EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Ilmoituksen numero : 2023/0761/ES (Spain)

KUNINKAAN ASETUS 5G-VERKKOJA JA -PALVELUJA KOSKEVAN KANSALLISEN TURVALLISUUSJÄRJESTELMÄN HYVÄKSYMISESTÄ

Saapumispäivä : 29/12/2023
Odotusajan päättyminen : 02/04/2024 (closed)

Message

Viesti 001

Komission tiedonanto - TRIS/(2023) 3739

Direktiivi (EU) 2015/1535

Ilmoitus: 2023/0761/ES

Jäsenvaltion ilmoitus luonnostekstistä

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx il-perijodi ta' dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20233739.FI

1. MSG 001 IND 2023 0761 ES FI 29-12-2023 ES NOTIF

2. Spain

3A. Subdirección de Asuntos Industriales, Energéticos, de Transportes, Comunicaciones y de Medioambiente
D.G. de Mercado Interior y otras Políticas Comunitarias
Ministerio de Asuntos Exteriores, UE y Cooperación

3B. Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
Secretaría General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual.
Subdirección General de Ordenación de las Telecomunicaciones.
Ministerio de Transformación Digital

4. 2023/0761/ES - V00T - Teleala

5. KUNINKAAN ASETUS 5G-VERKKOJA JA -PALVELUJA KOSKEVAN KANSALLISEN TURVALLISUUSJÄRJESTELMÄN HYVÄKSYMISESTÄ

6. Sähköiset 5G-viestintäverkot ja -palvelut

Viestintälaitteet.

7.

8. Asetus koostuu johdanto-osasta, yhdestä pykälästä, jolla hyväksytään ENS5G-järjestelmä (5G:tä koskeva kansallinen turvallisuusjärjestelmä), kahdesta lisäsäännöksestä ja neljästä loppusäännöksestä.
Hyväksyttävä ENS5G-järjestelmä koostuu 33 pykälästä, jotka on jaettu kahdeksaan lukuun, ja kolmesta liitteestä.
Perusteluissa esitetään säädöksen antamisen ja kehitteillä olevien kuninkaan lakiasetuksen pykälien perusteet.
Ainoassa pykälässä hyväksytään 5G-verkkoja ja -palveluja koskeva kansallinen turvallisuusjärjestelmä.
Ensimmäisessä lisäsäännöksessä säädetään, että hallituksen on digitalisaatioministerin esityksestä ja kansallisen turvallisuusneuvoston kertomuksen perusteella tarkistettava kuninkaan asetuksella 5G-verkkoja ja -palveluja koskeva kansallinen turvallisuusjärjestelmä olosuhteiden niin vaatiessa ja joka tapauksessa neljän vuoden välein.
Toisessa lisäsäännöksessä todetaan, että 29 päivänä maaliskuuta 2022 annettua kuninkaan lakiasetusta 7/2022 ja ENS5G-järjestelmää sovelletaan viidennen sukupolven jälkeisiin sähköisen viestinnän sukupolviin, vaikka niistä ei ole olemassa erityistä sääntelyä.
Toimivaltaa koskevassa ensimmäisessä loppusäännöksessä säädetään, että kuninkaan asetus ja sillä hyväksytty järjestelmä annetaan Espanjan perustuslain 149 §:n 1 momentin 21 kohdan ja 149 §:n 1 momentin 29 kohdan säännösten nojalla. Kyseisissä säännöksissä annetaan valtiolle yksinomainen toimivalta yleistä televiestintäjärjestelmää ja yleistä turvallisuutta koskevissa asioissa.
Toisessa loppusäännöksessä todetaan, että yleisestä televiestinnästä 28 päivänä kesäkuuta 2022 annettua lakia 11/2022 ja sen täytäntöönpanosäädöksiä on sovellettava täydentävästi. Lisäksi siinä säädetään, että kaikissa asioissa, joista ei säädetä mainitussa lainsäädännössä, sovelletaan täydentävästi verkkojen ja tietojärjestelmien turvallisuudesta 7 päivänä syyskuuta 2018 annettua kuninkaan lakiasetusta 12/2018 sekä toimenpiteistä kriittisten infrastruktuurien turvaamiseksi 28 päivänä huhtikuuta 2011 annettua lakia 8/2011 sekä niiden täytäntöönpanosäädöksiä.
Lainsäädännön kehittämistä koskevassa kolmannessa loppusäännöksessä annetaan digitalisaatioministeriön johtajalle mahdollisuus kehittää tämän kuninkaan asetuksen ja sillä hyväksytyn järjestelmän säännöksiä sekä muuttaa määräyksellä liitteiden sisältöä tekniikan kehityksen, televiestintälaitteita ja niihin liitettyjä tuotteita koskevien uusien teknisten standardien ja sertifiointijärjestelmien hyväksymisen sekä 5G-verkkojen ja -palvelujen ja tulevien sähköisen viestinnän sukupolvien eri kokoonpanojen ja teknisten parametrien kehityksen mukaan.
Neljännessä loppusäännöksessä säädetään, että säädös tulee voimaan sitä päivää seuraavana päivänä, jona se julkaistaan Espanjan virallisessa lehdessä.
Hyväksyttävän ENS5G-järjestelmän sisällön osalta:
Järjestelmän 1 §:ssä säädetään, että säädös annetaan 29 päivänä maaliskuuta 2022 annetun kuninkaan lakiasetuksen 7/2022 ja erityisesti sen IV luvun täytäntöönpanemiseksi.
Järjestelmän 2 §:ssä viitataan säädöksen tavoitteisiin, joita on jo arvioitu.
Järjestelmän 3 §:ssä säädetään, että on käytettävä 29 päivänä maaliskuuta 2022 annetussa kuninkaan lakiasetuksessa 7/2022, yleisestä televiestinnästä 28 päivänä kesäkuuta 2022 annetussa laissa 11/2022 ja eurooppalaisessa sähköisen viestinnän säännöstössä annettuja määritelmiä.
Järjestelmän 4 §:ssä säädetään, että säädöstä sovelletaan 5G-operaattoreihin, 5G-toimittajiin ja 5G-yrityskäyttäjiin, joille on myönnetty oikeus käyttää julkista radioverkkoa yksityisen 5G-verkon asentamiseen, käyttöönottoon tai käyttöön tai 5G-palvelujen tarjoamiseen ammattimaisiin tai itsenäisen toiminnan tarkoituksiin.
Järjestelmän 5 §:ssä yksilöidään sähköisen 5G-viestintäverkon muodostavat vähimmäiselementit, -infrastruktuurit ja -resurssit ja viitataan niiden yksityiskohtaiseen kuvaukseen liitteessä I. Siinä esitetään myös 5G-verkon kriittiset elementit, joiden on pääsääntöisesti sijaittava kansallisella alueella (mahdolliset poikkeukset mukaan luettuina).
Järjestelmän 6 §:ssä viitataan turvallisuuden kattavaan käsittelyyn kansainvälisen yhteisön ja sellaisen hyväksytyn tai mahdollisesti hyväksyttävän kansallisen lainsäädännön mukaisesti, jossa velvollisia vaaditaan arvioimaan kokonaisvaltaisella menetelmällä niihin talouden toimijoina vaikuttavia ja eri osien haavoittuvuuksia, uhkia ja riskejä sekä näiden riskien asianmukaista ja kattavaa hallintaa käyttämällä tekniikoita ja toimenpiteitä, jotka ovat asianmukaisia riskien lieventämiseksi tai poistamiseksi sekä 5G-verkkojen ja -palvelujen turvallista käyttöä ja toimintaa koskevan

lopullisen tavoitteen saavuttamiseksi.
Järjestelmän 7 §:ssä korostetaan, että riskianalyysi ja riskinhallinta ovat olennainen osa turvallisuusmenettelyä ja että niiden olisi oltava jatkuvaa ja jatkuvasti päivitettävää toimintaa.
Järjestelmän 8 §:ssä viitataan jatkuvaan seurantaan ja säännölliseen uudelleenarviointiin.
Järjestelmän 9 §:ssä todetaan, että kansallisella tasolla tehtävä riskianalyysi esitetään liitteessä II ja että se on toteutettu ottaen huomioon useita tekijöitä, kuten velvollisilta kerätyt tiedot, 5G-verkkojen ja -palvelujen toimitusketjuun liittyvien haavoittuvuuksien tutkiminen, toimittajien riippuvuusasteen arviointi, toimitusten keskeytymisen riski toimittajiin vaikuttavien taloudellisten, yrityksiin liittyvien tai kaupallisten olosuhteiden vuoksi tai sovellettujen turvatoimenpiteiden tehokkuuden arviointi.
Kansallisella tasolla tehtävää riskinhallintaa koskevassa 10 §:ssä todetaan, että liitteessä III vahvistetaan perusteet, vaatimukset, edellytykset ja määräajat, joiden mukaisesti velvolliset suunnittelevat ja toteuttavat riskinlieventämistekniikoita ja -toimenpiteitä.
Järjestelmän 11 §:ssä kehitetään 29 päivänä maaliskuuta 2022 annetun kuninkaan lakiasetuksen 7/2022 14 §:n säännöksiä, jotka koskevat menettelyä ja näkökohtia, jotka ministerineuvoston on arvioitava luokiteltaessa suurta riskiä edustavia toimittajia, sekä huomioon otettavia seikkoja määrättäessä kyseisten toimittajien tarjoamien laitteiden, tuotteiden ja palvelujen mahdollisesta korvaamisesta. Samoin edellä mainitun kuninkaan lakiasetuksen säännösten mukaan suurta riskiä edustavat toimittajat, joiden televiestintälaitteita, laitteistoja, ohjelmistoja tai oheispalveluja käytetään yksinomaan ja ainoastaan yksityisissä 5G-verkoissa tai itsenäisen toiminnan puitteissa 5G-palvelujen tarjoamiseen, luokitellaan keskisuurta riskiä edustaviksi toimittajiksi.
Järjestelmän 12 § koskee niiden paikkojen määrittämistä, joihin suurta riskiä edustaviksi luokiteltujen toimittajien laitteita ei saa asentaa. Siinä todetaan, että kansallinen turvallisuusneuvosto voi digitalisaatioministeriön kertomuksen perusteella määrittää paikat, alueet ja keskukset, joihin suurta riskiä edustavaksi luokiteltujen toimittajien laitteita ei saa asentaa. 5G-operaattoreiden on pyydettävä lupa digitalisaatioministeriöltä sellaisten radioasemien asentamiseen, muuttamiseen tai mukauttamiseen, jotka kattavat nämä paikat, alueet ja keskukset.
Järjestelmän 13 §:ssä velvoitetaan 5G-operaattorit laatimaan toimitusketjun monipuolistamista koskeva strategia ja sisällyttämään liityntäverkkoon siirtolaitteita, joita tarjoaa vähintään kaksi eri toimittajaa. Siinä säädetään myös perusteista, jotka ministerineuvoston on otettava huomioon, jotta voidaan päättää, onko mahdollista säilyttää yksi ainoa toimittaja, jos toimittajien määrä vähenee yritysten yhteensulautumisen seurauksena. Lisäksi siinä esitetään oletukset ja menettelytavat, joilla digitalisaatioministeriö voi muuttaa 5G-operaattorin toimitusketjun monipuolistamista koskevaa strategiaa.
Järjestelmän 14 §:ssä keskitytään riskianalyysiin, joka 5G-operaattoreiden on tehtävä kaikista liitteessä I tarkoitetuista verkon elementeistä, infrastruktuurista ja resursseista, luetellaan huomioon otettavat tekijät ja velvoitetaan operaattorit keräämään toimittajiltaan turvallisuuskäytännöt ja -toimenpiteet, joita ne ovat toteuttaneet niille toimittamissaan tuotteissa ja palveluissa, sekä sisällyttämään riskien etusijajärjestys ja hierarkia tiettyjen lueteltujen parametrien mukaisesti. 5G-operaattoreiden on toimitettava riskianalyysi 1 päivään lokakuuta 2024 mennessä ja sen jälkeen kahden vuoden välein.
5G-toimittajien tekemää riskianalyysiä koskevassa 15 §:ssä edellytetään 5G-verkkojen toimintaan tai käyttöön tai 5G-palvelujen tarjoamiseen liittyvien televiestintälaitteiden, laitteistojen ja ohjelmistojen sekä oheispalvelujen riskien analysointia ja kyseisen analyysin toimittamista ministeriölle pyynnöstä. Jos toimittajien luokitellaan edustavan suurta riskiä tai keskisuurta riskiä, analyysi on toimitettava kuuden kuukauden kuluessa kyseisestä luokittelusta ja sen jälkeen kahden vuoden välein.
5G-yrityskäyttäjien riskianalyysiä koskevassa 16 §:ssä edellytetään, että tämä riskianalyysi toimitetaan digitalisaatioministeriölle, kun kyseisiltä käyttäjiltä tällaista edellytetään.
Järjestelmän 17 §:n mukaan digitalisaatioministeriö voi kerätä velvollisilta riskianalyysiä varten tarvittavat tiedot ja kyseisten tietojen toimittamatta jättäminen 15 työpäivän kuluessa luokitellaan vakavaksi rikkomukseksi. Tietoja pidetään luottamuksellisina, eikä niitä saa käyttää muuhun tarkoitukseen kuin 29 päivänä maaliskuuta 2022 annetussa kuninkaan lakiasetuksessa 7/2022, ENS5G-järjestelmässä ja molempien säädösten täytäntöönpanemiseksi annetuissa säädöksissä vahvistettujen tavoitteiden ja velvoitteiden täyttämiseen.
Järjestelmän 18 §:ssä säädetään kaikkien velvollisten yleisestä velvollisuudesta hallita turvallisuusriskejä.
Järjestelmän 19 §:ssä keskitytään 5G-operaattoreiden turvallisuudenhallintaan, luetellaan kaikkien operaattoreiden velvollisuudet (kuten valmiussuunnitelmien ja -toimenpiteiden hyväksyminen, eurooppalaisten standardien tai teknisten eritelmien ja sertifiointijärjestelmien noudattaminen, turvallisuustarkastuksen teettäminen omalla kustannuksella tai

toimittajien velvoittaminen noudattamaan turvallisuusstandardeja) ja lisävelvollisuudet niille operaattoreille, jotka omistavat tai käyttävät julkisen 5G-verkon kriittisiä elementtejä (kuten kielto käyttää suurta riskiä edustavien toimittajien laitteita kriittisissä verkkoelementeissä tai tietyissä paikoissa, alueilla ja keskuksissa). 5G-operaattoreiden on toimitettava digitalisaatioministeriölle kuvaus teknisistä ja organisatorisista toimenpiteistä, jotka on suunniteltu ja toteutettu riskien hallitsemiseksi ja lieventämiseksi, 1 päivään lokakuuta 2024 mennessä ja sen jälkeen kahden vuoden välein. Lisäksi 5G-operaattoreiden, jotka omistavat tai käyttävät julkisen 5G-verkon kriittisiä elementtejä, on toimitettava digitalisaatioministeriölle toimitusketjun monipuolistamista koskeva strategia 1 päivään lokakuuta 2024 mennessä ja sen jälkeen aina, kun strategiaa muutetaan. Tiedot tämän strategian täytäntöönpanosta on toimitettava kunkin vuoden lokakuun 1 päivään mennessä.
5G-toimittajien toteuttamaa turvallisuudenhallintaa koskeva 20 § sisältää luettelon velvoitteista, mukaan lukien toimittajien laitteiden, tuotteiden ja palvelujen turvallisuustarkastuksen suorittaminen, tietojen antaminen kolmansien osapuolten mahdollisesta puuttumisesta toimittajien laitteiden, tuotteiden ja palvelujen suunnitteluun, käyttöön ja toimintaan sekä yhteistyöstä 5G-operaattoreiden ja 5G-yrityskäyttäjien kanssa antamalla tietoja ja varmentamalla standardien ja sertifiointien noudattaminen. 5G-toimittajien on laadittava raportti teknisistä ja organisatorisista toimenpiteistä, jotka on suunniteltu ja toteutettu riskien hallitsemiseksi ja lieventämiseksi, ja toimitettava kyseinen raportti ministeriölle pyynnöstä. Jos toimittajien luokitellaan edustavan suurta riskiä tai keskisuurta riskiä, raportti on toimitettava kuuden kuukauden kuluessa kyseisestä luokittelusta ja sen jälkeen kahden vuoden välein.
5G-yrityskäyttäjien toteuttamaa turvallisuudenhallintaa koskevassa 21 §:ssä todetaan, että kyseiset käyttäjät eivät saa käyttää kriittisissä verkkoelementeissä televiestintälaitteita, siirtojärjestelmiä, kytkentä- tai reitityslaitteita ja muita resursseja, joilla mahdollistetaan signaalien siirtäminen, laitteistoja, ohjelmistoja tai oheispalveluja, joiden toimittajien on luokiteltu edustavan keskisuurta riskiä. Lisäksi käyttäjien on pyynnöstä toimitettava digitalisaatioministeriölle kuvaus teknisistä ja organisatorisista toimenpiteistä, jotka on suunniteltu ja toteutettu riskien hallitsemiseksi ja lieventämiseksi.
Viranomaisten toteuttamaa turvallisuudenhallintaa koskevassa 22 §:ssä säädetään, että julkisten ja yksityisten 5G-verkkojen asentamisessa, käyttöönotossa ja käytössä tai 5G-palvelujen tarjoamisessa, riippumatta siitä, tarjotaanko niitä julkisesti saataville vai itsenäiseen toimintaan, viranomaiset eivät saa kansallisen turvallisuuden vuoksi käyttää suurta tai keskisuurta riskiä edustavien toimittajien tarjoamia laitteita, tuotteita ja palveluja.
Järjestelmän 23 §:ssä säädetään, että edellisissä pykälissä säädettyjen velvoitteiden mukaisesti velvollisten on otettava huomioon 29 päivänä maaliskuuta 2022 annettu kuninkaan lakiasetus 7/2022, ENS5G-järjestelmä ja molempien säädösten täytäntöönpanemiseksi annetut säädökset ja sovellettava niitä.
Järjestelmän 24 §:n mukaan digitalisaatioministeriö voi kerätä velvollisilta riskinhallintaa varten tarvittavat tiedot ja kyseisten tietojen toimittamatta jättäminen 15 työpäivän kuluessa luokitellaan vakavaksi rikkomukseksi. Tietoja pidetään luottamuksellisina, eikä niitä saa käyttää muuhun tarkoitukseen kuin 29 päivänä maaliskuuta 2022 annetussa kuninkaan lakiasetuksessa 7/2022, ENS5G-järjestelmässä ja molempien säädösten täytäntöönpanemiseksi annetuissa säädöksissä vahvistettujen tavoitteiden ja velvoitteiden täyttämiseen.
Järjestelmän 25 §:ssä säädetään, että kaikkien velvollisten sekä viranomaisten, valmistajien, maahantuojien, jakelijoiden ja niiden, jotka saattavat markkinoille ja myyvät 5G-verkkoon liitettäviä ja 5G-palvelujen tarjoamiseen kykeneviä päätelaitteita ja laitteita, on tehtävä yhteistyötä ja toimitettava ENS5G-järjestelmän muuttamista ja täytäntöönpanoa varten tarvittavat tiedot.
Järjestelmän 26 §:ssä säädetään, että digitalisaatioministeriön johtajan määräyksellä tietyn laitteen, järjestelmän, ohjelman tai palvelun käytön edellytyksenä voi olla, että sille on saatu etukäteen kyberturvallisuutta koskevan 17 päivänä huhtikuuta 2019 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 tai Euroopan tai kansainvälisellä tasolla mahdollisesti hyväksyttävien 5G-laitteiden ja -tuotteiden sertifiointia koskevien sertifiointijärjestelmien ja teknisten standardien mukainen sertifiointi.
Järjestelmän 27 §:ssä säädetään, että säädöksen soveltaminen ei rajoita ulkomaisia investointeja eikä kilpailua koskevan lainsäädännön soveltamista.
Päätelaitteita koskevassa 28 §:ssä säädetään, että 5G-verkkoon liitettävien ja 5G-palvelujen tarjoamiseen kykenevien päätelaitteiden ja laitteiden valmistuksen, tuonnin, jakelun, markkinoille saattamisen ja kaupan pitämisen edellytyksenä on, että noudatetaan Euroopan unionin lainsäädännön mukaisesti hyväksyttyjä digitaalisten tuotteiden turvallisuusvaatimuksia ja sovellettavia olennaisia kyberturvallisuusvaatimuksia, jotka koskevat erityisesti henkilötietojen suojaa, yksityisyyttä ja petosten torjuntaa.
Järjestelmän 29 §:ssä viitataan kansainväliseen yhteistyöhön, jota digitalisaatioministeriön on määrä kehittää erityisesti Euroopan unionin tasolla.

Järjestelmän 30 §:ssä viitataan digitalisaatioministeriön toimivaltaan ENS5G-järjestelmän täytäntöönpanossa. Ministeriön olisi koordinoitava toimintaansa muiden kyberturvallisuudesta ja kriittisestä infrastruktuurista vastaavien elinten kanssa ENS5G-järjestelmän johdonmukaisen täytäntöönpanon varmistamiseksi.
Järjestelmän 31 §:ssä eritellään digitalisaatioministeriölle kuuluvat ENS5G-järjestelmän täytäntöönpanovaltuudet, joita ovat esimerkiksi ENS5G-järjestelmän sisällön kehittäminen, määrittely ja yksityiskohdat, asetettujen velvoitteiden noudattamisen tarkastamiseksi ja valvomiseksi tehtävien tarkastusten suorittaminen sekä julkisen tuen myöntäminen.
Järjestelmän 32 §:ssä annetaan digitalisaatioministeriölle kaikki tarkastustoimintavaltuudet.
Seuraamusjärjestelmää koskevassa 33 §:ssä viitataan 29 päivänä maaliskuuta 2022 annetun kuninkaan lakiasetuksen 7/2022 30 ja 31 §:n säännöksiin.
Liitteessä I kuvataan 5G-verkon muodostavat elementit, infrastruktuuri ja resurssit.
Liitteessä II esitetään riskianalyysi kansallisella tasolla.
Liitteessä III esitetään riskinhallinta kansallisella tasolla.

9. Viidennen sukupolven eli 5G-matkaviestintä on sähköisen viestinnän uusi malli, johon sisältyy yhteiskuntaa ja taloutta merkittävästi hyödyttäviä muutosmahdollisuuksia, koska sen myötä on mahdollista ottaa käyttöön uusia, vaikutuksiltaan merkittäviä toimintoja, kuten verkkolaskenta. Lisäksi se mahdollistaa virtuaaliverkkojen luomisen, takaa vähäisen viipeen ja tarjoaa merkittävästi lisäarvoa tuottavia palveluja esimerkiksi lääketieteen, liikenteen ja energian aloilla.
Näin ollen sekä Euroopan unioni että Espanja edistävät 5G-verkkojen nopeaa käyttöönottoa ja sellaisten hankkeiden toteuttamista, joilla osoitetaan niiden hyödyllisyys eri aloilla 5G-palvelujen tarjoamisella.
5G-verkoilla ja -palveluilla on suhteellisia turvallisuusetuja edellisiin sukupolviin verrattuna. Niihin liittyy kuitenkin myös erityisiä riskejä, jotka johtuvat esimerkiksi niiden monimutkaisemmasta, avoimesta ja eriytetystä verkkoarkkitehtuurista sekä kyvystä siirtää valtavia määriä tietoa ja mahdollistaa useiden ihmisten ja asioiden samanaikainen vuorovaikutus. Niiden yhteenliittäminen muihin verkkoihin ja monien uhkien kansainvälinen luonne vaikuttavat niiden turvallisuuteen, ja näiden verkkojen ennakoitavissa oleva laajamittainen käyttö talouden ja yhteiskunnan keskeisiin toimintoihin lisää niihin kohdistuvien turvallisuushäiriöiden mahdollisia vaikutuksia.
5G-matkaviestinnän uusia erityisiä turvallisuusriskejä käsiteltiin sääntelyllisesti viidennen sukupolven sähköisten viestintäverkkojen ja -palvelujen turvallisuuden varmistamista koskevista vaatimuksista 29 päivänä maaliskuuta 2022 annetussa kuninkaan lakiasetuksessa 7/2022, jolla saatetaan osaksi kansallista lainsäädäntöä kokonaisuudessaan 5G-verkkojen kyberturvallisuudesta 26 päivänä maaliskuuta 2019 annettu Euroopan komission suositus (EU) 2019/534 sekä suositukset, joita jäsenvaltioille annettiin 29 päivänä tammikuuta 2020 annetussa Euroopan komission tiedonannossa (5G:n turvallinen käyttöönotto EU:ssa – EU:n välineistön täytäntöönpano, COM/2020/50 final) kyseisen välineistön käytöstä.
Edellä mainitussa 29 päivänä maaliskuuta 2022 annetussa kuninkaan lakiasetuksessa 7/2022 säädetään kyseisen asetuksen sääntelyn kehittämisestä 5G-verkkoja ja -palveluja koskevalla kansallisella turvallisuusjärjestelmällä (ENS5G).
Edellä mainitun kuninkaan lakiasetuksen 5 §:n 3 momentin mukaisesti ENS5G-järjestelmässä on käsiteltävä kattavasti 5G-verkkojen ja -palvelujen turvallisuutta ottaen huomioon 5G-arvoketjun kunkin toimijan osuudet sekä Euroopan unionin, Kansainvälisen televiestintäliiton (ITU) ja muiden kansainvälisten järjestöjen määräykset, suositukset ja tekniset standardit, jotta Espanjassa voidaan taata 5G-verkkojen ja -palvelujen turvallista käyttöä ja toimintaa koskeva perimmäinen tavoite.
Kuninkaan lakiasetuksen 20 §:ssä puolestaan säädetään, että 5G-verkon ja -palvelujen jatkuvan ja turvallisen toiminnan varmistamiseksi ENS5G-järjestelmässä on tehtävä kansallisella tasolla riskianalyysi 5G-verkkojen ja -palvelujen turvallisuudesta sekä yksilöitävä, täsmennettävä ja kehitettävä toimenpiteitä analysoitujen riskien lieventämiseksi ja hallitsemiseksi.
Kuninkaan lakiasetuksen 21 §:n mukaisesti hallitus hyväksyy ENS5G-järjestelmän kuninkaan asetuksella digitalisaatioministeriön esityksestä kansallisen turvallisuusneuvoston kertomuksen perusteella.
Tällä asetuksella hyväksytään ENS5G-järjestelmä, jolla kehitetään viidennen sukupolven sähköisten viestintäverkkojen ja -palvelujen turvallisuuden varmistamista koskevista vaatimuksista 29 päivänä maaliskuuta 2022 annetun kuninkaan lakiasetuksen 7/2022 säännöksiä.

10. Viittaukset perusteksteihin:

11. Ei

12.

13. Ei

14. Ei

15. Kyllä

16.
TBT-näkökohta: Ei

SPS-näkökohta: Ei

****
Euroopan komissio
Yhteysviranomainen direktiivin (EU) 2015/1535
Sähköposti: grow-dir2015-1535-central@ec.europa.eu