

Lausunto

02.10.2026

Asia: VN/23332/2026

Työ- ja elinkeinoministeriön lausuntopyyntö luonnoksesta hallituksen esitykseksi eduskunnalle laiksi datakeskusrekisteristä

Lausunnonantajan lausunto

Soveltamisala: 0,5 megawatin raja-arvo ja turvallisuuspoikkeus (1 §)

Raja-arvo on suuruudeltaan perusteltu, mutta oikeusvarmuuden vuoksi laissa on yksilöitävä objektiivinen tapa raja-arvon todentamiseen suunnitelluille, mutta ei vielä rakennetuille datakeskuksille.

Suosittellemme korvaamaan datakeskuksen määritelmän yksiselitteisellä viittauksella EU:n energiatilastoista annettuun asetukseen, kuten on tehty energiatehokkuuslain muutoksen yhteydessä (846/2024 3§). Kyseisen EU-asetuksen määritelmä on sama, joka on kirjoitettu auki hallituksen esitykseen.

Energiatehokkuuslain muutos 846/2024 3 §:

datakeskuksella tarkoitetaan energiatilastoista annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1099/2008 liitteessä A olevassa 2.6.3.1.16 kohdassa tarkoitettua datakeskusta.

Vapaaehtoinen ilmoittaminen (5 §:n 3 momentti) on kannatettava, mutta sille on luotava kannustin. Turvallisuuskriittisyys ei korreloi suoraan kokoon. Myös alle 0,5 megawatin konesaleilla voi olla huoltovarmuuden kannalta olennainen rooli esimerkiksi terveydenhuollon, energiahuollon, logistiikan tai teollisuusautomaation palveluissa, ja reunalaskennan yleistyessä kapasiteetti hajautuu nykyistä pienempiin yksiköihin. Laissa tai sen perusteluissa tulee todeta yksiselitteisesti, ettei vapaaehtoinen ilmoitus synnytä 7 §:n mukaista muutosilmoitusvelvollisuutta, 8 §:n mukaista maksuvelvollisuutta eikä 13 §:n mukaisen valvonnan piiriin kuulumista. Muutoin vapaaehtoisuudelle ei synny käytännön kannustinta eikä säännös tuota tilannekuvaan lisäarvoa.

[1] Energiatehokkuuslain muutoksen yhteydessä (846/2024 3§:
<https://www.finlex.fi/fi/lainsaadanto/saaduskokoelma/2024/846>

[2] Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1099/2008 liitteessä A oleva määritelmä datakeskukselle 2.6.3.1.16: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L_202400264

Ilmoitusvelvollisuuden ajankohta (5 §)

Ehdotamme 5 §:n ilmoitusvelvollisuuden ajankohdan täsmentämistä. Datakeskushankkeissa investointipäätös ei välttämättä ole yksittäinen ja yksiselitteisesti määriteltävä tapahtuma, vaan investointia koskevia päätöksiä tehdään tyypillisesti hankkeen edetessä vaiheittain. Vastaavasti myöskään rakennustöiden aloittaminen ei ole yksiselitteinen ajankohta, koska monia valmistelevia töitä ja esirakentamista saatetaan tehdä vaikka investointipäätöksestä ei olisikaan vielä varmuutta.

Ilmoitusvelvollisuus tulisi oikeusvarmuuden vuoksi sitoa objektiivisesti todennettavaan tapahtumaan, kuten hankkeen rakentamisen mahdollistavan luvan myöntämiseen tai sähköliittymäsopimuksen allekirjoittamiseen.

Samalla 5 ja 7 §:n keskinäistä suhdetta tulee selkeyttää. Laista tulisi käydä yksiselitteisesti ilmi, että 5 §:n mukainen ilmoitus on kertaluonteinen hankekohtainen ilmoitus ja että 7 § koskee tämän jälkeen tapahtuvia olennaisia muutoksia.

Lisäksi ilmoitusvelvollisuus tulee kohdentaa yksiselitteisesti yhdelle datakeskuksesta vastuussa olevalle taholle. Rakennusvaiheessa datakeskuksen ylläpitäjä ensisijaisena tai omistaja toissijaisena ilmoitusvelvollisena ei välttämättä ole riittävän yksiselitteisesti määriteltä. Datakeskusten omistus- ja toimintamallit vaihtelevat, ja esimerkiksi colocation-, wholesale-, powered land-, shell- ja build-to-suit-malleissa kiinteistön tai rakennuksen omistaja, teknisen infrastruktuurin omistaja sekä datakeskustoiminnan harjoittaja voivat olla eri tahoja. Laissa tai sen nojalla annettavassa asetuksessa tulee määritellä selkeästi, mikä taho vastaa ilmoituksen tekemisestä eri toimintamalleissa, jotta samasta datakeskuksesta ei synny päällekkäisiä ilmoitusvelvollisuuksia tai epäselvyyttä ilmoitusvastuusta.

Vastuutahon yksiselitteinen määrittely on tarpeen myös turvallisuussäätelyn näkökulmasta. Datakeskuksiin kohdistuu jo nyt useita velvoitteita, joissa vastuutaho on tunnistettava: kyberturvallisuuslain mukainen rekisteröityminen ja riskienhallintavelvoitteet, kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain mukainen kriittisen toimijan asema sekä ulkomaisten yritysostojen seurannasta annetun lain (172/2012) ja valmisteilla

olevan sijoituslupasääntelyn mukaiset menettelyt. Jos vastuutaho määrittellään näissä eri tavoin, syntyy tilanteita, joissa yksikään taho ei tosiasiallisesti vastaa kokonaisuudesta. Ehdotamme, että 5 §:n vastuutahon määrittelyssä käytetään yhdenmukaisia käsitteitä kyberturvallisuuslain ja sijoituslupasääntelyn kanssa ja että perusteluissa kuvataan, miten vastuu määräytyy edellä mainituissa toimintamalleissa.

Ilmoituksen yhteydessä toimitettavat tiedot sekä tietojen toimittamisesta poikkeaminen (6 §)

Kerättävät tietoluokat on perusteltu, mutta päällekkäisen tiedonkeruun välttäminen on tehtävä vielä paljon selkeämmäksi periaatteeksi.

Rekisteristä vastaavaa viranomaista on myös velvoitettava valmistelevaan ja julkaisemaan tarkat määritelmät, mittayksiköt ja raportointiohjeet määräajassa ennen tiedon keruun aloittamista.

Korostamme, että osa 6 §:ssä jo ehdotetuista tiedoista on varautumisen ja kokonaisturvallisuuden kannalta erityisen arvokkaita. Sijaintitieto (1 kohta) mahdollistaa maantieteellisten keskittymien ja yhteisvikariskien tunnistamisen. Omistusta ja määräysvaltaa koskevat tiedot (2 ja 3 kohta) ovat keskeisiä sekä toimitusketjuriskien arvioinnin että sijoitusten seurannan kannalta. Varavoimaa, omaa energiantuotantoa, energiavarastointia, kulutusjoustoja ja hukkalämmön hyödyntämistä koskevat suunnitelmat (12 kohta) ovat huoltovarmuustietoa, joka on tällä hetkellä saatavilla vain hajanaisesti.

Ehdotamme, että 6 §:ssä ilmoitettavat tiedot jaetaan selkeästi EU:n datakeskustietokannan mukaisiin tietoihin ja niitä täydentäviin kansallisiin tietoihin.

EU:n datakeskusrekisterin mukaiset tiedot:

- Mikäli datakeskus on tehnyt vuotuisen ilmoituksen EU:n datakeskusrekisteriin momentin 1 mukaisia tietoja ei tarvitse toimittaa.

- Muussa tapauksessa tiedot tulee voida ilmoittaa arvioina ja tarkoituksenmukaisina vaihteluväleinä sellaisina kuin niiden arvioidaan toteutuvan silloin kun raportoiva datakeskus alkaa tarjota tietotekniikkapalveluja.

- Arvioiden myöhempi muuttuminen hankkeen tarkentuessa ei sellaisenaan saa merkitä ilmoituksen oikaisutarvetta tai ilmoitusvelvollisuuden rikkomista.

EU:n datakeskusrekisterin mukaisia tietoja täydentävät tiedot:

- Suunniteltu datakeskuksen tai laajennusten toteuttamisaikataulu ilmoituksen jättämisvuoden ja sitä seuraavien neljän kalenterivuoden aikana.

- Vaihteluvälinä ilmoitettava arvio raportoivan datakeskuksen vuosittaisesta kokonaisenergiankulutuksesta ilmoituksen jättämisvuoden ja sitä seuraavien neljän kalenterivuoden aikana.

- Vaihteluvälinä ilmoitettava arvio asennetun tietotekniikan vuosittaisesta tehontarpeesta painotettua keskiarvoa käyttäen ilmoituksen jättämisvuoden ja sitä seuraavien neljän kalenterivuoden aikana.

- Vaihteluvälinä ilmoitettava arvio työllistämisestä rakennusvaiheessa ilmoituksen jättämisvuoden ja sitä seuraavien neljän kalenterivuoden aikana.

- Vaihteluvälinä ilmoitettava arvio työllistämisestä ylläpitovaiheessa ilmoituksen jättämisvuoden ja sitä seuraavien neljän kalenterivuoden aikana.

Datakeskuksen käyttötarkoitusta koskevan tiedon osalta tulee hyödyntää EU:n datakeskustietokantaan ilmoitettavaa datakeskuksen tyyppiä (delegoidun asetuksen liite 1, kohta 1 d) kansallisen sääntelyn sijaan.

[3] EU:n datakeskusrekisteri, delegoidun asetuksen liite 1: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L_202401364#anx_

Lakiin tai sen nojalla annettavaan asetukseen tulee sisällyttää yhdenmukaiset määritelmät, mittayksiköt ja raportointiohjeet. Tämä on tärkeää, jotta eri datakeskushankkeista toimitettavat tiedot ovat vertailukelpoisia. Kaikissa niissä kohdissa, joissa se on mahdollista käytetään EU:n datakeskusrekisterin määritelmiä, mittayksiköitä ja raportointiohjeita.

Rekisteriin ei tule kerätä turvallisuusjärjestelyjä koskevia tietoja. Esityksen 6 §:n säännöskohtaisissa perusteluissa todetaan, ettei rekisteriin kerätä tietoja datakeskuksissa käsiteltävän datan sisällöstä, asiakkaista tai turvallisuusjärjestelyistä. Rajausta on oikea ja erittäin tärkeä, mutta se tulee kirjata pykälätasolle eikä jättää perustelujen varaan. Keskitetty rekisteri, joka sisältäisi tiedot kriittisen infrastruktuurin fyysisistä ja teknisistä suojausratkaisuista, kulunvalvonnasta, pääsynhallinnasta, tietoliikenteen reiteistä tai käytetyistä laite- ja ohjelmistotoimittajista, muodostaisi itsessään

korkean arvon kohteen sekä valtiollisille toimijoille että rikollisryhmille. Tällaisten tietojen käsittely kuuluu kyberturvallisuuslain mukaiseen valvontaan ja turvallisuusselvitysmenettelyihin, ei elinkeinopoliittisen tilannekuvan tuottamiseen. Ehdotamme 6 §:ään uutta momenttia, jonka mukaan datakeskusrekisteriin ei saa tallentaa tietoja datakeskuksen turvallisuusjärjestelyistä, haavoittuvuuksista, asiakkaista eikä käsiteltävän datan sisällöstä.

Korostamme, että 12 kohdan osalta on kysyttävä kuvausta suunnitelmista, ei sellaisia teknisiä yksityiskohtia, joista voidaan päätellä datakeskuksen varautumisen kesto aika, varavoiman polttoainevarastojen sijainti tai muut suojattavat yksityiskohdat.

Datakeskuksen tyyppi ja kriittisyys. Edellä esitetyn mukaisesti käyttötarkoituksen osalta tulee käyttää EU:n datakeskustietokannan mukaista datakeskuksen tyyppiä. Tämän lisäksi tilannekuvan kannalta olisi arvokasta tietää, tarjoaako datakeskus palveluja kyberturvallisuuslain tai kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain soveltamisalaan kuuluville toimijoille. Tieto on kerättävissä kyllä/ei-tasoisena ilman asiakaslistoja tai asiakaskohtaisia tietoja, ja se ohjaisi sekä Huoltovarmuuskeskuksen että Liikenne- ja viestintäviraston huomiota oikeisiin kohteisiin. Tätä pidemmälle menevää asiakas- tai palvelutason tiedonkeruuta emme kannata.

Yhtenäistetään omistus- ja määräysvaltatiedot sijoituslupasääntelyn kanssa

Ehdotamme, että 3 kohdan määräysvaltaa koskeva käsite yhdenmukaistetaan sijoituslupasääntelyn kanssa ja että ilmoitettavaksi tulee myös tosiasiallinen edunsaaja. Esityksen 6 §:n 1 momentin 3 kohta sitoo määräysvallan kirjanpitolain (1336/1997) 1 luvun 5 §:ään eli käytännössä yli puoleen äänivallasta. Sijoituslupasääntelyn valmisteluaineiston mukaan määräysvallan määritelmä olisi tiukempi ja siinä tunnistetaan nimenomaisesti tosiasiallinen vaikutusvalta. Huoltovarmuuskeskus toimii myös valmisteilla olevan sijoituslupasääntelyn mukaisena lupaviranomaisena. Sama viranomainen soveltaisi siten samoihin datakeskuksiin kahta eri määräysvaltakäsitettä. Tällaista tilannetta tulee pyrkiä välttämään.

Sijoituslupasääntelyn greenfield-seuranta kohdistuu valmisteluaineiston mukaan vasta kapasiteetiltaan olennaisesti suurempiin datakeskuksiin kuin tämän lain 0,5 megawatin raja-arvo. Valtaosa esityksen soveltamisalaan kuuluvista noin 50–60 datakeskuksesta jää siten pelkästään tämän rekisterin varaan. Juuri tästä syystä rekisterin määräysvaltakäsitteen on katettava riittävä turvallisuusintressi: näiden kohteiden osalta rekisteri on ainoa kansallinen väline, jonka kautta omistus- ja vaikutusvaltarakenne tulee viranomaisten tietoon.

Datakeskuksen tyyppi ratkaisee, mitä omistustiedosta voi päätellä. Colocation- ja wholesale-malleissa ylläpitäjä ei tiedä eikä lähtökohtaisesti voi tietää, mitä dataa asiakkaan laitteissa käsitellään; vastuu käsittelystä on asiakkaalla. Omaan käyttöön rakennetussa tai hyperscale-tyyppisessä datakeskuksessa ylläpitäjä on sen sijaan itse käsittelystä vastaava taho. Sama omistustieto tarkoittaa näissä malleissa eri asiaa. Tämä yhteys 4 kohdan tyyppitiedon ja 2 ja 3

kohdan omistustietojen välillä tulee todeta säännöskohtaisissa perusteluissa, jotta tilannekuvan perusteella ei tehdä väärää päätelmiä siitä, millaista dataa Suomen oikeudenkäyttöpiirissä käsitellään.

Oikeudenkäyttöpiiri on eri kysymys kuin omistus. Sitä, minkä valtion lainkäyttövalta datakeskuksessa käsiteltävään tietoon ulottuu, ei ratkaise kiinteistön tai yhtiön omistus vaan se, mihin konserniin ylläpitäjä kuuluu, kenellä on tekninen pääsy järjestelmiin ja mistä maasta pääsyä käytetään. Kolmannen maan lainsäädäntöön perustuvat ekstraterritoriaaliset tiedonluovutusvelvoitteet ulottuvat myös unioniin sijoittautuneisiin tytäryhtiöihin.

Vastaavasti kotimaisessa omistuksessa oleva datakeskus voi olla altis, jos sen tekninen ylläpito tapahtuu kolmannelta maasta. Ehdotamme, että 6 §:ään lisätään kaksi tietoa, jotka ovat kerättävissä ilman asiakkaita tai datan sisältöä koskevia tietoja:

kyllä/ei-tasoinen tieto siitä, kohdistuuko datakeskuksen ylläpitäjään tai siihen konserniin, johon ylläpitäjä kuuluu, kolmannen maan lainsäädäntöön perustuvia tiedonluovutusvelvoitteita;

maatasoinen tieto siitä, mistä maasta datakeskuksen teknistä ylläpitoa ja etähallintaa tosiasiaassa suoritetaan.

Jälkimmäinen tieto on kerättävä yksinomaan viranomaiskäyttöön tarkoitettuun tilannekuvaan, eikä sitä tule sisällyttää julkiseen tilannekuvaan missään muodossa. Kumpikaan tieto ei paljasta datakeskuksen suojausratkaisuja, asiakkaita eikä käsiteltävän datan sisältöä, joten ne ovat sovitettavissa yhteen edellä esitetyn rajauksen kanssa. Tietoja ei myöskään tule tulkita arvioksi ylläpitäjän luotettavuudesta, vaan lähtötiedoksi, jonka perusteella toimivaltainen viranomainen voi kohdentaa oman menettelynsä.

Rekisteri on indeksi, ei tutkintaväline. Korostamme, ettei ilmoitusperusteinen rekisteri sovellu laittoman toiminnan tai vieraan valtion tiedustelutoiminnan havaitsemiseen. Toimija, joka harjoittaa tällaista toimintaa, ei täytä ilmoitusvelvollisuuttaan, eikä Huoltovarmuuskeskuksella ole tähän soveltuvia toimivaltuuksia; 13 §:n ainoa tehoste on uhkasakko. Rekisterin turvallisuusarvo perustuu kahteen muuhun seikkaan. Ensinnäkin se luo kattavan perustason, jota vasten poikkeamat erottuvat. Toiseksi 10 §:n mukainen tiedonsaantioikeus mahdollistaa ilmoitettujen tietojen ristiintarkistamisen sähköliittymiä, rakennuslupia ja ympäristölupia koskeviin tietoihin, mikä on käytännössä ainoa tapa havaita ilmoittamatta jätetyt kohteet. Ilman ristiintarkistusta rekisteri kuvaa vain sitä, mitä toimijat itse haluavat kertoa. Tämä puoltaa 10 §:n tiedonsaantioikeuden säilyttämistä.

Rekisterin tehtävä turvallisuuden kannalta on siten mahdollistaa varsinaisten instrumenttien – sijoituslupamenettelyn, turvallisuusselvitysmenettelyn, kyberturvallisuuslain mukaisen valvonnan ja kriittisten toimijoiden nimeämisen – kohdentaminen oikeisiin kohteisiin. Tämä on syytä todeta esityksen perusteluissa, jotta rekisteriltä ei odoteta sellaista, mihin se ilmoitusperusteisena välineenä ei kykene.

Yhteyshenkilötiedot on kerättävä roolipohjaisina. Esityksen mukaan rekisteriin tallennettavat yhteystiedot voivat sisältää myös kotiosoitteita, ja henkilötiedot voivat siten olla julkisuuslain 24 §:n 1 momentin 31 kohdan nojalla salassa pidettäviä. Kriittisen infrastruktuurin avainhenkilöitä koskevien henkilötietojen kokoaminen yhteen kansalliseen rekisteriin on itsessään henkilöturvallisuusriski. Ehdotamme, että 6 §:n 1 momentin 1 kohdassa edellytetään yhteyshenkilön roolia ja työnantajaan liittyviä yhteystietoja. Ratkaisu vastaisi myös perustuslakivaliokunnan käytäntöä henkilötietojen käsittelyn rajaamisesta välttämättömään.

Ilmoita kerran, hyödynnä monesti. Datakeskuksiin kohdistuu jo nyt raportointi- ja ilmoitusvelvollisuuksia ainakin EU:n datakeskustietokantaan (delegoitu asetus (EU) 2024/1364), energiatehokkuuslain (1429/2014) nojalla, kyberturvallisuuslain nojalla Liikenne- ja viestintävirastolle, kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla sekä yritysosto- ja sijoituslupamenettelyissä. Kannatamme voimakkaasti periaatetta, jonka mukaan sama tieto ilmoitetaan viranomaisille kerran ja viranomaiset hyödyntävät sitä yhdessä. Periaate tulee kirjata lain tavoitteisiin ja toteuttaa käytännössä 10 §:n tiedonsaantioikeuden kautta niin laajasti kuin tietojen luonne sallii.

Muutoksista ilmoittaminen ja muutosilmoitusten ajankohta (7 §)

Muutosilmoitusvelvollisuutta tulee täsmentää siten, ettei datakeskushankkeiden tavanomaisesta suunnittelusta, rakentamisesta ja vaiheittaisesta käyttöön otosta muodostu jatkuvaa raportointivelvollisuutta, eikä aiemmin ilmoitetun suunnitelman mukainen eteneminen laukaise velvollisuutta muutosten ilmoittamiseen. Velvollisuuden tulisi koskea vain olennaisia ja pysyviä sekä aiemmin ilmoitetusta poikkeavia muutoksia. Kalenterivuoden aikana tapahtuvista muutoksista tulisi lisäksi voida ilmoittaa kootusti sen sijaan, että jokainen vaihe tai kapasiteetin lisäys edellyttäisi erillistä ilmoitusta.

Ehdotamme, että omistusta, määräysvaltaa ja ylläpitäjää koskevien muutosten 30 päivän ilmoitusaikaa pidennetään vähintään 60 päivään. Tällaiset muutokset liittyvät usein yritys- ja omistusjärjestelyihin, joissa lopullisten ilmoitettavien tietojen varmistaminen voi edellyttää tietojen kokoamista useilta konserniyhtiöiltä ja muilta järjestelyn osapuolilta. Määräajan tulee mahdollistaa oikeiden ja lopullisten tietojen toimittaminen ilman tarpeetonta hallinnollista taakkaa.

Omistusta ja määräysvaltaa koskevat muutokset ovat rekisterin tietolajeista turvallisuuden kannalta merkityksellisimpiä, ja juuri siksi on tärkeää, että tieto on oikea. Oikea ja lopullinen tieto 60 päivän kuluessa palvelee viranomaista paremmin kuin nopea mutta puutteellinen tai myöhemmin oikaistava ilmoitus. Samalla on varmistettava, ettei 7 §:n mukainen ilmoitus muodostu päällekkäiseksi ulkomaisten yritysostojen seurannasta annetun lain ja valmisteilla olevan sijoituslupasääntelyn mukaisten menettelyjen kanssa. Kun samasta järjestelystä on tehty ilmoitus tai haettu lupa mainittujen säännösten nojalla, tiedon tulisi siirtyä viranomaisten välillä 10 §:n nojalla eikä sitä tulisi vaatia erikseen ilmoitusvelvolliselta. Huoltovarmuuskeskus toimii uuden sijoituslupasääntelyn mukaisena lupaviranomaisena, joten menettelyjen yhteensovittaminen on käytännössä mahdollista ja tarkoituksenmukaista.

Huoltovarmuuskeskuksen tiedonsaantioikeus, tietojenantovelvollisuus ja tietojen luovuttaminen (10, 11 ja 12 §)

Pidämme välttämättömänä, että yksittäisten yritysten kaupallisesti ja kriittisen infrastruktuurin turvallisuuden näkökulmasta arkaluonteisten tietojen salassapito turvataan yksiselitteisesti lain tasolla. Samalla edellytämme, että aggregoitu, julkisen keskustelun ja päätöksenteon kannalta olennainen tilannekuvatieto datakeskustoimialan kehityksestä tulee median, päättäjien ja kansalaisten saataville avoimesti ja ajantasaisesti.

Ehdotamme, että lain 4 §:ssä ja 12 §:ssä erotetaan toisistaan julkinen tilannekuva ja viranomaiskäyttöön tarkoitettu tilannekuva. Julkisen tilannekuvan tulisi muodostua riittävän laajoista toimiala- ja aluetason aggregoiduista tiedoista. Viranomaiskäyttöön tarkoitettu tilannekuva voisi puolestaan sisältää lain tarkoituksen toteuttamiseksi välttämättömiä yksittäisiä datakeskuksia koskevia tietoja, joiden salassapito olisi turvattu laissa.

Julkisen tilannekuvan sääntelyssä on varmistettava, ettei julkaistavista tiedoista voida suoraan tai välillisesti tunnistaa yksittäistä datakeskusta, datakeskushanketta tai toimijaa. Tämä on erityisen tärkeää alueilla tai tietoluokissa, joissa toimijoiden määrä on pieni. Myöskään julkisten tietojen yhdistäminen muihin saatavilla oleviin tietolähteisiin ei saisi mahdollistaa yksittäistä hanketta koskevien arkaluonteisten tietojen päättelemistä.

Salassa pidettävien tietojen salassapidon ja käyttötarkoitussidonnaisuuden tulee säilyä myös silloin, kun tietoja luovutetaan viranomaiselta toiselle. Erityistä huomiota tulee kiinnittää 12 §:ssä tarkoitettuun tietojen edelleen luovuttamiseen. Tiedon luovuttamisen tulee perustua vastaanottavan viranomaisen yksilöityyn ja laissa säädettyyn tietotarpeeseen. Lisäksi tulisi arvioida mahdollisuutta säätää menettelystä, jossa tiedot toimittaneille yrityksille ilmoitetaan muiden viranomaisten tekemistä tietopyynnöistä.

Katsomme, että selkeä jako julkiseen ja viranomaiskäyttöön tarkoitettuun tilannekuvaan palvelisi samanaikaisesti kahta esityksen keskeistä tavoitetta: se mahdollistaisi datakeskustoimialan kehitystä koskevan avoimen ja tietoon perustuvan yhteiskunnallisen keskustelun sekä turvaisi yksittäisten yritysten liikesalaisuudet ja kriittisen infrastruktuurin turvallisuuden kannalta arkaluonteiset tiedot.

Emme näe tarvetta 11 §:ssä esitetty yksityisiin elinkeinonharjoittajiin ja elinkeinoelämän järjestöihin kohdistuvaan yleiseen tietojen antovelvollisuuteen. Perusteluissa on viitattu erityisesti kantaverkkoyhtiöltä (Fingrid) pyydettyihin tietoihin, mikä tulisikin sallia, mutta samaa oikeutta ei tule määrittämättömästi ulottaa kaikkiin toimijoihin.

Rekisteri on itsessään suojattava kohde. Esityksen vaikutusarvioinnissa todetaan, että keskitetty tietovaranto voi lisätä laittoman kohdistetun tiedonhankinnan riskiä ja että käyttöoikeudet, loki,

salassapito, turvallisuusluokittelu ja korkea tekninen suojaustaso ovat välttämättömiä. Havainto on oikea, mutta se jää pelkästään perustelujen tasolle eikä saa vastinetta säännöksissä. Kun samaan tietovarantoon kootaan kansallisesti kattava kuva siitä, missä Suomen laskentakapasiteetti sijaitsee, kuka sitä omistaa ja miten se on sähköistetty, tietovarannosta muodostuu tiedustelullisesti kiinnostava kohde.

Ehdotamme, että lakiin lisätään erillinen säännös rekisterin tietoturvallisuudesta, jossa säädetään ainakin:

- julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) ja asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019) soveltamisesta rekisterin tietoihin;

- Vähintään viittaus lakiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain muuttamisesta (HE 85/2026 vp)

- siitä, että rekisterin tiedot muodostavat kokonaisuutena aineiston, jonka suojaustaso arvioidaan erikseen ja jota käsitellään tämän arvion mukaisesti myös silloin, kun yksittäinen tieto ei olisi salassa pidettävä.

Lisäksi katsomme, että rekisterin tietojärjestelmän tietoturvallisuus tulee arvioida ennen käyttöönottoa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain mukaisessa menettelyssä. Rekisteriä koskeva tietoturvallisuuden arviointi ja sen ylläpito on tarkoituksenmukaista toteuttaa markkinaehtoisesti hyödyntäen hyväksytyjä arviointilaitoksia.

Julkisen tilannekuvan aggregointi ja uudelleentunnistaminen. Julkaistavista tiedoista ei pidä voida suoraan tai välillisesti tunnistaa yksittäistä datakeskusta tai hanketta. Korostamme, että arvio on tehtävä nimenomaan tietojen yhdisteltävyyden näkökulmasta: julkisesti on jo saatavilla kaavoitus- ja rakennuslupatietoja, ympäristölupia, EU:n datakeskustietokannan tietoja, energiatehokkuuslain mukaisia maakuntatason tietoja sekä sähköverkkoyhtiöiden liityntätietoja. Yksittäin harmiton aluetason luku voi näiden kanssa yhdistettynä yksilöidä hankkeen.

Ehdotamme, että julkisen tilannekuvan julkaisemiselle asetetaan nimenomainen aggregointikynnys ja että Huoltovarmuuskeskus tekee uudelleentunnistamisen riskiarvion ennen ensimmäistä julkaisua sekä aina julkaisutiheyden tai tietosisällön olennaisesti muuttuessa. Näillä edellytyksillä pidämme välttämättömänä julkisen keskustelun ja tietopohjaisen päätöksenteon tukemiseksi, että julkinen tilannekuva julkaistaan automaatiota esimerkiksi kuukausittain tai vähintään kvartaalitasolla.

Uudelleentunnistamisen ehkäisemiseksi julkaistavissa tiedoissa voidaan käyttää esimerkiksi pidemmän ajan liukuvia keskiarvoja, jolloin julkaisuutiheyttä ei tarvitse rajoittaa vaikka sensitiiviset tiedot suojataan.

Tiedonkulun on oltava kaksisuuntaista. Ilmoitusvelvollisuus on toimialan näkökulmasta perusteltu vain, jos siitä syntyvää tietoa myös palautetaan toimialalle. Ehdotamme, että perusteluissa todetaan Huoltovarmuuskeskuksen tehtäväksi tuottaa datakeskustoimijoille toimialakohtaista varautumis- ja uhkatietoa yhteistyössä mm. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen sekä Suomessa toimivan kyberturvallisuusteollisuuden kanssa.

Yksittäistä datakeskusta koskevan tiedon luovuttaminen (12 §) on rajattava välttämättömään. Esityksen 12 § sallisi yksittäistä datakeskusta koskevan rekisteritiedon luovuttamisen kaikille julkisuuslain 4 §:n 1 momentin 1, 4 ja 7 kohdassa tarkoitetuille viranomaisille, mukaan lukien kaikki kunnalliset viranomaiset. Rajaus on liikesalaisuuksien ja kriittisen infrastruktuurin suojan kannalta liian laaja. Perustuslakivaliokunnan käytännön mukaisesti yksittäistä toimijaa koskevien salassa pidettävien tietojen luovuttaminen tulisi sitoa välttämättömyyteen ja luovutuksensaajat yksilöidä laissa tarkasti. Ehdottamamme ajantasainen julkinen tilannekuva, joka sisältää aggregoitua tukee sellaisenaan myös monien viranomaisten toimintaa.

Tiedonsaantioikeuden täydentäminen (10 §). Jotta "ilmoita kerran" -periaate toteutuisi, Huoltovarmuuskeskuksen tiedonsaantioikeus tulisi ulottaa Energiaviraston, elinvoimakeskusten, Lupa- ja valvontaviraston ja Turvallisuus- ja kemikaaliviraston lisäksi Liikenne- ja viestintävirastoon siltä osin kuin kyse on kyberturvallisuuslain nojalla ylläpidettävistä toimijoiden perus- ja rekisteröitymistiedoista. Korostamme, että tiedonsaantioikeus on tässä yhteydessä rajattava nimenomaisesti niin, ettei se ulotu kyberturvallisuuslain nojalla ilmoitettuihin poikkeamatietoihin, haavoittuvuustietoihin eikä valvonta-asioiden aineistoihin. Näiden tietojen luottamuksellisuus on poikkeamien ilmoittamishalukkuuden ja koko poikkeamailmoitusjärjestelmän toimivuuden edellytys.

Voimaantulon ajankohta sekä siirtymäaika rakentamisvaiheessa ja toiminnassa olevien datakeskusten osalta (15 §)

Rekisterinpitäjän tulee julkaista hyvissä ajoin ennen lain voimaantuloa yksityiskohtainen ilmoitusohje. Ohjeessa tulee täsmentää ainakin ilmoitusvelvollisuuden soveltaminen vaiheittain toteutettaviin hankkeisiin, asennetun tietotekniikan tehontarpeen laskenta, sähkötehon, liittymätehon ja vuosikulutuksen määritelmät, arvioiden ja vaihteluvälien käyttö, muutosilmoitusten kynnysarvot, luottamuksellisten tietojen merkitseminen ja käsittely, EU-raportoinnin ja kansallisen raportoinnin välinen työnjako sekä ilmoitusmaksujen määräytyminen.

Pidämme tärkeänä, että toimialaa kuullaan asetuksen, ilmoitusohjeen ja käytännön ilmoitusmenettelyn valmistelussa ennen niiden vahvistamista.

Siirtymäaika rakentamisvaiheessa tai toiminnassa oleville datakeskuksille on kohtuullinen ja ajoittuu hyvin suhteessa EU:n datakeskusrekisterin raportoinnin takarajaan, joka on vuosittain toukokuussa.

Huoltovarmuuskeskuksen tulee aloittaa ajantasaisen julkisen tilannekuvan julkaisu viimeistään 1.9.2027.

Ilmoitusohjeessa tulee käsitellä myös tietoturvallisuutta: miten ilmoitus toimitetaan suojatusti, miten luottamukselliset tiedot merkitään, kuka niitä Huoltovarmuuskeskuksessa käsittelee ja miten ilmoitusvelvollinen voi tarvittaessa toimittaa tiedot korotetun suojaustason menettelyssä. Ilmoituskanavan tulee perustua vahvaan tunnistautumiseen ja suojattuun tiedonsiirtoon. Suojaamaton sähköposti ei ole tähän tarkoitukseen soveltuva kanava.

Huoltovarmuuskeskuksen tehtävä ja sen resursointi

Datakeskusteollisuus ja Kyberala pitävät tärkeänä, että rekisterinpitäjän tehtävät ja resurssit suunnitellaan siten, että rekisteristä voidaan tuottaa sekä viranomaiskäyttöön tarkoitettu tilannekuva että ajantasainen julkinen tilannekuva. Julkisen tilannekuvan tuottamista tulee pitää rekisterin keskeisenä tehtävänä, jotta rekisteri ei muodostu itseisarvoiseksi hallinnolliseksi järjestelmäksi.

Jotta tilannekuvasta olisi hyötyä julkisessa keskustelussa ja päätöksenteossa tulee Huoltovarmuuskeskuksen päivittää julkinen tilannekuva esityksessä ehdotettua vuosittaista julkaisua merkittävästi useammin, esimerkiksi kuukausittain. Ajantasainen julkinen tilannekuva toimii myös markkinasignaalina sähköntuotannon hankkeiden investointipäätösten tukena.

Ajantasaisesti päivittyvässä julkisessa tilannekuvassa tiedot tulee julkaista riittävästi aggregoituina esimerkiksi kuuden kuukauden liukuvina keskiarvoina siten, ettei julkaistavista tiedoista voida tunnistaa yksittäisiä datakeskuksia tai hankkeita. Tilannekuvan koostaminen ja julkaiseminen tulee automatisoida mahdollisimman pitkälle, jotta ajantasaisen tiedon tuottaminen ei aiheuta tarpeetonta hallinnollista työtä.

Koska rekisterin tietoja voidaan täydentää myös muilta viranomaisilta saatavilla tiedoilla, ilmoitusvelvolliselle tulee toimittaa automaattisesti vuosittain rekisteriote, josta tämä voi tarkistaa itseään koskevien tietojen oikeellisuuden ja tarvittaessa ilmoittaa virheistä. Rekisteriotteen automaattinen toimittaminen ilmoitusvelvolliselle on tärkeää myös tietojen oikeellisuuden ja hyvän hallinnon näkökulmasta. Virheelliseen tai vanhentuneeseen tietoon perustuva tilannekuva on varautumisen kannalta huonompi kuin tieto siitä, että tilannekuva on puutteellinen.

Ilmoitusten käsittelystä perittävien maksujen tulee olla kohtuullisia, läpinäkyviä ja oikeassa suhteessa käsittelystä aiheutuviin todellisiin kustannuksiin. Maksuilla ei saa rahoittaa Huoltovarmuuskeskuksen yleistä toimintaa. Myös eri kokoisten datakeskushankkeiden oikeudenmukainen kohtelu tulee huomioida ilmoitusmaksuissa.

Maksujen määräytymisperusteet tulee julkaista hyvissä ajoin ennen lain voimaantuloa. Maksua ei tule periä viranomaisen pyytämistä teknisistä täydennyksistä tai korjauksista, viranomaisten välisestä tiedonsiirrosta eikä tiedoista, jotka on jo toimitettu EU:n datakeskustietokantaan. Muutosilmoituksista mahdollisesti perittävien maksujen tulee olla selvästi alkuperäistä ilmoitusta pienempiä.

Resursoinnissa on otettava huomioon myös rekisterin tietoturvallisuuden ylläpito ja jatkuva valvonta, ei ainoastaan ilmoitusten käsittely ja tilannekuvan tuottaminen. Rekisterin ylläpito edellyttää käyttövaltuushallintaa, lokien seuranta, poikkeamien havainnointia ja säännöllistä auditointia koko rekisterin elinkaaren ajan. Nämä kustannukset on tunnistettava esityksen taloudellisissa vaikutuksissa. Mikäli rekisterin ylläpitäjän tietoturvallisuusvelvoitteiden ei suunnitella asianmukaisesti, rekisteristä muodostuu kansallinen turvallisuusriski sen sijaan, että se tukisi varautumista.

Muut esitystä koskevat huomiot

Keskeisin ehdotuksemme kohdistuu kansallista tilannekuvaa koskevaan 4 §, jonka muotoiluksi ehdotamme seuraavaa:

Huoltovarmuuskeskus ylläpitää säännöllistä datakeskuksia koskevaa viranomaiskäyttöön tarkoitettua kansallista tilannekuvaa ja jakaa tilannekuvaa 12 §:ssä tarkoitetuille viranomaisille.

Huoltovarmuuskeskus ylläpitää ja julkaisee ajantasaista datakeskusten toimiala- ja aluekehitystä koskevaa julkista tilannekuvaa. Julkinen tilannekuva julkaistaan aggregoituna siten, ettei siitä voida tunnistaa tai päätellä yksittäistä datakeskusta, datakeskushanketta tai niitä koskevia salassa pidettäviä tietoja.

Huoltovarmuuskeskuksen on ennen julkisen tilannekuvan ensimmäistä julkaisemista ja aina sen tietosisällön tai julkaisutiheyden olennaisesti muuttuessa arvioitava, voidaanko julkaistavista tiedoista muihin saatavilla oleviin tietoihin yhdistämällä tunnistaa yksittäinen datakeskus tai datakeskushanke.

Rekisteröinti ei ole lupa eikä turvallisuushyväksyntä – mutta se tukee turvallisuussääntelyn toimeenpanoa. Esityksessä todetaan perustellusti, ettei ilmoitus tarkoita lupaa tai turvallisuushyväksyntää eikä sen laiminlyönti estä hankkeen toteuttamista. Toteamuksen säilyttäminen on tärkeää. Samalla katsomme, että rekisterin tuottamaa tietoa voidaan ja tulee hyödyntää kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain mukaisessa kriittisten toimijoiden tunnistamisessa sekä kyberturvallisuuslain soveltamisalan arvioinnissa. Tämä kytkentä on syytä kirjata perusteluihin, jotta rekisterin lisäarvo turvallisuussääntelyn toimeenpanossa tulee näkyväksi ja jotta päällekkäinen tiedonkeruu vältetään. Rekisteröinti ei kuitenkaan saa muodostua uudeksi tosiasialliseksi turvallisuusarvioinnin väyläksi ilman asianmukaista menettelyä, muutoksenhakuoikeutta ja oikeusturvaa.

Tietojen säilytysajasta on säädettävä. Esityksessä ei säädetä rekisteriin tallennettujen tietojen säilytysajasta. Koska rekisteri sisältää sekä liikesalaisuuksia että henkilötietoja, säilytysajasta tulee säätää laissa. Erityisesti on säädettävä siitä, kuinka kauan tietoja säilytetään sen jälkeen, kun datakeskushanke on 7 §:n 2 momentissa tarkoitetulla tavalla keskeytetty tai päättynyt taikka toiminta on lakannut. Tarpeettomien tietojen säilyttäminen kasvattaa rekisteriin kohdistuvan tietomurron vahinkopotentiaalia ilman vastaavaa hyötyä tilannekuvalle.

Suhde EU:n sääntelyyn. Pidämme tärkeänä, että kansallinen rekisteri rakennetaan EU:n datakeskustietokannan varaan eikä sen rinnalle. Mikäli EU-tason raportointia laajennetaan esimerkiksi valmisteilla olevan Cloud and AI Development Act -sääntelyn yhteydessä, kansallista ilmoitusvelvollisuutta tulee vastaavassa laajuudessa keventää. Suomen kilpailukyky datakeskusinvestointien sijoittumisessa ei saa heiketä kansallisen lisäsääntelyn vuoksi, ja tilannekuvan tuottamisen tulee perustua ensisijaisesti tietoon, joka toimijoilla on jo olemassa.

Poikola Antti

Datakeskusteollisuus (Finnish Data Center Association ry.) - Lausunnon antavat yhdessä Datakeskusteollisuus sekä Kyberala ry (Finnish Information Security Cluster, FISC). Kyberalan yhteyshenkilö Peter Sund, toimitusjohtaja, Kyberala ry, 050 565 0621, peter.sund@teknologiateollisuus.fi