ikke særregler om klage over politiet eller påtalemyndighetens pålegg om utlevering av informasjon som utferdiges under etterforskning.

11 Krav om at datasenteroperatøren skal ha en tilgjengelig fysisk representant i Norge

11.1 Bakgrunn

Politiet og NSM kan ha behov for å komme i kontakt med en datasenteroperatør av flere ulike årsaker. Blant annet vil det være behov for slik kontakt dersom politiet avverger, stanser eller for øvrig etterforsker straffbare handlinger som er rettet mot eller utføres fra servere i et datasenter. Dersom det er aktuelt å iverksette tvangsmidler under etterforskning av kunder i et datasenter, vil det for eksempel være behov for kontakt med operatøren for å få tilgang til senteret og vite hvor i senteret kunden er lokalisert. Også NSM og Nkom vil ha tilsvarende behov når myndighetene håndterer alvorlige digitale angrep. Nkom vil også ha behov for å komme i kontakt med datasenteroperatør for å ivareta sine oppgaver etter sikkerhetsloven.

Om det er mulig å komme i kontakt med datasenteroperatøren, vil variere i dagens situasjon. Politiet har erfaring med at det kan være vanskelig å komme i kontakt med enkelte operatører. Etter det departementet erfarer, har de fleste aktører i datasenterbransjen representanter som er fysisk til stede i datasenteret eller som kan møte opp i løpet av kort tid. Politiet beskriver imidlertid også situasjoner der det ikke er noen personer til stede i et datasenter, eller der personen som er til stede ikke har kunnskap om senteret, nødvendige språkkunnskaper eller fullmakt til å bistå myndighetene. Ut fra dette situasjonsbildet er det behov for en regel som pålegger datasenteroperatører å ha en representant som kan møte opp fysisk på datasenterets lokasjon i Norge og som har nødvendige fullmakter og kunnskap om senteret.

11.2 Gjeldende rett

Det følger av ekomloven § 3-7 femte ledd tredje punktum at departementet i forskrift kan fastsette krav om at datasenteroperatøren skal ha en tilgjengelig representant med nødvendig kunnskap om datasenteret. Med «nødvendig kunnskap» siktes det til at representanten skal ha den kunnskapen som trenges for å kunne bistå politiet eller EOS-tjenestene slik at tilgangen politiet eller EOS-tjenestene skal ha til datasentrene og informasjonen i eller i medhold av ekomloven eller annet regelverk blir reell, jf. Prop. 93 LS (2023–2024) side 281.

Etter ekomloven § 3-7 første ledd og datasenterforskriften § 1-3 har en datasenteroperatør plikt til å registrere seg hos Nkom før virksomheten starter opp. I datasenterforskriften § 1-3 andre ledd er det gitt bestemmelser om hva en melding om registrering skal inneholde. Etter andre ledd nummer 6 skal registreringen blant annet inneholde kontaktinformasjon til en representant for datasenteroperatøren som kan møte opp med fysisk med fullmakter og kunnskap til å følge opp henvendelser fra myndighetene.

11.3 Departementets vurderinger og forslag

Som beskrevet ovenfor følger det allerede av gjeldende datasenterforskrift § 1-3 andre ledd nummer 6 at datasenteroperatøren skal registrere kontaktinformasjon til en representant hos Nkom. Representanten skal kunne møte opp fysisk med fullmakter og kunnskap til å kunne følge opp henvendelser fra myndighetene. Etter

departementets syn er det imidlertid behov for å presisere kravene til representanten.

Under henvisning til behovet som er beskrevet i punkt 11.1, mener departementet at kravene til representanten bør reguleres i en egen bestemmelse i datasenterforskriften § 1-6, der kravene kan utdypes. En utførlig og presis angivelse av hvilke krav som stilles til den fysiske representanten vil kunne bidra til forutsigbarhet for datasenteroperatører.

Departementet foreslår derfor at ny § 1-6 viderefører kravet i datasenterforskriften § 1-3 andre ledd nummer 6. Departementet foreslår videre at kravene spesifiseres, og at det uttrykkelig fremgår at datasenteroperatør skal ha en representant som er til stede i Norge. Representanten skal kunne møte opp fysisk og ha nødvendig fullmakt og kunnskap til å kunne følge opp henvendelser fra myndighetene, herunder pålegg om utlevering etter § 1-5. Videre skal representanten kunne bistå myndighetene som nevnt i § 1-5 med deres gjennomføring av tiltak som har hjemmel i lov eller forskrift gitt i medhold av lov og som skal ivareta hensynet til kriminalitetsbekjempelse eller nasjonal sikkerhet. Plikten til å bistå i forbindelse med gjennomføring av tiltak er dermed begrenset til tiltak som skal ivareta hensynet til nasjonal sikkerhet eller kriminalitetsbekjempelse. Departementet viser i denne forbindelse til uttalelsene i Prop. 93 LS (2023–2024) side 281 om at representanten skal ha den kunnskapen som trengs for å kunne bistå politiet eller EOS-tjenestene slik at tilgangen politiet eller EOS-tjenestene skal ha til datasentrene og informasjonen i eller i medhold av ekomloven eller annet regelverk blir reell. Aktuelle tilgangshjemler kan for eksempel være tvangsmidler hjemlet i straffeprosesslovens fjerde del. Straffeprosessloven oppstiller detaljerte vilkår og rettsikkerhetsgarantier for de ulike tvangsmidlene. Felles for alle er at de bare kan brukes når det er tilstrekkelig grunn til det, og at de ikke brukes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep, jf. § 170a. Som eksempel på tiltak nevnes ransaking etter § 192 følgende og beslag etter § 203 følgende. Ransaking forutsetter i utgangspunktet beslutning av retten, men dersom det er fare ved opphold, kan beslutningen treffes av påtalemyndigheten, jf. § 197. I alvorlig saker kan retten gi tillatelse til kommunikasjonskontroll etter straffeprosessloven kapittel 16a eller dataavlesning etter kapittel 16 d.

Forslaget til ny § 1-6 må videre ses i sammenheng med uttalelsene i proposisjonen side 281 om at departementet i forskrift kan stille krav om at datasenteroperatøren skal registrere en representant som er *tilgjengelig*. Departementet kan ikke se at et slikt krav om tilgjengelighet kan ivaretas ved at representanten er lokalisert i et annet land enn Norge eller på en annen kant av landet enn der datasenteret ligger. For myndighetene er det av avgjørende betydning at representanten kan komme til datasenteret innen rimelig tid slik at tilgang til bygningen vil kunne oppnås raskt, for eksempel i tilfeller hvor formålet er å avverge eller stanse en straffbar handling eller dersom nasjonale sikkerhetsinteresser er truet.

12 Krav til responstid

Etter gjeldende rett skal datasenteroperatøren som tidligere nevnt registrere kontaktinformasjon til en representant for datasenteroperatøren som kan møte opp fysisk med fullmakter og kunnskap til å følge opp henvendelser fra myndighetene, jf. datasenterforskriften § 1-3 andre ledd nummer 6. Det er imidlertid ikke gitt

regler om hvor raskt datasenteroperatøren eller den fysiske representanten skal følge opp henvendelser fra myndighetene.

Etter departementets oppfatning bør forskriftsteksten inneholde føringer for hvor raskt datasenteroperatøren må etterkomme et pålegg om utlevering av informasjon eller en henvendelse om bistand. En uttrykkelig fristregel vil kunne bidra til forutsigbarhet for både myndighetene og datasenteroperatøren. Som det fremgår av punkt 6–9 i dette høringsnotatet, vil politiet, PST, NSM og Nkom regelmessig ha behov for rask tilgang til datasenteroperatørens kundeinformasjon, blant annet for å stanse eller avverge lovbrudd eller håndtere alvorlige digitale hendelser i datasentre. Hasteaspektet ved disse situasjonene taler med styrke for at fristen for å etterkomme pålegg er nokså kort. Den særskilte regelen om fristen for å etterkomme pålegg fra myndighetene må også ses i sammenheng med forslaget om at datasenteroperatøren skal ha en tilgjengelig representant, jf. punkt 11 ovenfor og forslaget til ny § 1-6 i datasenterforskriften.

Departementet erkjenner samtidig at det kan være noen ulemper ved å oppstille en kort og absolutt frist. For at datasenteroperatøren skal kunne etterleve sine forpliktelser etter forslaget uten at det pålegges for stor belastning, vil en viss fleksibilitet i fristregelen være hensiktsmessig.

På bakgrunn av dette foreslår departementet at datasenteroperatøren innenfor normal arbeidstid skal etterkomme pålegg om utlevering av kundeinformasjon etter forslaget til ny § 1-5 «uten ugrunnet opphold». Det samme gjelder bistand til gjennomføring av tiltak som nevnt i forslaget til ny § 1-6. Utenfor normal arbeidstid skal datasenteroperatøren ha beredskap for på kort varsel å følge opp henvendelser etter første ledd i saker som haster av hensyn til kriminalitetsbekjempelse eller nasjonal sikkerhet. Formuleringen vil sikre en viss fleksibilitet i det enkelte tilfellet, samtidig som det klare utgangspunktet er at datasenteroperatøren raskt skal gi myndighetene tilgang til de aktuelle opplysningene etter at de har mottatt pålegget om utlevering.

13 Plikt for datasenteroperatør til å registrere informasjon om navn på eier av bygning etter datasenterforskriften § 1-3

13.1 Bakgrunn

Trusselaktører bruker bevisst ulike økonomiske virkemidler for å få innpass i verdikjeder, og det er viktig at myndighetene har mulighet til å fange dette opp og gjøre vurderinger av konsekvensene, jf. Prop. 95 L (2022–2023) *Endringer i sikkerhetsloven (eierskapskontroll og lovens virkeområde)* side 6.
Datasentertjenester er en del av en verdikjede for en digital tjeneste. Slike tjenester leveres fra fysiske lokasjoner. Datasenteroperatører kan eie bygningen selv, eller det kan være inngått kontrakt om leie av bygningen. En eier av bygningen kan ha stor mulighet til å påvirke verdikjeden, for eksempel når det gjelder strømforsyning og fysiske tiltak.

13.2 Gjeldende rett

Etter ekomloven § 3-7 første ledd har en datasenteroperatør plikt til å registrere seg hos departementet før virksomheten starter opp. I datasenterforskriften § 1-3 er det gitt bestemmelser om hva en melding om registrering skal inneholde.

13.3 Departementets vurderinger og forslag

Departementet foreslår at datasenteroperatøren i forbindelse med registreringen av datasentervirksomheten også skal melde inn navn på eier av bygning hvor datasenteroperatøren er lokalisert, jf. datasenterforskriften § 1-3 andre ledd nummer 12. Forslaget er begrunnet i at en bygning er en del av verdikjeden for en digital tjeneste. Bygningen som rommer datasenteret som en tjeneste leveres fra, er en vesentlig del av en slik verdikjede. Eieren av bygningen kan ha stor påvirkningsmulighet over verdikjeden. Departementet mener at det kan være risiko for tilsiktede handlinger med potensielt negative konsekvenser. At Nkom får informasjon om hvem som er eier av bygning hvor datasenteroperatøren er lokalisert, er derfor av betydning.

14 Overtredelsesgebyr

I medhold av ekomloven § 15-12 første ledd bokstav b kan departementet ilegge fysiske personer og foretak overtredelsesgebyr dersom personen, foretaket eller noen som handler på vegne av foretaket, forsettlig eller uaktsomt overtrer forskrift gitt med hjemmel i loven, når det er fastsatt i forskriften at overtredelsen kan medføre overtredelsesgebyr. Overtredelse av enkeltvedtak fastsatt med hjemmel i nærmere angitte bestemmelser i ekomloven kan også gi grunnlag for overtredelsesgebyr, se bokstav c. Departementet er gitt kompetanse til å gi forskrift om hvilke forskriftsbestemmelser om kan føre til overtredelsesgebyr, jf. ekomloven § 15-12 andre ledd. En slik forskriftsbestemmelse er gitt i datasenterforskriften § 3-2. Etter denne bestemmelsen har Nkom myndighet til å ilegge foretak overtredelsesgebyr dersom foretaket eller noen som handler på vegne av det forsettlig eller uaktsomt overtrer nærmere angitte bestemmelser i datasenterforskriften, herunder plikten til å registrere seg etter § 1-3. Ekomloven gir også føringer om utmåling, oppfyllelsesfrister og foreldelse av overtredelsesgebyr, jf. § 15-13. Supplerende regler om overtredelsesgebyr, blant annet om domstolsprøving og orientering om taushetsplikt, følger av kapittel IX i forvaltningsloven. Et pålegg om overtredelsesgebyr regnes som et enkeltvedtak, og er derfor omfattet av de generelle reglene i forvaltningsloven og bestemmelser om saksbehandlingen for enkeltvedtak.

De foreslåtte endringene i datasenterforskriften oppstiller flere handlingsnormer for datasenteroperatørene. Datasenteroperatørene plikter å ha tilgjengelig oppdatert kundeinformasjon, utlevere denne på nærmere angitte vilkår, ha en representant til stede samt etterkomme og besvare enkelte henvendelser fra justis- og ekommyndighetene innen bestemte frister. Handlingsnormene har som formål at de skal bidra til at justis- og ekommyndighetene får nødvendig informasjon til henholdsvis å kunne forebygge, avverge og stanse kriminalitet eller virksomhet som truer nasjonal sikkerhet med tilknytning til et datasenter, ivareta forebyggende sikkerhet og robusthet i datasentre og håndtere hendelser med tilknytning til et datasenter.

Manglende etterlevelse av de foreslåtte pliktene vil derfor kunne vanskeliggjøre justis- og ekommyndighetenes arbeid med å iverksette egnede og nødvendige tiltak for å håndtere uønskede digitale hendelser og kriminalitet i eller med tilknytning til et datasenter. Datasentre er som tidligere nevnt en kritisk infrastruktur i samfunnet, og bortfall av datasentertjenester vil dermed potensielt kunne ha store samfunnsmessige konsekvenser. Etterlevelse av de foreslåtte

handlingsnormene vil derfor også være viktig for samfunnet i stort. Departementet mener på denne bakgrunnen at det er behov for å kunne ilegge overtredelsesgebyr som reaksjonsmiddel mot brudd på de foreslåtte handlingsnormene for å sikre tilstrekkelig etterlevelse av de foreslåtte reglene.

En sentral retningslinje ved valg av virkemidler for å sikre regeletterlevelse er imidlertid at mer inngripende virkemidler ikke bør anvendes hvis samme formålet kan nås gjennom mindre inngripende og tilgjengelige virkemidler, se Prop. 62 L (2015–2016) side 52. Departementet er gitt kompetanse til å ilegge tvangsmulkt for å sikre etterlevelse av krav fastsatt i eller i medhold av ekomloven, se ekomloven § 15-11. I tillegg til kan departementet i medhold av ekomloven § 15-5 gi pålegg om retting eller opphør av ulovlige forhold og fastsette vilkår for å sikre etterlevelse av krav fastsatt i eller i medhold av ekomloven.

Departementet antar at pålegg om retting og tvangsmulkt i en del tilfeller vil kunne være hensiktsmessige reaksjonsformer. Et enkeltvedtak om tvangsmulkt må utformes slik at mulkten ikke begynner å løpe før det har vært mulig å oppfylle plikten, se lignende uttalelser i Prop. 62 L (2015–2016) side 206. Fristen for å etterleve et påbud kan derfor ikke være så kort at det blir umulig å overholde. Handlingsnormene som er foreslått i høringsnotatet er ment å bidra til at de relevante myndighetene får nødvendige opplysninger eller tilgang til datasenteret raskt i saker som haster av hensyn til nasjonal sikkerhet og kriminalitetsbekjempelse. Dersom tvangsmulkt skal være et egnet virkemiddel i disse tilfellene, må det derfor antakelig fastsettes en kort frist for å etterleve plikten. Tvangsmulkt kan også være et egnet virkemiddel i saker med et mindre fremtredende hasteelement. Som virkemiddel er tvangsmulkt er imidlertid fremoverrettet og har som formål å stimulere til at pliktsubjektet ikke begår fremtidige regelbrudd. Etter departementets syn vil det i noen tilfeller også være et sanksjonsbehov, for eksempel hvis datasenteroperatøren ikke kan etterleve de foreslåtte pliktene i forskriften innen en frist som er kort nok til at myndighetene får de nødvendige opplysningene eller tilgang til datasenteret tilstrekkelig raskt i saker som haster. Den foreslåtte endringen av datasenterforskriften § 3-2 vil gi Nkom mulighet til å vurdere hvilken av reaksjonsformene som vil være mest hensiktsmessig og forholdsmessig i det konkrete tilfellet. Departementet mener på den bakgrunn at det er behov for å kunne ilegge overtredelsesgebyr som reaksjonsmiddel mot brudd på de foreslåtte handlingsnormene for å sikre tilstrekkelig etterlevelse av de foreslåtte reglene.

15 Økonomiske og administrative konsekvenser

Forslaget om at datasenteroperatør skal registrere navn på eier av bygning hvor datasenteroperatøren er lokalisert antas ikke å medføre økonomiske og administrative konsekvenser av betydning. Det samme gjelder forslaget om endringen i ordlyden i datasenterforskriften § 1-3 andre ledd nummer 6, det vil si kontaktinformasjonen til datasenteroperatørens fysiske representant.

Forslaget om at datasenteroperatøren skal ha beredskap til å svare ut hastehenvendelser utenfor normal arbeidstid kan medføre økonomiske konsekvenser for datasenteroperatørene. Departementets inntrykk er at mange datasenteroperatører allerede har en fysisk representant i Norge med beredskap for å kunne møte opp på kort varsel. Når det gjelder små datasenteroperatører er denne

antakelsen mer usikker, og vi ber særskilt om høringsinstansenes innspill på dette punktet.

Forslaget om at datasenteroperatøren skal ha tilgjengelig oppdatert informasjon om egne kunder må antas å ha begrensede administrative og økonomiske konsekvenser. Departementet legger til grunn at de fleste datasenteroperatører allerede har en slik oversikt for blant annet å kunne fakturerer sine kunder.

Forslaget om datasenteroperatørens plikt til å utlevere informasjon til politiet, PST, Nkom og NSM vil ikke ha særlige økonomiske og administrative konsekvenser. Avhengig av hastegrad, vil datasenteroperatøren måtte prioritere kravet om utlevering av informasjon, men departementet antar at det sannsynligvis ikke vil medgå spesielt mye tid, eller at det ikke vil være veldig ofte at en datasenteroperatør får slike henvendelser. For politiet, PST, Nkom og NSM vil det innebære noe økt ressursbruk å utarbeide og sende kravet om utlevering av informasjon. I tillegg vil overordnet klageinstans kunne få noen flere oppgaver knyttet til klagebehandling. Hvilket organ som er overordnet klageinstans vil avhenge av hvilket myndighetsorgan som gir pålegg om utlevering av informasjon, jf. redegjørelsen i kapittel 10.4. I sum vil forslaget likevel få begrensede konsekvenser for berørte offentlige myndigheter.

16 Merknader til de enkelte bestemmelsene

Til § 1-3

Andre ledd nummer 6 foreslås endret ved at det inntas at kontaktinformasjonen til «datasenteroperatørens fysiske representant i Norge» skal registreres hos Nasjonal kommunikasjonsmyndighet. Endringen er ment å være en forenkling av ordlyden, slik at de nærmere kravene til den fysiske representanten fremgår av ny § 1-6 i utkastet. Det vises til punkt 11 for en redegjørelse av behovet for en nærmere presisering av kravene til den fysiske representanten.

I *andre ledd* foreslås det inntatt et nytt *nummer 12* hvor det fremgår at datasenteroperatør skal melde inn navn på eier av bygning hvor datasenteroperatøren er lokalisert. Eieren av bygget kan være datasenteroperatøren selv, men det kan også tenkes tilfeller hvor datasenteroperatøren har inngått en husleiekontrakt eller hvor datasenteroperatørens utleier fremleier bygget. Eieren av bygget vil da kunne være utleier eller den som har inngått den opprinnelige husleieavtalen med fremleietakeren. Det vises for øvrig til departementets vurdering i punkt 13.3.

Til § 1-4

Forslaget er omtalt i punkt 4. Paragrafen er ny. *Første ledd* oppstiller en plikt til å ha tilgjengelig oppdatert informasjon om datasenteroperatørens egne kunder, og det er konkretisert i bestemmelsen hvilken informasjon om kunden som er omfattet av denne plikten. Uttrykket «datasenteroperatør» skal forstås som etter ekomloven § 1-5 nummer 38. Plikten etter første ledd påhviler alle datasenteroperatører, jf. ekomloven § 1-5 nummer 38 bokstav a og b. Det vil si at også fysiske og juridiske personer som driver datasenter med abonnert elektrisk effekt over terskelverdien i datasenterforskriften § 2, er omfattet.

Informasjonen om kundene som datasenteroperatøren plikter å ha tilgjengelig, er begrenset til informasjon som er nødvendig for at kunden på en enkel måte kan identifiseres og kontaktes av myndighetene når vilkårene for utlevering etter § 1-5 er oppfylt. Informasjonen må være oppdatert, noe som innebærer at datasenteroperatøren til enhver tid må ha en oversikt over den aktuelle informasjonen om egne kunder. Det kreves imidlertid ikke at informasjonen holdes oppdatert i egne fysiske lister, men at informasjonen for eksempel finnes digitalt.

Andre ledd i bestemmelsen utvider plikten til å ha tilgjengelig kundeinformasjon til også å omfatte opplysninger om hvor kundens fysiske utstyr er plassert i datasenteret. Det er kun datasenteroperatører som tilbyr andre tilgang til datasentertjeneste mot vederlag, jf. ekomloven § 1-5 nummer 38 bokstav a, som må ha tilgjengelig informasjon om plasseringen av det fysiske utstyret. Plikten etter andre ledd vil for eksempel omfatte informasjon om hvor servere, lagringsløsninger, nettverksutstyr og tilkoblingspunkter for slikt utstyr er plassert.

Til § 1-5

Bestemmelsen er ny og innebærer at datasenteroperatøren i visse situasjoner plikter å utlevere kundeinformasjon som nevnt i datasenterforskriften § 1-4 til politiet og påtalemyndigheten, PST, NSM eller Nkom. Behovet for og innholdet i forslaget er nærmere redegjort for i punkt 6, 7, 8 og 9.

Første ledd regulerer vilkårene for utlevering til politiet, herunder PST, og påtalemyndigheten. Datasenteroperatøren skal gi politiet eller påtalemyndigheten tilgang til informasjonen om én eller enkelte angitte kunders navn, deres kontaktopplysninger og plasseringen av deres fysiske utstyr når og i det omfang det er nødvendig for å stanse eller avverge et lovbrudd rettet mot eller ved bruk av utstyr i et datasenter. Med utstyr menes for eksempel servere og nettverksutstyr. Bestemmelsen kan ikke benyttes til å innhente opplysninger som regnes som forretningshemmeligheter etter straffeprosessloven § 124.

I kravet om at informasjonen må være «nødvendig» ligger det for det første et krav om at de aktuelle opplysningene må være egnet for å kunne oppnå formålet. Kravet skal ikke tolkes så strengt at utlevering av opplysningene må være den eneste måten å oppnå formålet på. På den andre siden vil det ikke være tilstrekkelig at opplysningene bare vil kunne lette myndighetens arbeid. Nødvendighetsvilkåret vil kunne få betydning for å begrense omfanget av kunder som det skal utleveres informasjon om. Vurderingen av hva som skal anses som nødvendig må imidlertid være konkret, og det vil være opp til den aktuelle myndigheten å vurdere og konkretisere hvilken kundeinformasjon som er nødvendig for å oppnå det aktuelle formålet.

Det er kun datasenteroperatører som tilbyr andre tilgang til datasentertjeneste mot vederlag, jf. ekomloven § 1-5 nummer 38 bokstav a, som vil ha en plikt til å utlevere informasjon etter datasenterforskriften § 1-5 første ledd. Det vil si at krav på tilgang til kundeinformasjonen til datasenteroperatører som nevnt i ekomloven § 1-5 nummer 38 bokstav b for politiets og påtalemyndighetens del må ha hjemmel i annen lov eller forskrift, for eksempel i straffeprosesslovens regler om beslag og utleveringspålegg.

Etter *andre ledd* skal PST også gis tilgang til informasjon om én eller enkelte angitte kunders navn, deres kontaktopplysninger og plasseringen av deres fysiske

utstyr når det er det er grunn til å undersøke om noen forbereder en handling som nevnt i politiloven § 17 b. Kravet om «grunn til å undersøke» tilsvarer kravet i politiloven § 17 d første ledd om når retten kan gi tillatelse til bruk av skjulte tvangsmidler i forebyggende øyemed, og skal forstås på samme måte. «Grunn til å undersøke» innebærer både et saklighetskrav, et krav om en viss sannsynlighet for at noe er under oppseiling, og et krav til forholdsmessighet. Det må være konkrete objektive omstendigheter som tilsier at noen forbereder en handling som angitt. Selv om forskriftsteksten ikke inneholder et tilsvarende vilkår som etter første ledd om at tilgang skal gis «i det omfang» det er behov for opplysningene, åpner den ikke for at PST kan pålegge utlevering av informasjon om flere kunder enn det er grunn til ut fra formålet.

Kravet i andre ledd om «grunn til å tro» innebærer at PST må ha konkrete holdepunkter for at kundeinformasjonen vil være av betydning for å forebygge handlingen, men det kreves ikke sannsynlighetsovervekt. At opplysningene må være av betydning, innebærer at det ikke kan innhentes opplysninger som er mer perifere eller mindre viktige for å forebygge handlingen. Andre ledd kan ikke brukes av PST for å kreve utlevert opplysninger som anses som forretningshemmeligheter etter straffeprosessloven § 124.

Etter andre ledd vil PST bare kunne gi pålegg om utlevering av kundeinformasjon fra datasenteroperatører som nevnt i ekomloven § 1-5 nummer 38 bokstav a. Krav på tilgang til kundeinformasjonen til datasenteroperatører som nevnt i ekomloven § 1-5 nummer 38 bokstav b vil for PSTs del måtte hjemles i annen lov eller forskrift, eksempelvis i straffeprosesslovens regler om beslag og utleveringspålegg eller politiloven § 17 d om tvangsmiddelbruk i forebyggende øyemed.

Tredje ledd gjelder NSMs tilgang til kundeinformasjon som nevnt i § 1-4. NSM vil kunne gi pålegg om utlevering av informasjon fra datasenteroperatør nevnt i ekomloven § 1-5 nummer 38 bokstavene a og b. Vilkårene må ses i sammenheng med NSMs ansvar for å drive den nasjonale responsfunksjonen ved alvorlige digitale angrep og det nasjonale varslingssystemet for digital infrastruktur etter sikkerhetsloven § 2-4. NSMs tilgang til informasjon vil for eksempel kunne benyttes til å kartlegge omfanget av et cyberangrep og den risikoen angrepet utgjør for øvrige kunder i et datasenter. Vilkåret om at informasjonen må være nødvendig skal forstås likt som etter første ledd i paragrafen.

Fjerde ledd gir Nkom tilgang til kundeinformasjon som nevnt i § 1-4. Nkom vil kunne gi pålegg om utlevering av informasjon fra datasenteroperatør nevnt i ekomloven § 1-5 nummer 38 bokstavene a og b. Vilkårene må sees i sammenheng med Nkoms sektoransvar for datasenternæringen etter sikkerhetsloven. Nkoms tilgang til informasjon må være nødvendig for at myndigheten i utøvelsen av sitt sektoransvar etter sikkerhetsloven for eksempel etter § 1-3 og § 2-1 har behov for å vurdere om et datasenter er av vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser. For at Nkom skal kunne ivareta sitt ansvar i relasjon til ekomCERT, vil det også være av betydning å få tilgang til kundeinformasjon.

I *femte ledd første punktum* reguleres hvem som kan gi pålegg om utlevering av informasjon. Politimesteren, lederen av det aktuelle særorganet i politiet, sjef PST og direktøren av NSM eller direktøren av Nkom kan gi pålegg om utlevering. Deres myndighet kan også delegeres til andre i organisasjonen.

Femte ledd annet og tredje punktum stiller krav til påleggets form og innhold. Kravene samsvarer til dels med kravene som stilles til anmodninger om utlevering av IP-informasjon etter ekomloven § 3-14. For det første skal kravet etter annet punktum være skriftlig og så vidt mulig opplyse om hva saken gjelder, formålet med kravet og hva det omfatter. Angivelsen av hva kravet omfatter, skal konkretisere og opplyse datasenteroperatøren om hvilke opplysninger som etterspørres. Begrensningen «så vidt mulig» tar høyde for at det i enkelte tilfeller ikke vil kunne gis fullstendige opplysninger om hva saken gjelder, for eksempel av etterforskningshensyn eller fordi opplysningene er graderte. Vurderingen av hvilke opplysninger som kan gis ved det enkelte kravet, ligger til myndigheten som krever informasjonen utlevert. Ettersom det vil variere hvem som er klageinstans for et pålegg om utlevering, foreslås det at pålegget også opplyser om hvilken myndighet som er klageinstans. Etter *tredje punktum* skal det fremgå at vilkårene for utlevering av informasjonen er vurdert. Dette kravet gjelder ubetinget. Kravet innebærer ikke at det må gis en utfyllende redegjørelse for vurderingen av hvorfor vilkårene er oppfylt, kun at det må fremgå av pålegget at vilkårene er vurdert. Dette kan eksempelvis gjøres ved en standardformulering.

Til § 1-6

Det vises til redegjørelsen i punkt 11.3. Paragrafen er ny. Bestemmelsen må ses i sammenheng med den foreslåtte endringen av datasenterforskriften § 1-3 andre ledd nummer 6. Kravet om fysisk representant gjelder for datasenteroperatører som nevnt i ekomloven § 1-5 nummer 38 bokstav a og b.

Bestemmelsen oppstiller et krav om at datasenteroperatøren skal ha en representant som er til stede i Norge. Representanten skal videre kunne møte opp fysisk og ha nødvendig fullmakt og kunnskap til å følge opp henvendelser fra myndighetene, herunder pålegg om utlevering etter § 1-5, og til å kunne bistå myndighetene som nevnt i § 1-5 i deres med gjennomføring av tiltak myndighetene har hjemmel til i medhold av gjeldende regelverk.

Dette kravet innebærer for det første at representanten må ha nødvendig kunnskap om datasenteret. Kriteriet «nødvendige» fullmakter vil være oppfylt om representanten har de fullmakter som trengs for å bistå politiet og NSM slik at tilgangen de skal ha etter øvrig regelverk, blir reell. I dette ligger det at representanten må ha fullmakter til å åpne fysiske rom i samme grad som datasenteroperatøren selv basert på hva som er regulert i kundeavtaler, ha en oversikt over kundene og deres fysiske plassering, samt forståelse av og kunnskap om den fysiske infrastrukturen. At representanten har slik fullmakt og kunnskap er viktig for å kunne bistå under hendelsen, undersøke utstyr og ellers ha nødvendig dialog i hendelseshåndteringen.

Den fysiske representanten må være til stede i Norge. Kravet om at representanten skal kunne møte opp fysisk innebærer også at vedkommende må kunne møte opp på datasenterets lokasjon i tråd med de krav til responstid som er satt i § 1-7.

Til § 1-7

Paragrafen er omtalt i punkt 12 og regulerer hvor raskt datasenteroperatøren må etterkomme pålegg om utlevering av informasjon etter § 1-5 og bistå myndighetene med gjennomføring av tiltak som nevnt i § 1-6.

Første ledd regulerer krav til responstid innenfor normal arbeidstid. Innenfor normal arbeidstid skal datasenteroperatøren etterkomme pålegg om utlevering av informasjon etter § 1-5 og bistå myndighetene som nevnt i § 1-6 uten ugrunnet opphold. Ordlyden er valgt for å tydeliggjøre at det er tale om en kort frist, og at informasjonen skal utleveres så raskt som mulig etter at datasenteroperatøren har mottatt pålegget. Kravet om uten ugrunnet opphold er likevel relativt. Hvor raskt datasenteroperatøren må respondere, vil derfor måtte vurderes konkret og vil blant annet avhenge av kravets omfang og kompleksitet. Andre faktorer som vil påvirke hvor raskt operatøren må respondere, er hendelsens alvorlighet og hvor fremtredende hasteelementet er. Kravene til responstid vil derfor skjerpes i saker som haster og i tilfeller hvor det pågår et omfattende og alvorlig angrep mot eller ved bruk av utstyr i datasenteret.

Andre ledd regulerer responstid utenfor normal arbeidstid. Det stilles krav om at datasenteroperatøren har beredskap for på kort varsel å kunne følge opp hastehenvendelser. Bestemmelsen andre punktum forutsetter at representanten følger opp henvendelser fra myndighetene raskt også utenfor arbeidstid, men da begrenset til tilfeller der hasteelementet er begrunnet i hensynet til kriminalitetsbekjempelse eller nasjonal sikkerhet. Det vil være opp til den aktuelle myndigheten å ta stilling til om saken er en hastesak.

Til § 3-2

I § 3-2 er det foreslått å utvide hvilke overtredelser av forskriften eller enkeltvedtak fastsatt med hjemmel i forskriften som kan medføre overtredelsesgebyr. Det vises til omtalen av behovet for overtredelsesgebyr i punkt 14. Overtredelser av plikten til å ha tilgjengelig oppdatert kundeinformasjon i § 1-4, plikten til å utlevere kundeinformasjon etter § 1-5, plikten til å ha en representant etter § 1-6 og plikten til å respondere innen nærmere fastsatte frister etter § 1-7 vil etter forslaget kunne lede til overtredelsesgebyr. Det er bare foretak eller noen som handler på vegne av foretaket som kan ilegges overtredelsesgebyr, og overtredelsen må være enten uaktsom eller forsettlig for at den kan sanksjoneres med overtredelsesgebyr.

Forslag til endringsforskrift

Fastsatt av Digitaliserings- og forvaltningsdepartementet @dato med hjemmel i lov @ om elektronisk kommunikasjon § 3-7.

I

I forskrift @dato nummer @ om datasenter gjøres følgende endringer:

§ 1-3 andre ledd nummer 6 skal lyde:
6. kontaktinformasjonen til *datasenteroperatørens fysiske representant i Norge*

§ 1-3 andre ledd ny nummer 12 skal lyde:
12. navn på eier av bygning der datasenteret er lokalisert

Ny § 1-4 skal lyde:
§ 1-4 *Plikt til å ha oppdatert kundeinformasjon tilgjengelig*

En datasenteroperatør skal ha tilgjengelig oppdatert informasjon om kundenes:

1. navn
2. eventuelle organisasjonsnummer eller rettslige status, form og registreringsnummer dersom kunden er registrert i et handelsregister eller et lignende offentlig register
3. adresse
4. telefonnummer
5. e-postadresse
6. eventuelle nettadresse

En datasenteroperatør som nevnt i ekomloven § 1-5 nummer 38 bokstav a skal også ha tilgjengelig oppdatert informasjon om hvor i datasenteret de enkelte kundenes fysiske utstyr er plassert.

Ny § 1-5 skal lyde:
§ 1-5 *Plikt til å utlevere kundeinformasjon*

Datasenteroperatør som nevnt i ekomloven § 1-5 nummer 38 bokstav a har plikt til å gi politiet eller påtalemyndigheten tilgang til informasjon som nevnt i § 1-4 om én eller enkelte angitte kunder når og i det omfang det er nødvendig for å stanse eller avverge et lovbrudd rettet mot eller ved bruk av utstyr i et datasenter.

Datasenteroperatør som nevnt i ekomloven § 1-5 nummer 38 bokstav a har også plikt til å gi Politiets sikkerhetstjeneste tilgang til informasjon som nevnt i § 1-4 om én eller enkelte angitte kunder når det er det er grunn til å undersøke om noen forbereder en handling som nevnt i politiloven § 17 b og det er grunn til å tro at informasjonen er av betydning for å forebygge handlingen.

Datasenteroperatør som nevnt i ekomloven § 1-5 nummer 38 bokstav a og b har plikt til å gi Nasjonal sikkerhetsmyndighet tilgang til informasjon som nevnt i § 1-4 når og i det omfang det er nødvendig for å drive den nasjonale responsfunksjonen ved alvorlige digitale angrep og det nasjonale varslingssystemet for digital infrastruktur etter sikkerhetsloven § 2-4.

Datasenteroperatør som nevnt i ekomloven § 1-5 nummer 38 bokstav a og b har plikt til å gi Nasjonal kommunikasjonsmyndighet tilgang til informasjon som nevnt i § 1-4 når og i det omfang det er nødvendig for å utføre oppgaver etter sikkerhetsloven.

Pålegget om utlevering av informasjon etter første til fjerde ledd skal fremsettes skriftlig av lederen av det aktuelle organet eller den denne bemyndiger. Pålegget skal så vidt mulig opplyse om hva saken gjelder, formålet med pålegget og hva det omfatter. Pålegget skal også opplyse om hvilken myndighet som er klageinstans. Det skal fremgå at vilkårene for utlevering av informasjonen er vurdert.

Ny § 1-6 skal lyde:
§ 1-6 *Krav om fysisk representant i Norge*

En datasenteroperatør skal ha en representant som er til stede i Norge. Representanten skal kunne møte opp fysisk og ha nødvendig fullmakt og kunnskap til å kunne følge opp henvendelser fra myndighetene, herunder pålegg om utlevering etter § 1-5, og til å kunne bistå myndighetene som nevnt i § 1-5 med deres gjennomføring av tiltak som har hjemmel i lov eller forskrift gitt i medhold av lov og som skal ivareta hensynet til kriminalitetsbekjempelse eller nasjonal sikkerhet.

Ny § 1-7 skal lyde:
§ 1-7 *Krav til responstid*

Innenfor arbeidstid skal datasenteroperatøren etterkomme pålegg etter § 1-5 uten ugrunnet opphold. Det samme gjelder bistand til gjennomføring av tiltak som nevnt i § 1-6.

Utenfor normal arbeidstid skal datasenteroperatøren ha beredskap for på kort varsel å følge opp henvendelser etter første ledd i saker som haster av hensyn til kriminalitetsbekjempelse eller nasjonal sikkerhet.

§ 3-2 lyde skal lyde:

§ 3-2 *Overtredelsesgebyr*

Nasjonal kommunikasjonsmyndighet kan pålegge et foretak overtredelsesgebyr dersom foretaket eller noen som handler på vegne av foretaket, forsettlig eller uaktsomhet

a. overtrer kravene i § 1-3 (Registreringsplikt for datasenteroperatører), *§ 1-4 (Plikt til å ha oppdatert kundeinformasjon tilgjengelig), § 1-5 (Plikt til å utlevere kundeinformasjon), § 1-6 (Krav om fysisk representant i Norge), § 1-7 (Krav til responstid)*, § 2-1 (Krav til sikkerhetsstyring), § 2-2 (Krav om risiko- og sårbarhetsvurderinger), § 2-3 (Krav til grunnsikring og skadebegrensningstiltak), § 2-4 (Krav til sikringsplaner), § 2-5 (Krav om beredskapsplanlegging og -øvelser), § 2-7 (Plikt til å følge opp at andre oppfyller sikkerhetskravene) og § 2-8 (Plikt til å varsle om uønskede hendelser).

b. overtrer enkeltvedtak fastsatt med hjemmel i *§ 1-5 (Plikt til å utlevere kundeinformasjon), § 1-7 (Krav til responstid)*, § 2-6 (Adgang til å pålegge sikkerhetsrevisjon), § 2-9 (Adgang til å pålegge datasentrene å ha nasjonal autonomi) og § 2-10 (Adgang til å pålegge prioritering av tjenestetilbud).

II

Forskriften trer i kraft @.