



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Single Market Enforcement

Notification of Regulatory Barriers

Teatise number : 2026/0346/ES (Spain)

Kuningliku määruse eelnõu elektrooniliste sidevõrkude ja -teenuste ning teatud digitaalsete infrastruktuuride turvalisuse ja vastupidavuse kohta.

Teatise saamise kuupäev : 08/07/2026

Ooteaja lõpp : 09/10/2026

Message

Sõnum 001

Komisjoni teade - TRIS/(2026) 1822

Direktiiv (EL) 2015/1535

Teavitamine: 2026/0346/ES

Liikmesriigi teade teksti kavandi kohta

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.ET

1. MSG 001 IND 2026 0346 ES ET 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 - Telekommunikatsioon

5. Kuningliku määruse eelnõu elektrooniliste sidevõrkude ja -teenuste ning teatud digitaalsete infrastruktuuride turvalisuse ja vastupidavuse kohta.

6. Selle eesmärk on tugevdada Hispaania elektrooniliste sidevõrkude ja -teenuste, nendega seotud vahendite ja teatud digitaalsete infrastruktuuride turvalisust, vastupidavust ja järjepidevust.

7.

8. Selle kuningliku määruse on tagada Hispaania elektrooniliste sidevõrkude ja -teenuste, nendega seotud vahendite ja teatud digitaalsete infrastruktuuride turvalisus, vastupidavus ja järjepidevus.

Eesmärk on tagada oluliste teenuste osutamine turvajuhtumite, teenuse katkestuste või oluliste halvenemiste korral ning reguleerida kohustust sellistest juhtumitest ametiasutustele teatada.

Kohustatud isikud on avalike elektrooniliste sidevõrkude operaatorid, avalikult kättesaadavate teenuste osutajad, seotud vahendite ja digitaalsete infrastruktuuride, näiteks allveekaablite, satelliitsüsteemide, andmetöötluskeskuste (DPC-de), sisuedastusvõrkude (CDN-ide) ja Interneti vahetuspunktide (IXP-de) operaatorid, samuti teatud aspektides hädaabikõnede keskused 112 ja avalikud hoiatussüsteemid. Tunnistatakse ka nende võrkude ja infrastruktuuride olulisust hädaolukordades.

Koostatud on riiklik julgeoleku- ja vastupidavuskava, milles määratakse kindlaks kriisidele reageerimise korraldus ja institutsioonilised koordineerimismehhanismid. Samuti on selles sätestatud kohustatud isikute kohustus koostada iga kohustatud isiku kohta „üldkava“ ning igat liiki võrgu ja konkreetsete teenuste kohta „konkreetsed kavad“. Need peavad hõlmama riskianalüüsi, olulise infrastruktuuri kindlaksmääramist, ennetusmeetmeid, taastamismehhanisme ja tegevusjuhendeid erinevate stsenaariumite jaoks, nagu näiteks elektrikatkestused, loodusõnnetused, tulekahjud, IT-rikked või küberrünnakud.

Telekommunikatsiooniteenuste järjepidevuse tagamiseks kehtestatakse konkreetsed kohustused. Operaatorid võtavad meetmeid, et vähendada juhtumite mõju ja tagada oluliste teenuste, eelkõige hädaolukorras side toimimine.

Erandjuhtudel võivad nad anda eelistuse teatud liiki liiklusele, näiteks hädaabikõnede või kõne- ja SMS-teenustele, järgides seejuures alati tehnoloogilise neutraalsuse põhimõtet. Lisaks on elutähtsa infrastruktuuri jaoks kehtestatud energiasõltumatuse miinimumnõuded ja mobiilsidevõrkudele on kehtestatud kohustus tagada järk-järgult vähemalt 4-tunnine varuvõimsus 75%-le elanikkonnast 3 aasta jooksul.

See hõlmab süsteemi oluliste juhtumite, mida ei peeta küberturvalisuse juhtumiteks, teatamiseks, kusjuures viimaseid reguleerivad NIS2 direktiiv ja CER direktiiv. Operaatorid teavitavad riigi sekretariaati igast olulisest juhtumist 1 tunni jooksul pärast sellest teadasaamist ning esitavad seejärel korrapäraselt ajakohastatud teavet häire kestuse kohta, millele järgneb lõpparuanne, kui teenus on taastatud.

Hädaabinumbri 112 ja üldsuse hoiatamissüsteemide kaudu toimuva hädaabiside jaoks on kehtestatud erimeetmed. Nii hädaabikõnekeskused kui ka operaatorid peavad kehtestama varusüsteemid ja tegevuse jätkuvuse tagamise meetmed, koostama konkreetsed situatsioonikavad ning teatama viivitamatult kõigist nende teenuste häiretest, mida loetakse automaatselt olulisteks vahejuhtumiteks.

Kuninglik määrus sätestab meetmed ja mehhanismid kriitiliste üksuste küberturvalisust ja vastupidavust käsitlevate määrustega (NIS2 direktiiv ja CER direktiiv) kooskõlastamiseks, turvalisuse ja vastupidavuse koordineerimiskomitee loomise ning juhtumite haldamise ja teabevahetuse digitaalsete platvormide tulevase kasutuselevõtu. Kokkuvõttes tähendab see telekommunikatsioonisektorile ja kriitilise tähtsusega digitaalsetele infrastruktuuridele kehtivate turvalisuse, tegevuse järjepidevuse ja järelevalve kohustuste märkimisväärselt tugevdamist.

9. Majanduse ja avalike teenuste üha suurem digitaliseerimine on märkimisväärselt suurendanud sõltuvust elektroonilistest sidevõrkudest ja neid toetavatest digiinfrastruktuuridest. Selline olukord on toonud esile nõrkused ja



EUROPEAN COMMISSION

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

riskid, mis ei piirdu üksnes küberturvalisusega, vaid mõjutavad ka füüsilist turvalisust ja infrastruktuuride suutlikkust vastu pidada ebasoodsatele sündmustele ja neist taastuda. Sellega seoses peetakse määruses vajalikuks tugevdada suutlikkust ennetada juhtumeid, mis võivad ohustada elektrooniliste sidevõrkude ja teenuste kättesaadavust, terviklust või toimimist, ning neile reageerida ja neist taastuda.

Kuningliku määruse seletuskirjas tuuakse esile mitu hiljutist sündmust, mis on näidanud vajadust suurendada nende infrastruktuuride vastupidavust. Nende hulgas nimetatakse loodusnähtusi, nagu 2021. aasta vulkaanipurse La Palmale ja 2024. aastal Hispaania erinevaid piirkondi mõjutanud külm madalrõhkkond, aga ka mitte-looduslikku päritolu sündmusi, nagu näiteks hiljutine üleriigiline elektrikatkestus. Need sündmused näitasid, et nii äärmuslikud loodusnähtused kui ka tehnilised või elektrikatkestused võivad põhjustada märkimisväärsed häireid sidevõrkudes ning ohustada üldsusele ja riigiasutustele oluliste teenuste järjepidevust.

Lisaks muudab digiüleminek põhjalikult telekommunikatsioonivõrkude ülesehitust ja toimimist. Selliste tehnoloogiate nagu asjade internet (IoT), tehisintellekt (AI), suured andmehulgad, pilvandmetöötlus ja teenuste virtualiseerimine kasutuselevõtt on võimaldanud tõsta tõhusust, parandada ühenduvust ja edendada majandusarengut, kuid samal ajal on see suurendanud süsteemide keerukust ning tekitanud uusi tegevus- ja turvariske. Seepärast peab komitee oluliseks, et õigusraamistikku arendataks edasi, et neid riske ennetada ning tagada kaitse- ja vastupanuvõime asjakohane tase. Õiguslikust seisukohast põhineb algatus peamiselt elektrooniliste sidevõrkude ja -teenuste terviklikkust ja turvalisust käsitleva seaduse 11/2022 (üldine telekommunikatsiooniseadus) artiklil 63. Lisaks põhineb see olemasolevatel 5G-võrgu turvalisust käsitlevatel õigusaktidel, eelkõige kuninglikul määrusel 7/2022, kuninglikul määrusel 12/2018 võrkude ja infosüsteemide turvalisuse kohta ning kuninglikul määrusel 443/2024, millega kiidetakse heaks 5G-võrkude ja -teenuste riiklik turberaamistik. Eespool öeldust hoolimata on need määrused küll toonud kaasa märkimisväärsed edusamme, kuid tuleb välja töötada konkreetne raamistik, mis käsitleks terviklikult kõigi elektrooniliste sidevõrkude ja -teenuste ning teatavate digitaalsete infrastruktuuride turvalisust ja vastupidavust.

Lõpuks selgitatakse tekstis, et uue kuningliku määruse eesmärk on täiendada tulevasi Hispaania õigusakte, mis käsitlevad elutähtsa teenuse osutajate küberturvalisust ja vastupidavusvõimet. Seega kehtivad NIS2 ja CERi ülevõtmise määrustest tulenevad kohustused ka edaspidi täielikult küberturvalisuse juhtumite ja nende juhtumite suhtes, mis mõjutavad digitaalsete võrke, teenuseid ja taristuid ning mida käesolevas kuninglikus määruses sõnaselgelt ei reguleerita. Eesmärk on seega tagada kooskõla erinevate regulatiivsete vahendite vahel, vältida regulatiivset kattumist ja luua terviklik kaitseüsteem, mis tugevdab Hispaania ühiskonna ja majanduse toimimiseks hädavajalikku telekommunikatsiooni ja digitaalset infrastruktuuri turvalisust, järjepidevust ja vastupidavust.

9a. Kõnealune meede on sobiv selleks, et saavutada seatud eesmärk – tugevdada elektrooniliste sidevõrkude ja -teenuste ning teatavate digitaalsete infrastruktuuride turvalisust, vastupidavust ja järjepidevust.

Viimaste aastate kogemus on näidanud, et telekommunikatsioonivõrgud on ühiskonna toimimiseks hädavajalikud infrastruktuurid, nagu selgus nii COVID-19-pandeemia ajal kui ka äärmuslikest loodusnähtustest, elektrikatkestustest või turvalisusega seotud vahejuhtumitest tingitud hädaolukordades, mis on mõjutanud teenuste kättesaadavust. Selle stsenaariumi puhul on asjakohane võtta vastu konkreetne õigusraamistik, et tugevdada suutlikkust ennetada juhtumeid, mis võivad ohustada elektroonilise side järjepidevust, neile reageerida ja neist taastuda.

Kõnealuse määrusega rakendatakse seaduse nr 11/2022 (telekommunikatsiooni üldseadus) artiklis 63 sisalduvaid sätteid. Samuti täiendab ja kohandab see õigusraamistikku vastavalt tehnoloogia arengule ning uutele riskidele, mis on seotud digitaliseerimise, võrgu virtualiseerimise, pilvandmetöötluse, tehisintellekti (AI) ja asjade internetiga (IoT), mille üha laiem kasutus suurendab nii füüsilise kui ka digitaalset iseloomuga haavatavuste ohtu. Sellega seoses on kuninglik määrus sobiv vahend, et määrata kindlaks valdkondlikud kohustused, mis võimaldavad läheneda telekommunikatsioonisektori tehnilistele ja tegevuslikele iseärasustele terviklikult.

Meetme asjakohasus väljendub eelkõige ennetus- ja planeerimismehhanismide rakendamises, mille eesmärk on parandada ettevõtjate valmisolekut kriisilukordadeks. Kohustus koostada võrgustiku või teenuse kaupa üld- ja erikavad koos riikliku julgeoleku- ja vastupidavuskava ning riikliku tsiviilhädaolukorra lahendamise kavaga võimaldab kehtestada konkreetset menetlust riskide tuvastamiseks, ennetamiseks, neile reageerimiseks ja nendest taastumiseks.

Samuti on juhtumitest teatamise menetluste ajakohastamine asjakohane meede, et parandada pädevate asutuste järelevalve- ja kriisiohjesuutlikkust. Kogemused on näidanud, et teadete kriteeriume, tähtaegu ja sisu tuleb kohandada keerukama tehnoloogilise ja operatiivse reaalsusega.

Lisaks sobib see meede hästi eriti tundlike teenuste, nagu näiteks numbril 112 toimuva hädaabikõnede ja avalike hoiatussüsteemide kaitse tugevdamiseks, kehtestades nii operaatoritele kui ka hädaabikõnekeskustele konkreetset



EUROPEAN COMMISSION

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

kohustused seoses teenuse järjepidevuse, varundatuse ja teavitamisega. See aitab tagada, et need olulised teenused toimiksid isegi olukordades, kus sideinfrastruktuur on tõsiselt häiritud.

Ametiasutuste ning riiklike ja Euroopa ametiasutuste vaheliste koostöömehhanismide loomine ning erinevaid sidusrühmi kaasava alalise koordineerimiskomitee loomine on asjakohane vahend teabevahetuse, institutsioonilise koordineerimise ning parimate tavade vastuvõtmise edendamiseks julgeoleku ja vastupidavuse valdkonnas.

Lõpuks on kõnealune meede kooskõlas NIS2- ja CER-direktiividest tuleneva Euroopa õigusraamistikuga, tagades nõuetekohase kooskõlastamise tulevaste riiklike ülevõtmisaktidega ning vältides regulatiivseid lünki sektoris, mis on strateegilise tähtsusega majanduse ja riikliku julgeoleku seisukohalt.

9b. Kuningliku määruse vastuvõtmine vastab tegelikule ja tõendatud vajadusele tugevdada ühiskonna, majanduse ja avalike teenuste toimimiseks hädavajalikuks muutunud infrastruktuuride ennetus-, kaitse- ja taastumissuutlikkust. Majandus- ja ühiskondliku tegevuse üha suurenev digitaliseerumine koos kasvava sõltuvusega elektroonilistest sidevõrkudest ja -teenustest, samuti sellised sündmused nagu La Palma vulkaanipurse, riigi erinevaid piirkondi mõjutanud külm madalrõhkkond või hiljutine elektrikatkestus on näidanud, et elektroonilised sidevõrgud ja -teenused on avatud erinevatele ohtudele, mis võivad tõsiselt ohustada oluliste teenuste osutamist kodanikele, ettevõtetele ja riigiasutustele. Need juhtumid on toonud esile vajaduse tugevdada digiinfrastruktuuri vastupanuvõimet ning parandada hädaolukordadele ja kriisidele reageerimise võimet.

See meede on vajalik, et rakendada ja jõustada seaduse 11/2022 (telekommunikatsiooni üldseadus) artiklit 63, milles on sätestatud operaatorite kohustus juhtida asjakohaselt turvariske ning tagada oma võrkude ja teenuste terviklikkus.

Oluline on koostada eeskirjad, milles sätestatakse üksikasjalikumalt planeerimise, ennetamise, juhtumitest teatamise, institutsioonilise koordineerimise ja järelevalvega seotud kohustused, mida ettevõtjad ja muud asjaomased isikud peavad täitma.

Samuti on määruse vastuvõtmise vajadus põhjendatud sellega, et praegu kehtiv juhtumitest teatamise õigusraamistik on osaliselt aegunud. Olemasolevad menetlused ei vasta enam piisavalt digivõrke, -teenuseid ja -infrastruktuuri mõjutada võivate juhtumite keerukusele. Erinevate juhtumite, teabevahetusmenetluste ja aruandlustähtaegade ajakohastamine on vajalik selleks, et pädevatel asutustel oleks piisav ja ajakohane teave, koordineerimaks kiiret ja tõhusat reageerimist kriisiolukordadele.

Samuti tuleb kehtestada konkreetsed mehhanismid, et tagada eriti kriitiliste teenuste järjepidevus, näiteks hädaabiside 112 numbri ja avalike hoiatussüsteemide kaudu. Kogemus näitab, et nende teenuste mis tahes katkemine avaldab otsest mõju inimeste elu ja füüsilise puutumatuse kaitsele ning hädaolukordade juhtimisele. Seetõttu kehtestab määrus nii operaatoritele kui ka hädaabikeskustele konkreetsed kohustused seoses planeerimise, varusüsteemide ja tegevuse järjepidevusega.

Lisaks on see meede vajalik riiklike ja Euroopa tasandi koostöömehhanismide täiustamiseks ning spetsiaalse koordineerimiskomitee loomiseks, et hõlbustada teabevahetust, kogemuste jagamist ja ühiste menetluste kehtestamist selliste juhtumite puhul, mis oma olemuselt mõjutavad tavaliselt mitut käitajat ja infrastruktuuri korraga.

Lõpuks on vaja tagada Hispaania õigussüsteemi sidusus NIS2 ja CER direktiividest tuleneva uue Euroopa regulatiivse raamistikuga. Need Euroopa õigusaktid tugevdavad kriitilise infrastruktuuri turvalisuse, riskijuhtimise ja vastupidavusega seotud kohustusi ning nõuavad liikmesriikidelt tõhusate mehhanismide väljatöötamist juhtumite ennetamiseks, avastamiseks, nende reageerimiseks ja nendest taastumiseks.

9c. Kavandatud meede ei tekita taotletavate eesmärkidega võrreldes ülemäärast või ebaproportsionaalset koormust, kuna sellega kehtestatavad kohustused vastavad vajadusele tagada ühiskonna, majanduse ja avalike teenuste toimimiseks oluliste infrastruktuuride turvalisus, vastupidavus ja järjepidevus.

Meetme proportsionaalsus ilmneb eelkõige sellest, et paljud sätestatud kohustused on juba osa telekommunikatsioonioperaatorite ja digitaalse infrastruktuuri haldajate tavapäraest riskijuhtimise ja tegevuse järjepidevuse tavadest. Riskianalüüsid, hädaolukorra lahendamise kavad, taasteprotokollid ja järelevalvemehhanismid on elutähtsa infrastruktuuri ja elutähtsate teenuste haldamise standardelemendid. Kuningliku määrusega ei nähta ette täiesti uute struktuuride loomist, vaid pigem süstematiseeritakse ja ühtlustatakse teatavaid kohustusi, et tagada kõigile kohustatud isikutele ühised miinimumstandardid.

Lisaks on kavandatud meetmed proportsionaalsed nende riskide ulatusega, mida nendega kavatakse leevendada. Neid riske silmas pidades on turvalisuse ja vastupidavuse kavade, varundusmehhanismide ning varajase teavitamise korra kehtestamise nõue mõistlik ja vajalik meede kahjude vähendamiseks ning teenuste taastamise kiirendamiseks.



EUROPEAN COMMISSION

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

Määrus sisaldab ka mehhanisme, mis võimaldavad kohandada kohustusi vastavalt iga reguleeritud üksuse olukorrale. Konkreetsed kavad tuleks koostada, võttes arvesse iga võrgu, teenuse või infrastruktuuri eripärasid, et võimaldada operaatoritel määrata kindlaks oma konkreetsetele riskidele kõige sobivamad tehnilised ja organisatsioonilised meetmed. Selline paindlikkus aitab vältida ühtsete või jäikade lahenduste pealesurumist, mis võiksid tekitada tarbetuid kulusid, ning soodustab tõhusal riskijuhtimisel põhinevat lähenemisviisi.

Juhtumitest teatamise osas on need kohustused põhjendatud vajadusega saada ajakohast ja usaldusväärset teavet, et koordineerida reageerimist juhtumitele, mis võivad mõjutada suurt arvu kasutajaid, operaatoreid või piirkondi. Lisaks on nõutav teave see, mida operaatorid on juba kohustatud ettevõttesiseselt koguma ja haldama, et lahendada juhtume ja tagada oma teenuste järjepidevus; seega ei tekita see ebaproportsionaalset halduskoormust võrreldes kasuga, mida see toob koordineerimise ja reageerimisvõime seisukohast.

Regulatiivse mõju hindamise aruandes järeldatakse ka, et määrusest tulenev majanduslik mõju on hallatav ja proportsionaalne kaitstava avaliku huviga. Kuigi reguleeritud üksuste hinnangulised rahalised kulud jäävad vahemikku 45–90 miljonit eurot, on need kulud peamiselt seotud investeeringutega, mille eesmärk on tugevdada infrastruktuuri vastupidavust ja tagada oluliste teenuste järjepidevus. Lisaks on uus halduskoormus hinnanguliselt ligikaudu 19 276 eurot, mis on väike summa võrreldes asjaomaste ettevõtjate tegevuse mahu ja majandusliku suurusega. Lisaks ei too määrus avaliku sektori asutustele kaasa eelarvekulusid ega mõjuta märkimisväärselt konkurentsi.

Kõigi nende põhjuste tõttu on alust järeldata, et kõnealune meede ei pane selle kohaldamisalasse kuuluvatele osalistele ülemääraast koormust, vaid kehtestab kohustused, mis on proportsionaalsed, mõistlikud ja vajalikud elektrooniliste sidevõrkude ja -teenuste kõrge turvalisuse ja vastupidavuse tagamiseks.

10. Viited alustekstidele:

11. Ei

12.

13. Jah

Riigi strateegilised huvid

Elektroonilised sidevõrgud ja -teenused on riigi julgeoleku, avalike teenuste, hädaabiteenuste, majandustegevuse ja territoriaalse ühtekuuluvuse jaoks hädavajalik infrastruktuur.

14. Ei

15. Jah

16.

TBT aspekt: Ei

SPS aspekt: Ei

Euroopa Komisjon

Direktiivi (EL) 2015/1535 üldine kontaktinfo

e-post: grow-dir2015-1535-central@ec.europa.eu