



EUROPEAN COMMISSION

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

Ilmoituksen numero : 2026/0346/ES (Spain)

Luonnos kuninkaalliseksi asetukseksi sähköisten viestintäverkkojen ja -palvelujen sekä tiettyjen digitaalisten infrastruktuurien turvallisuudesta ja häiriönsietokyvystä.

Saapumispäivä : 08/07/2026

Odotusajan päättymisen : 09/10/2026

Message

Viesti 001

Komission tiedonanto - TRIS/(2026) 1822

Direktiivi (EU) 2015/1535

Ilmoitus: 2026/0346/ES

Jäsenvaltion ilmoitus luonnostekstistä

Notification – Notificación – Notifizierung – 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 késéset - Non fa decorrere la mora - Atidējimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħ 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: 20261822.FI

1. MSG 001 IND 2026 0346 ES FI 08-07-2026 ES NOTIF

2. Spain

3A. Subdirección General de Ordenación de las Telecomunicaciones.

Secretaría General de Telecomunicaciones, Infraestructuras Digitales y Seguridad Digital.

Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Ministerio para la Transformación Digital y de la Función Pública

Calle Poeta Joan Maragall 41

28020 Madrid

+34 913462750

3B. Subdirección General de Ordenación de las Telecomunicaciones.

Secretaría General de Telecomunicaciones, Infraestructuras Digitales y Seguridad Digital.

Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Ministerio para la Transformación Digital y de la Función Pública



EUROPEAN COMMISSION

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

Calle Poeta Joan Maragall 41
28020 Madrid
+34 913462750

4. 2026/0346/ES - V00T - Telela

5. Luonnos kuninkaalliseksi asetukseksi sähköisten viestintäverkkojen ja -palvelujen sekä tiettyjen digitaalisten infrastruktuurien turvallisuudesta ja häiriönsietokyvystä.

6. Asetuksen tavoitteena on vahvistaa sähköisten viestintäverkkojen ja -palvelujen sekä niihin liittyvien toimintojen ja tiettyjen digitaalisten infrastruktuurien turvallisuutta, häiriönsietokykyä ja jatkuvuutta Espanjassa.

7.

8. Kuninkaallisen asetuksen tavoitteena on varmistaa sähköisten viestintäverkkojen ja -palvelujen sekä niihin liittyvien laitteistojen ja tiettyjen digitaalisten infrastruktuurien turvallisuus, kestävyys ja toiminnan jatkuvuus Espanjassa. Sillä varmistetaan keskeisten palvelujen tarjoaminen turvallisuuspoikkeamien, palvelun keskeytysten tai merkittävien häiriöiden yhteydessä sekä säännellään velvoitteita ilmoittaa tällaisista poikkeamista viranomaisille.

Velvollisuuden piiriin kuuluvat julkisten sähköisten viestintäverkkojen toimijat, yleisesti saatavilla olevien palvelujen tarjoajat, niihin liittyvien laitteistojen ja digitaalisten infrastruktuurien toimijat (esim. merikaapelit, satelliittijärjestelmät, tietojenkäsittelykeskukset (DPC), sisällönjakeluverkot (CDN) ja internetin yhdysliikennepisteet (IXP)) sekä tietyiltä osin 112-hätäpuhelukeskukset ja julkiset varoitusjärjestelmät. Siinä tunnustetaan myös näiden verkostojen ja infrastruktuurien keskeinen merkitys hätätilanteissa.

Kansallinen turvallisuus- ja häiriönsietokykyä koskeva suunnitelma, jossa määritellään kriisinhallintatoiminnan järjestäminen ja institutionaaliset koordinoitummekanismat, on laadittu. Siinä säädetään myös, että velvoitettujen tahojen on laadittava yleistason suunnitelma jokaiselle velvoitetulle osapuolelle sekä erityissuunnitelmat jokaiselle verkkotyyppille ja määrättyille palveluille. Näihin on sisällyttävä riskianalyysit, välttämättömän infrastruktuurin tunnistaminen, ennaltaehkäisevät toimenpiteet, palautusmekanismat ja toimintaprotokollat erilaisia skenaarioita, kuten sähkökatkoksia, luonnonkatastrofeja, tulipaloja, tietoteknisiä vikoja tai kyberhyökkäyksiä varten.

Siinä asetetaan televiestintäpalveluiden jatkuvuuden varmistamiseksi erityisiä velvoitteita. Toimijoiden on toteutettava toimenpiteitä, joilla minimoidaan häiriöiden vaikutukset ja varmistetaan keskeisten palvelujen, erityisesti hätäviestinnän, toimivuus. Poikkeustapauksissa ne voivat asettaa etusijalle tietyn tyyppisen liikenteen, kuten hätäviestinnän tai puhe- ja tekstiviestipalvelut, noudattaen kuitenkin aina teknologianeutraaliuden periaatetta. Lisäksi keskeiselle infrastruktuurille asetetaan energiaomavaraisuuden vähimmäisvaatimukset, ja matkaviestinverkoille määrätään velvollisuus varmistaa asteittain vähintään neljän tunnin varavirtalähde 75 prosentille väestöstä kolmen vuoden kuluessa.

Asetukseen sisältyy järjestelmä sellaisten merkittävien tapahtumien ilmoittamiseksi, joita ei pidetä kyberturvallisuustapahtumina, joita säännellään NIS2-direktiivissä ja CER-direktiivissä. Toimijoiden on ilmoitettava valtiosihteeristölle kaikista merkittävistä häiriötilanteista tunnin kuluessa siitä, kun ne ovat saaneet tiedon häiriöstä, ja toimitettava sen jälkeen säännöllisiä tilannetietoja häiriön keston ajan sekä lopullinen raportti, kun palvelu on palautettu. Hätäviestintää 112-numeron ja julkisten varoitusjärjestelmien kautta koskevat erityistoimenpiteet. Sekä hätäpuhelukeskusten että toimijoiden on otettava käyttöön varajärjestelmiä ja liiketoiminnan jatkuvuuden varmistavia toimenpiteet, laadittava erityiset varautumissuunnitelmat ja ilmoitettava välittömästi näiden palvelujen häiriöistä, jotka luokitellaan automaattisesti merkittäviksi häiriötilanteiksi.

Kuninkaallisessa asetuksessa säädetään toimenpiteistä ja mekanismeista, jotka koskevat koordinoitua kriittisten toimijoiden kyberturvallisuutta ja häiriönsietokykyä koskevien asetusten (NIS 2 -direktiivi ja kriittisten yksiköiden häiriönsietokykyä koskeva direktiivi) kanssa, turvallisuuden ja häiriönsietokyvyn koordinoitukomitean perustamista sekä poikkeamien hallintaan ja viestintään tarkoitettujen digitaalisten alustojen tulevaa käyttöönottoa. Kaiken kaikkiaan, asetus tiukentaa merkittävästi televiestintäalaa ja kriittisiin digitaalisiin infrastruktuureihin sovellettavien turvallisuus-, jatkuvuus- ja valvontavelvoitteita.

9. Talouden ja julkisten palvelujen lisääntyvä digitalisaatio on lisännyt merkittävästi riippuvuutta sähköisistä



EUROPEAN COMMISSION

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

viestintäverkoista ja niitä tukevista digitaalisista infrastruktuureista. Tilanne on nostanut esiin haavoittuvuuksia ja riskejä, jotka eivät rajoitu yksinomaan kyberturvallisuuteen, vaan vaikuttavat myös fyysiseen turvallisuuteen ja infrastruktuurien kykyyn kestää häiritsevyyttä ja toipua niistä. Tässä yhteydessä määräyksessä katsotaan tarpeelliseksi vahvistaa ennaltaehkäisy-, reagointi- ja toipumisvalmiuksia sellaisten vaaratilanteiden varalta, jotka voivat vaarantaa sähköisten viestintäverkkojen ja -palvelujen saatavuuden, eheyden tai toiminnan.

Kuninkaallisen asetuksen perusteluissa tuodaan esiin useita viimeaikaisia tapahtumia, jotka ovat osoittaneet, että näiden infrastruktuurien sietokykyä on lisättävä. Siinä mainitaan muun muassa luonnonilmiöitä, kuten vuoden 2021 La Palman tulivuorenpurkaus ja vuoden 2024 kylmä matalapaineilmiö, joka vaikutti useisiin osiin Espanjaa, sekä muista kuin luonnollisista syistä johtuvia vaaratilanteita, kuten hiljattain tapahtunut valtakunnallinen sähkökatkos. Nämä tapahtumat osoittivat, että niin äärimmäiset luonnonilmiöt kuin tekniset viat tai sähkökatkokset voivat aiheuttaa merkittäviä häiriöitä viestintäverkoissa ja vaarantaa kansalaisille ja viranomaisille välttämättömien palvelujen jatkuvuuden.

Lisäksi digitaalinen siirtymä muuttaa perusteellisesti televiestintäverkkojen arkkitehtuuria ja toimintaa. Esineiden internetin, tekoälyn, massadatan, pilvipalvelujen ja palvelujen virtualisoinnin kaltaisten teknologioiden käyttöönotto on mahdollistanut tehokkuuden, yhteenliitettävyyden ja taloudellisen kehityksen, mutta samalla se on tehnyt järjestelmistä monimutkaisempia ja luonut uusia operatiivisia riskejä ja turvallisuusriskejä. Asetuksessa pidetäänkin olennaisen tärkeänä, että sääntelykehystä kehitetään näiden riskien ennakoinniseksi ja asianmukaisen suojelun ja häiriönsietokyvyn varmistamiseksi.

Oikeudellisesti aloite perustuu pääasiassa sähköisten viestintäverkkojen ja -palvelujen eheydestä ja turvallisuudesta annetun lain 11/2022 (yleinen televiestintälaki) 63 §:ään. Lisäksi se perustuu 5G-verkon turvallisuutta koskevaan voimassa olevaan lainsäädäntöön, erityisesti verkko- ja tietojärjestelmien turvallisuudesta annettuun kuninkaalliseen asetukseen 7/2022, verkko- ja tietojärjestelmien turvallisuutta koskevaan kuninkaalliseen asetukseen 12/2018 ja 5G-verkkoja ja -palveluja koskevan kansallisen turvallisuuskehyksen hyväksymisestä annettuun kuninkaalliseen asetukseen 443/2024. Edellä esitetyistä huolimatta, vaikka nämä säännökset ovatkin saaneet aikaan merkittävää edistystä, on tarpeen kehittää erityinen sääntelykehys, jossa käsitellään kattavasti kaikkien sähköisten viestintäverkkojen ja -palvelujen sekä tiettyjen digitaalisten infrastruktuurien turvallisuutta ja kestävyyttä.

Lopuksi tekstissä selitetään, että uudella kuninkaallisella asetuksella pyritään täydentämään Espanjan tulevaa lainsäädäntöä, joka koskee kriittisten toimijoiden kyberturvallisuutta ja häiriönsietokykyä. Näin ollen NIS2- ja CER-direktiivin kansalliseen lainsäädäntöön saattamisesta johtuvat velvoitteet ovat edelleen täysin sovellettavissa kyberturvallisuuspoikkeamiin sekä niihin poikkeamiin, jotka vaikuttavat digitaalisiin verkkoihin, palveluihin ja infrastruktuureihin, eikä niitä koskevia säännöksiä ole tässä kuninkaallisessa asetuksessa. Tavoitteena on näin ollen varmistaa eri sääntelyvälineiden välinen johdonmukaisuus, välttää sääntelyn päällekkäisyyttä ja luoda kattava suojajärjestelmä, joka vahvistaa Espanjan yhteiskunnan ja talouden toiminnan kannalta olennaisen televiestintä- ja digitaalisen infrastruktuurin turvallisuutta, jatkuvuutta ja häiriönsietokykyä.

9a. Toimenpide soveltuu asetetun tavoitteen saavuttamiseen eli sähköisten viestintäverkkojen ja -palvelujen sekä tiettyjen digitaalisten infrastruktuurien turvallisuuden, häiriönsietokyvyn ja jatkuvuuden vahvistamiseen.

Viime vuosien kokemukset ovat osoittaneet, että tietoliikenneverkot ovat yhteiskunnan toiminnalle välttämättömiä infrastruktuureja, kuten kävi ilmi koronaviruspandemian aikana sekä hätätilanteissa, jotka johtuivat äärimmäisistä luonnonilmiöistä, sähkökatkokista tai turvallisuusuhista, jotka ovat vaikuttaneet palvelujen saatavuuteen. Tässä skenaariossa erityisen sääntelykehyksen käyttöönotto on asianmukainen toimenpide, jolla vahvistetaan valmiuksia ehkäistä sähköisen viestinnän jatkuvuutta mahdollisesti vaarantavia häiriöitä, reagoida niihin ja toipua niistä.

Asetuksella pannaan täytäntöön yleisen televiestintälain (11/2022) 63 §:n säännökset. Se täydentää myös sääntelykehystä ja mukauttaa sitä teknologian kehitykseen sekä digitalisaatioon, verkkojen virtualisointiin, pilvipalveluihin, tekoälyyn ja esineiden internetiin (IoT) liittyviin uusiin riskeihin, joiden yleistyminen lisää alttiutta sekä fyysisille että digitaalisille haavoittuvuuksille. Tältä osin kuninkaallinen asetus on asianmukainen väline sellaisten alakohtaisten velvoitteiden määrittämiseksi, jotka mahdollistavat kokonaisvaltaisen lähestymistavan televiestintäalan teknisiin ja toiminnallisiin erityispiirteisiin.

Toimenpiteen tarkoituksenmukaisuus näkyy erityisesti siinä, että siihen on sisällytetty ennaltaehkäisy- ja suunnittelumekanismeja, joilla pyritään parantamaan toimijoiden varautumista kriisitilanteisiin. Velvollisuus laatia verkosto- tai palvelukohtaisia yleis- ja erityissuunnitelmia sekä kansallinen turvallisuus- ja kestävyysuunnitelma ja kansallinen siviilivalmiussuunnitelma mahdollistavat yhdessä riskien tunnistamista, ennaltaehkäisyä, reagointia ja palautumista koskevien erityismenettelyjen laatimisen.



EUROPEAN COMMISSION

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

Poikkeamista ilmoittamista koskevien menettelyjen päivittäminen on lisäksi asianmukainen toimenpide toimivaltaisten viranomaisten seuranta- ja kriisinhallintavalmiuksien parantamiseksi. Kokemus on osoittanut, että ilmoitusten kriteerejä, määräaikoja ja sisältöä on mukautettava vastaamaan monimutkaisempaa teknistä ja toiminnallista todellisuutta.

Lisäksi toimenpide soveltuu hyvin erityisen arkaluonteisten palvelujen, kuten 112-hätäviestinnän ja julkisten varoitusjärjestelmien, suojausten vahvistamiseen asettamalla jatkuvuutta, päällekkäisyyttä ja ilmoittamista koskevia erityisvelvoitteita sekä toimijoille että hätäkeskuksille. Näin varmistetaan, että kriittiset palvelut pysyvät toiminnassa myös vakavissa viestintäinfrastruktuurin häiriötilanteissa.

Yhteistyömekanismien luominen viranomaisten sekä kansallisten ja eurooppalaisten viranomaisten välille sekä eri sidosryhmät kattavan pysyvän koordinoitukomitean perustaminen ovat sopivia keinoja edistää tiedonvaihtoa, toimielinten välistä koordinaatiota ja parhaiden käytäntöjen omaksumista turvallisuuden ja kestävyysalalla. Toimenpide on myös yhdenmukainen NIS 2 -direktiiviin ja kriittisten yksiköiden häiriönsietokykyä koskevaan direktiiviin perustuvan EU:n sääntelykehityksen kanssa, ja sillä varmistetaan asianmukainen koordinaatio tulevan kansallisen täytäntöönpanolainsäädännön kanssa ja ehkäistään sääntelyn puutteita talouden ja kansallisen turvallisuuden kannalta strategisesti tärkeällä alalla.

9b. Kuninkaallisen asetuksen hyväksymisellä vastataan todelliseen ja todistettuun tarpeeseen vahvistaa ennaltaehkäisy-, suojele- ja palautumisvalmiuksia infrastruktuureissa, joista on tullut välttämättömiä yhteiskunnan, talouden ja julkisten palvelujen toiminnan kannalta.

Taloudellisen ja yhteiskunnallisen toiminnan lisääntyvä digitalisaatio yhdistettynä kasvavaan riippuvuuteen sähköisistä viestintäverkoista ja -palveluista sekä tapahtumat, kuten La Palman tulivuorenpurkaus, maan eri osia koetellut kylmä matalapaineilmiö tai hiljattain tapahtunut sähkökatkos, ovat osoittaneet, että sähköiset viestintäverkot ja -palvelut ovat alttiita monenlaisille riskeille, jotka voivat vakavasti vaarantaa kansalaisille, yrityksille ja viranomaisille välttämättömät palvelut. Nämä poikkeamat ovat korostaneet tarvetta vahvistaa digitaalisen infrastruktuurin häiriönsietokykyä ja parantaa valmiuksia reagoida hätätilanteisiin ja kriiseihin.

Tämä toimenpide on tarpeen yleisen televiestintälain (11/2022) 63 §:n täytäntöönpanemiseksi ja voimaansaattamiseksi, jossa säädetään toimijoiden velvollisuudesta hallita turvallisuusriskejä asianmukaisesti ja varmistaa verkkojensa ja palvelujensa eheys. On välttämätöntä laatia säännökset, joissa määritellään tarkemmin suunnittelua, ennaltaehkäisyä, poikkeustilanteiden ilmoittamista, toimielinten välistä koordinaatiota ja valvontaa koskevat velvollisuudet, joita toimijoiden ja muiden asianomaisten osapuolten on noudatettava.

Asetuksen tarve perustuu myös siihen, että tällä hetkellä voimassa oleva poikkeustapahtumien ilmoittamista koskeva sääntelykehys on osittain vanhentunut. Tämänhetkiset menettelyt eivät enää vastaa riittävällä tavalla niiden tapahtumien monimutkaisuutta, jotka voivat vaikuttaa nykyajan digitaalisiin verkkoihin, palveluihin ja infrastruktuureihin. Tapahtumatyyppien, viestintämenettelyjen ja ilmoitusmääräaikojen päivittäminen on välttämätöntä, jotta toimivaltaisilla viranomaisilla on riittävät ja ajantasaiset tiedot, joiden avulla ne voivat koordinoida nopean ja tehokkaan reagoinnin kriisitilanteissa.

On myös tarpeen luoda erityisiä mekanismeja, joilla varmistetaan erityisen kriittisten palvelujen jatkuvuus, kuten 112-hätäpuhelut ja kansalaisille suunnatut varoitusjärjestelmät. Kokemus on osoittanut, että näiden palveluiden häiriöt voivat vaikuttaa suoraan ihmishenkien ja ihmisten ruumiillisen koskemattomuuden turvaamiseen sekä hätätilanteiden hallintaan. Tästä syystä asetuksessa määrätään sekä toimijoille että hätäpuhelukeskuksille erityisiä velvoitteita, jotka koskevat suunnittelua, varajärjestelmiä ja toiminnan jatkuvuutta.

Lisäksi toimenpide on tarpeen kansallisten ja eurooppalaisten yhteistyömekanismien parantamiseksi sekä erityisen koordinoitukomitean perustamiseksi, joilla helpotetaan tietojenvaihtoa, kokemusten jakamista ja yhteisten menettelyjen käyttöönottoa sellaisten poikkeamien käsittelyssä, jotka luonteensa vuoksi vaikuttavat yleensä useisiin toimijoihin ja infrastruktuuriin samanaikaisesti.

Lopuksi on tarpeen varmistaa Espanjan lainsäädännön johdonmukaisuus uuden eurooppalaisen sääntelykehityksen kanssa, joka perustuu NIS2- ja CER-direktiiveihin. Nämä eurooppalaiset säädökset tiukentavat kriittisen infrastruktuurin turvallisuutta, riskienhallintaa ja sietokykyä koskevia velvoitteita ja velvoittavat jäsenvaltiot kehittämään tehokkaita mekanismeja poikkeustilanteiden ehkäisemiseksi, havaitsemiseksi, niihin reagoimiseksi ja niistä toipumiseksi.

9c. Ehdotettu toimenpide ei aiheuta kohtuutonta tai suhteetonta taakkaa asetettuihin tavoitteisiin nähden, koska sen sisältämät velvoitteet vastaavat tarpeeseen varmistaa yhteiskunnan, talouden ja julkisten palvelujen toiminnan kannalta olennaisten infrastruktuurien turvallisuus, häiriönsietokyky ja jatkuvuus.



EUROPEAN COMMISSION

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

Toimenpiteen oikeasuhteisuus käy ilmi ennen kaikkea siitä, että monet asetetuista velvoitteista ovat jo osa televiestintätoimijoiden ja digitaalisen infrastruktuurin haltijoiden tavanomaisia riskinhallinta- ja liiketoiminnan jatkuvuuskäytäntöjä. Riskianalyysit, varautumissuunnitelmat, palautumisprotokollat ja valvontamekanismit ovat peruselementtejä kriittisen infrastruktuurin ja keskeisten palvelujen hallinnassa. Kuninkaallisella asetuksella ei vaadita täysin uusien rakenteiden luomista, vaan sillä järjestelmällistetään ja yhdenmukaistetaan tietyt velvoitteet, jotta kaikille velvoitetuille tahoille voidaan taata yhteiset vähimmäisvaatimukset.

Suunnitellut toimenpiteet ovat lisäksi asianmukaisia suhteessa riskien suuruuteen, joita niillä on tarkoitus lieventää. Näiden riskien vuoksi turvallisuus- ja jatkuvuussuunnitelmien, varajärjestelmien sekä varhaisilmoitusmenettelyjen laatiminen on asianmukainen ja välttämätön toimenpide vahinkojen minimoimiseksi ja palvelujen palauttamisen nopeuttamiseksi.

Asetuksessa on myös mekanismeja, joiden avulla velvoitteet voidaan räätälöidä kunkin säännellyn toimijan olosuhteiden mukaan. Erytysuunnitelmat tulee laatia ottaen huomioon kunkin verkon, palvelun tai infrastruktuurin ominaispiirteet, jotta toimijat voivat määrittää omien riskiensä kannalta välttämättömät tekniset ja organisatoriset toimenpiteet. Tämän joustavuuden ansiosta vältetään jäykkiä tai yhtenäisratkaisuja, jotka saattaisivat aiheuttaa tarpeettomia kustannuksia, ja suositaan tehokkaaseen riskinhallintaan perustuvaa lähestymistapaa.

Tapahtumien ilmoittamisen osalta nämä velvoitteet perustuvat tarpeeseen saada ajantasaista ja luotettavaa tietoa, jotta mahdollistetaan koordinaatio sellaisten tapahtumien varalta, jotka saattavat vaikuttaa suureen määrään käyttäjiä, toimijoita tai alueita. Vaaditut tiedot ovat lisäksi sellaisia, joita toimijoiden on jo nyt kerättävä ja hallinnoitava sisäisesti poikkeustilanteiden ratkaisemiseksi ja palvelujensa jatkuvuuden varmistamiseksi; ne eivät siis aiheuta kohtuutonta hallinnollista taakkaa suhteessa niiden tuomiin etuihin koordinoinnin ja reaktiokyvyn kannalta.

Sääntelyn vaikutusten arviointiraportissa todetaan myös, että sääntelystä aiheutuvat taloudelliset vaikutukset ovat hallittavia ja oikeasuhtaisia siihen yleiseen etuun nähden, jota sääntelyllä suojellaan. Säännellyille toimijoille aiheutuvat arvioidut taloudelliset kustannukset ovat 45-90 miljoonaa euroa, mutta nämä kustannukset liittyvät pääasiassa investointeihin, joilla pyritään vahvistamaan infrastruktuurin häiriönsietokykyä ja varmistamaan keskeisten palvelujen jatkuvuus. Lisäksi uusien hallinnollisten rasitteiden summaksi on arvioitu noin 19 276 euroa, joka on alhainen luku verrattuna toiminnan määrään ja asianomaisten toimijoiden taloudelliseen kokoon. Asetus ei myöskään aiheuta viranomaisille budjettikustannuksia, eikä sillä ole merkittäviä vaikutuksia kilpailuun.

Kaikista näistä syistä voidaan todeta, että toimenpide ei aiheuta kohtuutonta taakkaa sen kohteena oleville osapuolille, vaan siinä asetetaan velvoitteita, jotka ovat oikeasuhteisia, kohtuullisia ja tarpeellisia sähköisten viestintäverkkojen ja -palvelujen korkeatasoisen turvallisuuden ja häiriönsietokyvyn varmistamiseksi.

10. Viittaukset perusteksteihin:

11. Ei

12.

13. Kyllä

Maan strateginen etu

Sähköiset viestintäverkot ja -palvelut ovat kansallisen turvallisuuden, julkisten palvelujen, hätäpalvelujen, taloudellisen toiminnan ja alueellisen yhteenkuuluvuuden kannalta välttämätöntä infrastruktuuria.

14. Ei

15. Kyllä

16.

TBT-näkökohta: Ei

SPS-näkökohta: Ei



EUROPEAN COMMISSION

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

Euroopan komissio

Yhteysviranomainen direktiivin (EU) 2015/1535

Sähköposti: grow-dir2015-1535-central@ec.europa.eu