



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Pranešimo numeris : 2026/0346/ES (Spain)

Karaliaus dekreto dėl elektroninių ryšių tinklų ir paslaugų bei tam tikrų skaitmeninių infrastruktūrų saugumo ir atsparumo projektas.

Gauti duomenys : 08/07/2026

Status quo pabaiga : 09/10/2026

Message

Pranešimas 001

Komisijos pranešimas - TRIS/(2026) 1822

Direktyva (ES) 2015/1535

Pranešimas: 2026/0346/ES

Valstybės narės pranešimas apie teksto projektą

Notification – Notification – 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 - Καμία 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.LT

1. MSG 001 IND 2026 0346 ES LT 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

Calle Poeta Joan Maragall 41

28020 Madrid



EUROPEAN COMMISSION

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

+34 913462750

4. 2026/0346/ES - V00T - Telekomunikacijos

5. Karaliaus dekreto dėl elektroninių ryšių tinklų ir paslaugų bei tam tikrų skaitmeninių infrastruktūrų saugumo ir atsparumo projektas.

6. Juo siekiama sustiprinti elektroninių ryšių tinklų ir paslaugų, su jais susijusių įrenginių bei tam tikrų skaitmeninių infrastruktūrų Ispanijoje saugumą, atsparumą ir veiklos tęstinumą.

7.

8. Karaliaus dekretu siekiama užtikrinti elektroninių ryšių tinklų ir paslaugų, su jais susijusių įrenginių bei tam tikrų skaitmeninių infrastruktūrų Ispanijoje saugumą, atsparumą ir veiklos tęstinumą.

Tikslas – užtikrinti būtinųjų paslaugų teikimą saugumo incidentų, paslaugų teikimo pertraukų ar žymių paslaugų kokybės pablogėjimų atveju, taip pat reglamentuoti pareigą pranešti apie tokius incidentus valdžios institucijoms.

Įpareigoti subjektai – tai viešųjų elektroninių ryšių tinklų operatoriai, viešai prieinamų paslaugų teikėjai, susijusių įrenginių ir skaitmeninių infrastruktūrų, pavyzdžiui, povandeninių kabelių, palydovinių sistemų, duomenų tvarkymo centrų (DTC), turinio platinimo tinklų (TPT) ir interneto mainų taškų (IXP), operatoriai, taip pat tam tikrais atžvilgiais 112 skubios pagalbos iškvietimo centrai ir viešosios įspėjimo sistemos. Taip pat pripažįstama šių tinklų ir infrastruktūrų esminė svarba ekstremaliosiose situacijose.

Parengtas nacionalinis saugumo ir atsparumo planas, kuriame bus apibrėžtas reagavimo į krizes organizavimas ir instituciniai koordinavimo mechanizmai. Jame taip pat nustatoma įpareigotųjų subjektų pareiga parengti „bendrąjį planą“ kiekvienam įpareigotajam subjektui ir „konkrečius planus“ kiekvienam tinklo tipui bei konkrečioms paslaugoms. Juose turi būti numatyta rizikos analizė, svarbiausios infrastruktūros duomenys, prevencinės priemonės, atkūrimo mechanizmai ir veiksmų protokolai įvairiems scenarijams, pavyzdžiui, elektros tiekimo pertraukoms, stichinėms nelaimėms, gaisrams, IT gedimams ar kibernetinėms atakoms.

Siekiant užtikrinti telekomunikacijų paslaugų tęstinumą, nustatomi konkretūs įpareigojimai. Operatoriai imasi priemonių, kad kuo labiau sumažintų incidentų poveikį ir užtikrintų esminių paslaugų, visų pirma ekstremaliųjų situacijų ryšių, veikimą. Išimtiniais atvejais jie gali teikti pirmenybę tam tikroms duomenų srauto rūšims, pavyzdžiui, ekstremaliųjų situacijų ryšiams arba balso ir SMS paslaugoms, visada laikydamiesi technologinio neutralumo principo. Be to, nustatyti būtiniausi energetinio savarankiškumo reikalavimai, taikomi svarbiausiai infrastruktūrai, o judriojo ryšio tinklams nustatytas įpareigojimas per trejus metus palaipsniui užtikrinti 75 proc. gyventojų ne mažiau kaip keturių valandų atsarginės elektros energijos tiekimą.

Jis apima pranešimo apie reikšmingus incidentus, kurie nelaikomi kibernetinio saugumo incidentais, sistemą; pastarieji reglamentuojami TIS 2 direktyvoje ir Direktyvoje dėl ypatingos svarbos subjektų atsparumo. Operatoriai privalo pranešti Valstybės sekretariatui apie bet kokią reikšmingą incidentą per vieną valandą nuo to momento, kai apie jį sužino, ir vėliau reguliariai teikti naujausią informaciją, kol trunka sutrikimas, o atkūrus paslaugą – pateikti galutinę ataskaitą.

Nustatomos specialios ekstremaliųjų situacijų ryšio naudojant telefono numerį 112 ir viešojo įspėjimo sistemas priemonės. Tiek skubios pagalbos iškvietimo centrai, tiek operatoriai privalo įgyvendinti pertekumo ir veiklos tęstinumo priemones, parengti konkrečius nenumatytų atvejų planus ir nedelsiant pranešti apie bet kokius šių paslaugų sutrikimus, kurie automatiškai klasifikuojami kaip reikšmingi incidentai.

Karaliaus dekretu nustatytos koordinavimo su reglamentais dėl ypatingos svarbos subjektų kibernetinio saugumo ir atsparumo (TIS 2 direktyva ir Direktyva dėl ypatingos svarbos subjektų atsparumo) priemonės ir mechanizmai, Saugumo ir atsparumo koordinavimo komiteto įsteigimas ir būsimas skaitmeninių incidentų valdymo ir komunikacijos platformų diegimas. Apskritai juo gerokai sustiprinami telekomunikacijų sektoriui ir ypatingos svarbos skaitmeninėms infrastruktūroms taikomi saugumo, tęstinumo ir priežiūros įpareigojimai.

9. Dėl didėjančio ekonomikos ir viešųjų paslaugų skaitmeninimo gerokai padidėjo priklausomybė nuo elektroninių ryšių tinklų ir juos palaikančių skaitmeninių infrastruktūrų. Ši situacija parodė esant pažeidžiamumą ir riziką, kurie neapsiriboja tik kibernetinio saugumo sritimi, bet taip pat daro poveikį fiziniam saugumui ir infrastruktūrų gebėjimui



EUROPEAN COMMISSION

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

atlaikyti nepageidaujamus įvykius ir po jų atsigauti. Atsižvelgiant į tai, reglamente manoma, kad būtina stiprinti incidentų, kurie galėtų pakenkti elektroninių ryšių tinklų ir paslaugų prieinamumui, vientisumui ar veikimui, prevencijos, reagavimo į juos ir veiklos atkūrimo pajėgumus.

Karaliaus dekreto aiškinamajame memorandume atkreipiamas dėmesys į kelis pastarojo meto įvykius, kurie parodė, jog reikia didinti šių infrastruktūrų atsparumą. Tarp jų paminėti tokie gamtiniai reiškiniai kaip 2021 m. ugnikalnio išsiveržimas La Palmoje ir 2024 m. įvairias Ispanijos vietas paveikęs šaltas žemo slėgio frontas, taip pat negamtinės kilmės įvykiai, pavyzdžiui, neseniai įvykęs visos šalies masto elektros tiekimo sutrikimas. Šie įvykiai parodė, kad tiek ekstremalūs gamtos reiškiniai, tiek techniniai gedimai ar elektros tiekimo sutrikimai gali smarkiai sutrikdyti ryšių tinklų veiklą ir kelti grėsmę esminių paslaugų teikimo tęstinumui visuomenei ir valdžios institucijoms.

Be to, dėl skaitmeninimo iš esmės keičiama telekomunikacijų tinklų architektūra ir veikimas. Tokios technologijos kaip daiktų internetas (IoT), dirbtinis intelektas (DI), didieji duomenys, debesų kompiuterija ir paslaugų virtualizacija leido padidinti veiksmingumą, ryšio galimybes ir paskatinti ekonominę plėtrą, tačiau kartu padidino sistemų sudėtingumą ir sukėlė naujų veiklos bei saugumo rizikų. Todėl manoma, kad būtina tobulinti reguliavimo sistemą, siekiant numatyti šias rizikas ir užtikrinti tinkamą apsaugos ir atsparumo lygį.

Teisiniu požiūriu iniciatyva iš esmės grindžiama Įstatymo Nr. 11/2022 dėl elektroninių ryšių tinklų ir paslaugų vientisumo ir saugumo (Bendrojo telekomunikacijų įstatymo) 63 straipsniu. Be to, jis grindžiamas galiojančiais teisės aktais dėl 5G tinklo saugumo, visų pirma Karaliaus įstatyminiu dekretu Nr. 7/2022, Karaliaus įstatyminiu dekretu Nr. 12/2018 dėl tinklų ir informacinių sistemų saugumo ir Karaliaus dekretu Nr. 443/2024, kuriuo patvirtinama 5G tinklų ir paslaugų nacionalinio saugumo sistema. Nepaisant to, kas išdėstyta pirmiau, nors dėl šių reglamentų padaryta didelė pažanga, būtina parengti specialią sistemą, kurioje būtų visapusiškai atsižvelgiama į visų elektroninių ryšių tinklų ir paslaugų, taip pat tam tikrų skaitmeninių infrastruktūrų saugumą ir atsparumą.

Galiausiai tekste paaiškinama, kad naujuoju Karaliaus dekretu siekiama papildyti būsimus Ispanijos teisės aktus dėl ypatingos svarbos subjektų kibernetinio saugumo ir atsparumo. Todėl įpareigojimai, kylantys iš reglamentų, kuriais TIS 2 direktyva ir Direktyva dėl ypatingos svarbos subjektų atsparumo perkeliama į nacionalinę teisę, ir toliau bus visapusiškai taikomi kibernetinio saugumo incidentams ir tiems incidentams, kurie daro poveikį skaitmeniniams tinklams, paslaugoms ir infrastruktūroms ir kurie nėra aiškiai reglamentuojami šiuo Karaliaus dekretu. Taigi siekiama užtikrinti įvairių reguliavimo priemonių nuoseklumą, išvengti reguliavimo dubliavimosi ir sukurti visapusišką apsaugos sistemą, kuri sustiprintų telekomunikacijų ir skaitmeninės infrastruktūros, būtinos Ispanijos visuomenės ir ekonomikos veikimui, saugumą, tęstinumą ir atsparumą.

9a. Priemonė yra tinkama siekiamam tikslui – stiprinti elektroninių ryšių tinklų ir paslaugų bei tam tikrų skaitmeninių infrastruktūrų saugumą, atsparumą ir tęstinumą – pasiekti.

Pastarųjų metų patirtis parodė, kad telekomunikacijų tinklai yra esminė visuomenės veikimo infrastruktūra, kaip paaiškėjo per COVID-19 pandemiją, taip pat esant nepaprastosioms padėtimis, susidarančioms dėl ekstremalių gamtinių įvykių, elektros energijos tiekimo nutraukimo ar saugumo incidentų, turėjusių įtakos paslaugų prieinamumui. Pagal šį scenarijų tikslinga priimti specialią reguliavimo sistemą, kad būtų sustiprinti pajėgumai užkirsti kelią incidentams, dėl kurių gali kilti pavojus elektroninių ryšių tęstinumui, į juos reaguoti ir po jų atsigauti.

Reglamentu įgyvendinamos Įstatymo Nr. 11/2022 (Bendrasis telekomunikacijų įstatymas) 63 straipsnio nuostatos. Be to, juo reguliavimo sistema papildoma ir pritaikoma prie technologinių pokyčių bei naujų rizikų, susijusių su skaitmeninimu, tinklų virtualizavimu, debesų kompiuterija, dirbtiniu intelektu ir daiktų internetu (IoT), kuriuos vis plačiau diegiant didėja tiek fizinio, tiek skaitmeninio pobūdžio pažeidžiamumas. Šiuo atžvilgiu Karaliaus dekretas yra tinkama priemonė nustatyti sektoriaus įsipareigojimus, kuriais sudaromos sąlygos visapusiškai atsižvelgti į telekomunikacijų sektoriaus techninius ir veiklos ypatumus.

Priemonės tinkamumą visų pirma atspindi prevencinių ir planavimo mechanizmų, kuriais siekiama pagerinti operatorių pasirengimą krizinėse situacijose, įtraukimas. Įpareigojimas parengti „bendruosius planus“ ir „konkrečius planus“ pagal tinklą ar paslaugą, kartu su „nacionalinio saugumo ir atsparumo plano“ ir „nacionalinio civilinių ekstremaliųjų situacijų valdymo plano“ rengimu, suteikia galimybę nustatyti konkrečias rizikos nustatymo, prevencijos, reagavimo ir atkūrimo procedūras.

Be to, pranešimo apie incidentus tvarkos atnaujinimas yra tinkama priemonė, skirta pagerinti kompetentingų institucijų stebėsenos ir krizių valdymo gebėjimus. Patirtis parodė, kad būtina pritaikyti pranešimų kriterijus, terminus ir turinį prie sudėtingesnių technologinių ir veiklos sąlygų.

Be to, ši priemonė puikiai tinka stiprinti ypač jautrių paslaugų, pavyzdžiui, skubios pagalbos iškvietimo numeriu 112 ir



EUROPEAN COMMISSION

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

visuomenės įspėjimo sistemų, apsaugą, nustatant tiek operatoriams, tiek skubios pagalbos iškvietimo centrams konkrečius įpareigojimus, susijusius su veiklos tęstinumu, pertekliumu ir pranešimų teikimu. Tai padeda užtikrinti, kad šios ypatingos svarbos paslaugos būtų toliau teikiamos net ir tais atvejais, kai ryšių infrastruktūra yra labai sutrikdyta. Valdžios institucijų ir nacionalinių bei Europos valdžios institucijų bendradarbiavimo mechanizmų sukūrimas, taip pat nuolatinio koordinavimo komiteto, kuriame dalyvautų įvairūs suinteresuotieji subjektai, įsteigimas yra tinkama priemonė skatinti keitimąsi informacija, institucinį koordinavimą ir geriausios praktikos taikymą saugumo ir atsparumo srityje. Galiausiai ši priemonė atitinka Europos reguliavimo sistemą, nustatytą TIS 2 direktyvoje ir Direktyvoje dėl ypatingos svarbos subjektų atsparumo, užtikrinant tinkamą koordinavimą su ateityje priimamais nacionaliniais teisės aktais dėl perkėlimo į nacionalinę teisę, ir padedant išvengti reguliavimo spragų sektoriuje, kuris yra strategiškai svarbus ekonomikai ir nacionaliniam saugumui.

9b. Priėmus Karaliaus dekretą reaguojama į realų ir įrodytą poreikį stiprinti infrastruktūrą, kurios tapo būtinos visuomenės, ekonomikos ir viešųjų paslaugų veikimui, prevencijos, apsaugos ir atkūrimo pajėgumus.

Vis didėjantis ekonominės ir socialinės veiklos skaitmeninimas, kartu su vis didesniu priklausomumu nuo elektroninių ryšių tinklų ir paslaugų, taip pat tokie įvykiai kaip ugnikalnio išsiveržimas La Palmoje, šaltas žemo slėgio frontas, paveikęs įvairias šalies vietas, ar neseniai įvykę elektros tiekimo sutrikimas, parodė, kad elektroninių ryšių tinklai ir paslaugos susiduria su įvairiausiomis rizikomis, kurios gali rimtai pakenkti esminių paslaugų teikimui piliečiams, įmonėms ir valdžios institucijoms. Šie incidentai išryškino poreikį didinti skaitmeninės infrastruktūros atsparumą ir gerinti gebėjimą reaguoti į ekstremaliąsias situacijas ir krizes.

Ši priemonė būtina siekiant įgyvendinti Įstatymo Nr. 11/2022 (Bendrojo telekomunikacijų įstatymo) 63 straipsnį, kuriuo nustatomas operatorių įpareigojimas tinkamai valdyti saugumo rizikas ir užtikrinti savo tinklų bei paslaugų vientisumą. Labai svarbu parengti reglamentus, kuriuose būtų išsamiau nustatytos planavimo, prevencijos, pranešimo apie incidentus, institucinio koordinavimo ir priežiūros pareigos, kurias turi vykdyti operatoriai ir kitos susijusios šalys.

Be to, reguliavimo poreikis grindžiamas tuo, kad šiuo metu galiojanti pranešimų apie incidentus reguliavimo sistema iš dalies pasenusi. Šiuo metu taikoma tvarka nebeatitinka šiuolaikinių incidentų, galinčių turėti įtakos skaitmeniniams tinklams, paslaugoms ir infrastruktūrai, sudėtingumo. Būtina atnaujinti incidentų rūšis, komunikacijos procedūras ir pranešimo terminus, kad kompetentingos institucijos turėtų pakankamai naujausios informacijos ir galėtų koordinuoti greitą ir veiksmingą reagavimą į krizines situacijas.

Be to, būtina sukurti specialius mechanizmus, kurie užtikrintų ypatingos svarbos paslaugų, pavyzdžiui, skubios pagalbos iškvietimo numeriu 112 ir visuomenės įspėjimo sistemų, tęstinumą. Patirtis rodo, kad bet koks šių paslaugų teikimo sutrikimas gali turėti tiesioginių pasekmių žmonių gyvybės ir fizinės neliečiamybės apsaugai bei ekstremaliųjų situacijų valdymui. Todėl reglamentu operatoriams ir skubios pagalbos iškvietimo centrams nustatomi konkretūs įpareigojimai, susiję su planavimu, pertekliumu ir veiklos tęstinumu.

Be to, ši priemonė yra būtina siekiant patobulinti nacionalinius ir Europos bendradarbiavimo mechanizmus bei įsteigti specialų koordinavimo komitetą, kuris palengvintų keitimąsi informacija, patirtimi ir bendros tvarkos, skirtos reaguoti į incidentus, kurie dėl savo pobūdžio paprastai vienu metu paveikia kelis operatorius ir infrastruktūros objektus, nustatymą.

Galiausiai būtina užtikrinti Ispanijos teisės sistemos suderinamumą su naujuoju Europos reguliavimo pagrindu, nustatytu TIS 2 direktyvoje ir Direktyvoje dėl ypatingos svarbos subjektų atsparumo. Šiomis Europos priemonėmis sugriežtinamos pareigos, susijusios su ypatingos svarbos infrastruktūros saugumu, rizikos valdymu ir atsparumu, ir reikalaujama, kad valstybės narės sukurtų veiksmingus incidentų prevencijos, nustatymo, reagavimo į juos ir veiklos atkūrimo po jų mechanizmus.

9c. Siūloma priemone nesukuriama pernelyg didelė ar neproporcinga našta, palyginti su siekiamais tikslais, nes ja nustatomi įpareigojimai atitinka poreikį užtikrinti infrastruktūrą, kurios yra būtinos visuomenės, ekonomikos ir viešųjų paslaugų veikimui, saugumą, atsparumą ir tęstinumą.

Priemonės proporcingumas akivaizdus visų pirma dėl to, kad daugelis nustatytų įpareigojimų jau yra telekomunikacijų operatorių ir skaitmeninės infrastruktūros valdytojų standartinės rizikos valdymo ir veiklos tęstinumo praktikos dalis. Rizikos analizės, nenumatytų atvejų planai, atkūrimo protokolai ir priežiūros mechanizmai yra standartiniai ypatingos svarbos infrastruktūrų ir esminių paslaugų valdymo elementai. Karaliaus dekretu nenustatomos visiškai naujos struktūros, o veikiau sisteminamos ir homogenizuojamos tam tikros prievolės, kad būtų užtikrinti minimalieji standartai, bendri visiems įpareigotiesiems subjektams.



EUROPEAN COMMISSION

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

Be to, numatytos priemonės yra proporcingos rizikos, kurią jos skirtos sumažinti, mastui. Atsižvelgiant į šias rizikas, reikalavimas turėti parengtus saugumo ir atsparumo planus, atsarginius mechanizmus bei išankstinio pranešimo tvarką yra pagrįsta ir būtina priemonė, skirta žalai sumažinti ir paslaugų atkūrimui pagreitinti.

Į reglamentą taip pat įtraukti mechanizmai, pagal kuriuos įpareigojimus galima pritaikyti prie kiekvieno reguliuojamojo subjekto aplinkybių. Konkretūs planai turėtų būti rengiami atsižvelgiant į kiekvieno tinklo, paslaugos ar infrastruktūros ypatybes, kad operatoriai galėtų nustatyti tinkamiausias technines ir organizacines priemones atsižvelgdami į savo konkrečią riziką. Šis lankstumas leidžia išvengti vienodų ar nelanksčių sprendimų, kurie galėtų sukelti nereikalingas išlaidas, ir skatina taikyti požiūrį, grindžiamą veiksmingu rizikos valdymu.

Kalbant apie pranešimų apie incidentus teikimą, šie įpareigojimai grindžiami poreikiu turėti naujausią ir patikimą informaciją, kad būtų galima koordinuoti reagavimą į incidentus, kurie gali paveikti daug naudotojų, operatorių ar teritorijų. Be to, reikalaujama informacija yra ta, kurią operatoriai jau dabar privalo rinkti ir tvarkyti viduje, siekdami išspręsti incidentus ir užtikrinti savo paslaugų tęstinumą; todėl ji nesukelia neproporcingos administracinės naštos, palyginti su nauda, kurią ji teikia koordinavimo ir reagavimo srityse.

Reglamentavimo poveikio vertinimo ataskaitoje taip pat daroma išvada, kad reglamento ekonominis poveikis yra valdomas ir proporcingas juo saugomam viešajam interesui. Nors numatoma, kad reguliuojamos įmonės patirs nuo 45 mln. iki 90 mln. EUR finansinių išlaidų, šios išlaidos visų pirma susijusios su investicijomis, kuriomis siekiama stiprinti infrastruktūros atsparumą ir užtikrinti esminių paslaugų tęstinumą. Be to, naujos administracinės naštos vertė apskaičiuota kaip sudaranti maždaug 19 276 EUR – tai nedidelė suma, palyginti su atitinkamų operatorių veiklos apimtimi ir ekonominiu dydžiu. Be to, dėl reglamentavimo valdžios institucijos nepatiria jokių biudžeto išlaidų ir jis neturi didelio poveikio konkurencijai.

Atsižvelgiant į visas šias priežastis, galima daryti išvadą, kad ši priemonė nesukelia pernelyg didelės naštos šalims, kurioms ji taikoma; ja nustatomi proporcingi, pagrįsti ir būtini įpareigojimai, siekiant užtikrinti aukštą elektroninių ryšių tinklų ir paslaugų saugumo bei atsparumo lygį.

10. Nuorodos į pagrindinius tekstus:

11. Ne

12.

13. Taip

Strateginiai šalies interesai

Elektroninių ryšių tinklai ir paslaugos yra esminė nacionalinio saugumo, viešųjų paslaugų, skubiosios pagalbos tarnybų, ekonominės veiklos ir teritorinės sanglaudos infrastruktūra.

14. Ne

15. Taip

16.

Techninių prekybos kliūčių aspektas: Ne

Sanitarinių ir fitosanitarinių
prionių aspektas: Ne

Europos Komisijos

Direktyvos (ES) 2015/1535 Kontaktinis taškas

el. pašto adresas: grow-dir2015-1535-central@ec.europa.eu