



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Paziņojuma numurs : 2026/0346/ES (Spain)

Karaļa dekrēta projekts par elektronisko sakaru tīklu un pakalpojumu, kā arī atsevišķu digitālās infrastruktūras objektu drošību un noturību.

Saņemšanas datums : 08/07/2026

Bezdarbības perioda beigas : 09/10/2026

Message

Ziņa 001

Komisijas ziņojums - TRIS/(2026) 1822

Direktīva (ES) 2015/1535

Notifikācija: 2026/0346/ES

Dalībvalsts paziņojums par projekta tekstu

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.LV

1. MSG 001 IND 2026 0346 ES LV 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 - Telesakari

5. Karaļa dekrēta projekts par elektronisko sakaru tīklu un pakalpojumu, kā arī atsevišķu digitālās infrastruktūras objektu drošību un noturību.

6. Dekrēta mērķis ir stiprināt elektronisko sakaru tīklu un pakalpojumu, ar tiem saistīto iekārtu un atsevišķu digitālās infrastruktūras objektu drošību, noturību un darbības nepārtrauktību Spānijā.

7.

8. Karaliskā dekrēta mērķis ir nodrošināt elektronisko sakaru tīklu un pakalpojumu, ar tiem saistīto iekārtu un atsevišķu digitālās infrastruktūras objektu drošību, noturību un darbības nepārtrauktību Spānijā.

Dekrēta uzdevums ir nodrošināt pamatpakalpojumu sniegšanu gadījumos, kad ir noticis drošības incidents vai pakalpojumu pārrāvums vai ir būtiski pasliktinājusies pakalpojumu kvalitāte, kā arī noteikt pienākumus ziņot iestādēm par šādiem incidentiem.

Atbildīgie subjekti ir publisku elektronisko sakaru tīklu operatori, publiski pieejamu pakalpojumu sniedzēji, saistīto iekārtu un digitālās infrastruktūras objektu, piemēram, zemūdens kabeļu, satelītsistēmu, datu apstrādes centru (DPC), satura piegādes tīklu (CDN) un interneta plūsmu apmaiņas punktu (IXP), operatori un dažos aspektos arī "112" neatliekamās palīdzības zvanu centru un sabiedrības brīdināšanas sistēmu operatori. Tiek atzīta arī minēto tīklu un infrastruktūras objektu būtiskā nozīme ārkārtas situācijās.

Ir izstrādāts "Valsts drošības un noturības plāns", kurā noteikts, kā jāorganizē reaģēšana krīzes situācijās un kādus koordinācijas mehānismus jāizmanto iestādēm. Tajā arī ir noteikts, ka atbildīgajiem subjektiem ir pienākums izstrādāt "vispārējo plānu" katrai no atbildīgajām personām un "konkrētus plānus" katram tīkla veidam un konkrētiem pakalpojumiem. Plānos jāiekļauj riska analīze, būtisku infrastruktūras objektu noteikšana, preventīvie pasākumi, darbības atjaunošanas mehānismi un rīcības protokoli dažādu veidu scenārijiem, piemēram, elektroenerģijas padeves pārtraukumiem, dabas katastrofām, ugunsgrēkiem, IT sistēmu darbības traucējumiem vai kiberuzbrukumiem.

Telesakaru pakalpojumu nepārtrauktības nodrošināšanai tiek ieviesti konkrēti pienākumi. Operatoriem jāveic pasākumi, lai līdz minimumam samazinātu incidentu radīto ietekmi un nodrošinātu pamatpakalpojumu darbību, it īpaši saziņu ārkārtas situācijās. Izņēmuma gadījumos tie var piešķirt prioritāti konkrētiem datplūsmu veidiem, piemēram, saziņai ārkārtas situācijās vai balss un SMS pakalpojumiem, vienlaikus vienmēr ievērojot tehnoloģiskās neitralitātes principu. Turklāt būtiskiem infrastruktūras objektiem ir noteiktas enerģētiskās autonomijas minimālās prasības, bet mobilajiem tīkliem – pienākums trīs gadu laikā pakāpeniski nodrošināt 75 % iedzīvotāju ar rezerves elektroapgādi vismaz četru stundu ilgumā.

Dekrēta projekts ietver sistēmu ziņošanai par būtiskiem incidentiem, ko neuzskata par kiberdrošības incidentiem, jo kiberdrošības incidentus reglamentē TID 2 direktīva un Kritisko vienību noturības (CER) direktīva. Par ikvienu būtisku incidentu operatoriem ir jāpaziņo Valsts sekretariātam vienas stundas laikā pēc incidenta konstatēšanas un turpmāk līdz traucējumu novēršanai ir regulāri jāsniedz jaunākā informācija, bet tūlīt pēc pakalpojuma atjaunošanas ir jāsapatavo galaziņojums.

Tiek ieviesti konkrēti pasākumi saziņas nodrošināšanai ārkārtas situācijās, izmantojot tālruna numuru "112" un sabiedrības brīdināšanas sistēmas. Ārkārtas palīdzības izsaukumu centriem un to operatoriem ir jāievieš rezerves sistēmas un pasākumi darbības nepārtrauktības nodrošināšanai, jāizstrādā konkrēti rīcības plāni ārkārtas situācijām un nekavējoties jāziņo par visiem pārrāvumiem minēto pakalpojumu sniegšanā, kurus automātiski klasificē kā būtiskus incidentus.

Karaļa dekrētā ir aprakstīti pasākumi un mehānismi saskaņošanai ar noteikumiem par kiberdrošību un kritisko vienību noturību (TID 2 direktīva un CER direktīva), Drošības un noturības koordinācijas komitejas izveide, kā arī nākotnē plānotā digitālo platformu ieviešana incidentu pārvaldībai un saziņai. Kopumā dekrēts būtiski pastiprina drošības, darbības nepārtrauktības un uzraudzības pienākumus, kuri attiecas uz telesakaru nozari un kritiskās digitālās infrastruktūras objektiem.



EUROPEAN COMMISSION

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

9. Ekonomikas un publisko pakalpojumu arvien plašākā digitalizācija ir ievērojami palielinājusi atkarību no elektronisko sakaru tīkliem un digitālās infrastruktūras objektiem, kuri atbalsta šādu tīklu darbību. Šādos apstākļos ir pilnīgi skaidrs, ka ir tādas ievainojamības un riski, kas apdraud ne tikai kiberdrošību, bet arī ietekmē infrastruktūras objektu fizisko drošību un spēju izturēt nevēlamus notikumus un atjaunot normālu darbību. Šajā sakarā regulējumā ir uzsvērts, ka jāstiprina spēja novērst incidentus, kas varētu apdraudēt elektronisko sakaru tīklu un pakalpojumu pieejamību, integritāti vai darbību, reaģēt uz šādiem incidentiem un pēc tam atjaunot normālu darbību.

Karaļa dekrētā pievienotajos paskaidrojumos ir norādīti vairāki neseni notikumi, kas apliecina nepieciešamību uzlabot attiecīgo infrastruktūras objektu noturību. Starp piemēriem ir minētas dabas parādības, piemēram, vulkāna izvirdums Palmas (La Palma) salā 2021. gadā un ciklona izraisītās vētras un lietusgāzes, kas 2024. gadā skāra vairākus Spānijas reģionus, kā arī incidenti, kuru izcelsme nav saistīta ar dabas spēkiem, piemēram, nesena elektroapgādes pārrāvums visā valstī. Minētie notikumi parādīja, ka gan ekstrēmas dabas parādības, gan tehniskas kļūmes vai elektroapgādes pārrāvumi var izraisīt būtiskus traucējumus sakaru tīklos un apdraudēt sabiedrībai un valsts iestādēm nepieciešamo pamatpakalpojumu nepārtrauktību.

Turklāt digitālā pārveide ievieš nozīmīgas pārmaiņas telesakaru tīklu arhitektūrā un darbībā. Ieviešot tādas tehnoloģijas kā lietu internets (IoT), mākslīgais intelekts (MI), lieli dati, mākoņdatošana un pakalpojumu virtualizācija, ir izdevies uzlabot efektivitāti, savienotību un ekonomisko izaugsmi, taču vienlaikus sistēmas ir kļuvušas sarežģītākas un radušies jauni darbības un drošības riski. Tāpēc ir būtiski pilnveidot tiesisko regulējumu, lai prognozētu tādus riskus un nodrošinātu pienācīga līmeņa aizsardzību un noturību.

No tiesiskā viedokļa konkrētās iniciatīvas pamatā ir galvenokārt Likuma Nr. 11/2022 (Vispārējais telekomunikāciju likums) 63. pants par elektronisko sakaru tīklu un pakalpojumu integritāti un drošību. Tā pamatojas arī uz spēkā esošajiem tiesību aktiem par 5G tīkla drošību, konkrētāk – uz karaļa Dekrētlukumu Nr. 7/2022, karaļa Dekrētlukumu Nr. 12/2018 par tīklu un informācijas sistēmu drošību un karaļa Dekrētu Nr. 443/2024, ar ko apstiprina valsts drošības satvaru 5G tīkliem un pakalpojumiem. Minētie noteikumi ir nodrošinājuši ievērojamu progresu, tomēr, neraugoties uz iepriekš minēto, ir jāizstrādā īpašs regulējums, kas vispusīgi risinātu visu elektronisko sakaru tīklu un pakalpojumu, kā arī atsevišķu digitālās infrastruktūras objektu drošības un noturības jautājumus.

Visbeidzot, tekstā ir paskaidrots, ka karaļa jaunā dekrēta mērķis ir atvieglot Spānijai turpmāku tiesību aktu pieņemšanu par kiberdrošību un kritisko vienību noturību. Līdz ar to pienākumi, kas izriet no regulējuma TID 2 un CER direktīvu transponēšanai, arī turpmāk pilnā mērā attieksies uz kiberdrošības incidentiem un incidentiem, kas skar digitālos tīklus, pakalpojumus un infrastruktūras objektus un kas nav skaidri reglamentēti šajā karaļa dekrētā. Tādējādi dekrēta mērķis ir nodrošināt saskaņotību starp dažādiem regulatīvajiem instrumentiem, novērst regulējuma pārklāšanos un izveidot visaptverošu aizsardzības sistēmu, kas stiprinātu Spānijas sabiedrībai un ekonomikai būtiskas telesakaru un digitālās infrastruktūras drošību, darbības nepārtrauktību un noturību.

9.a Šis pasākums ir piemērots izvīrītā mērķa sasniegšanai, proti, elektronisko sakaru tīklu un pakalpojumu, kā arī atsevišķu digitālās infrastruktūras objektu drošības, noturības un darbības nepārtrauktības stiprināšanai.

Pēdējos gados gūtā pieredze liecina, ka telesakaru tīkli ir sabiedrībai būtiska infrastruktūra, par ko pārliecinājāmies gan Covid-19 pandēmijas laikā, gan ārkārtas situācijās, ko izraisīja ekstrēmas dabas parādības, elektroapgādes pārrāvumi vai drošības incidenti, kas ietekmēja pakalpojumu pieejamību. Šādos apstākļos būtu lietderīgi pieņemt īpašu tiesisko regulējumu, kas stiprinātu spēju novērst incidentus, kuri var apdraudēt elektronisko sakaru nepārtrauktību, spēju reaģēt uz tādiem incidentiem un atjaunot normālu darbību.

Ar šo regulējumu tiek īstenoti Likuma Nr. 11/2022 (Vispārējais telekomunikāciju likums) 63. panta noteikumi. Tas arī papildina un pielāgo tiesisko regulējumu, kas attiecas uz tehnoloģiju attīstību un jaunajiem riskiem, kas saistīti ar digitalizāciju, tīkla virtualizāciju, mākoņdatošanu, mākslīgo intelektu un lietu internetu, kuru plašāka izmantošana paaugstina kā fiziskas, tā digitālas ievainojamības risku. Šajā sakarā karaļa dekrēts ir piemērots instruments, lai noteiktu nozares pienākumus un tādējādi nodrošinātu vispusīgu pieeju telesakaru nozares tehniskajai un operacionālajai specifikai.

Pasākuma piemērotību jo īpaši apliecina paredzētie preventīvie un plānošanas mehānismi, kam jāuzlabo operatoru sagatavotība krīzes situācijām. Pienākums izstrādāt “vispārējos plānus” un “konkrētos plānus” katram tīklam vai pakalpojumam paralēli “Valsts drošības un noturības plāna” un “Valsts rīcības plāna civilām ārkārtas situācijām” izstrādei ļauj noteikt konkrētas procedūras risku identificēšanai, novēršanai, reaģēšanai un normālas darbības atjaunošanai. Ziņošanai par incidentiem izstrādāto procedūru atjaunināšana arī ir piemērots pasākums kompetento iestāžu uzraudzības un krīzes pārvaldības spēju uzlabošanai. Pieredze rāda, ka kritēriji, termiņi un paziņojumu saturs ir jāpielāgo sarežģītākai



EUROPEAN COMMISSION

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

tehnoloģiskajai un operacionālajai realitātei.

Turklāt šis pasākums ir labi piemērots tādu īpaši sensitīvu pakalpojumu aizsardzības stiprināšanai kā, piemēram, saziņa ārkārtas situācijās, izmantojot tālruņa numuru "112" un sabiedrības brīdināšanas sistēmas, jo gan operatoriem, gan ārkārtas palīdzības izsaukumu centriem tiek noteikti konkrēti pienākumi attiecībā uz darbības nepārtrauktību, rezerves sistēmām un paziņošanu. Tas atvieglos minēto kritisko pakalpojumu pieejamības nodrošināšanu pat tad, ja sakaru infrastruktūras darbībā būs nopietni traucējumi.

Izveidot sadarbības mehānismus starp publiskā sektora struktūrām un valsts un Eiropas līmeņa iestādēm un nodibināt pastāvīgu koordinācijas komiteju, kurā piedalās arī dažādas ieinteresētās personas, ir piemērots veids, kā veicināt informācijas apmaiņu, koordināciju starp iestādēm un paraugprakses pārņemšanu drošības un noturības jomā.

Visbeidzot, šis pasākums saskan ar Eiropas tiesisko regulējumu, kas izriet no TID 2 un CER direktīvām, jo nodrošina pienācīgu saskaņotību ar turpmākajiem valsts tiesību aktiem attiecībā uz minēto direktīvu transponēšanu un novērš nepilnības ekonomikai un valsts drošībai stratēģiski svarīgas nozares regulējumā.

9.b Šis karaļa dekrēts tiks pieņemts, reaģējot uz reālu un pierādītu nepieciešamību stiprināt sabiedrībai, ekonomikai un publiskajiem pakalpojumiem būtiskas infrastruktūras spējas novērst incidentus, aizsargāt sevi pret tiem un atjaunot normālu darbību.

Ekonomisko un sociālo norišu arvien plašāka digitalizācija apvienojumā ar arvien lielāku atkarību no elektronisko sakaru tīkliem un pakalpojumiem, kā arī tādi notikumi kā vulkāna izvirdums Palmas salā, ciklona izraisītās vētras un lietusgāzes, kas izpostīja vairākus valsts reģionus, vai nesena elektroapgādes pārrāvums pierāda, ka elektronisko sakaru tīkli un pakalpojumi ir pakļauti visdažādākajiem riskiem, kuri var nopietni apdraudēt pamatpakalpojumu pieejamību iedzīvotājiem, uzņēmumiem un publiskā sektora struktūrām. Minētie incidenti spilgti apliecina nepieciešamību stiprināt digitālās infrastruktūras noturību un uzlabot spēju reaģēt uz ārkārtas situācijām un krīzēm.

Šis pasākums ir nepieciešams, lai faktiski īstenotu Likuma Nr. 11/2022 (Vispārējais telekomunikāciju likums) 63. pantu, kurš nosaka operatoriem pienākumu pienācīgi pārvaldīt drošības riskus un nodrošināt savu tīklu un pakalpojumu integritāti. Ir būtiski izstrādāt regulējumu, kurā būtu sīkāk aprakstīti operatoru un citu attiecīgo personu pienākumi attiecībā uz plānošanu, novēršanu, ziņošanu par incidentiem, koordināciju starp iestādēm un uzraudzību.

Šāds regulējums ir nepieciešams arī tāpēc, ka pašreizējais tiesiskais regulējums, kas attiecas uz ziņošanu par incidentiem, ir daļēji novecojis. Esošās procedūras vairs nenodrošina pienācīgu reaģēšanu uz sarežģītajiem incidentiem, ar kuriem mūsdienās var saskarties digitālie tīkli, pakalpojumi un infrastruktūra. Incidentu veidi, saziņas procedūras un ziņošanas termiņi ir jāatjaunina, lai kompetento iestāžu rīcībā būtu pietiekama un aktuāla informācija un tās spētu koordinēt ātru un efektīvu reaģēšanu uz krīzes situācijām.

Ir jāizveido arī konkrēti mehānismi, kas nodrošinās darbības nepārtrauktību tādiem īpaši svarīgiem pakalpojumiem kā, piemēram, saziņa ārkārtas situācijās, izmantojot tālruņa numuru "112" un sabiedrības brīdināšanas sistēmas. Pieredze liecina, ka ikvienam minēto pakalpojumu pārrāvumam var būt tiešas negatīvas sekas uz cilvēka dzīvību un fizisko neaizskaramību un uz neatliekamās palīdzības pārvaldību. Tāpēc regulējumā ir noteikti konkrēti pienākumi attiecībā uz plānošanu, rezerves sistēmām un darbības nepārtrauktību gan operatoriem, gan neatliekamās palīdzības izsaukumu centriem.

Šis pasākums ir arī nepieciešams, lai uzlabotu valsts un Eiropas līmeņa sadarbības mehānismus un izveidotu īpašu koordinācijas komiteju, kas veicinās informācijas un pieredzes apmaiņu un vienotu procedūru izstrādi reaģēšanai uz incidentiem, kuri kaut vai tikai savas būtības dēļ visbiežāk skar vairākus operatorus un infrastruktūras objektus vienlaikus.

Visbeidzot, ir jānodrošina Spānijas tiesību sistēmas saskaņotība ar jauno Eiropas tiesisko regulējumu, kas izriet no TID 2 un CER direktīvām. Attiecīgie Eiropas tiesību akti pastiprina pienākumus, kas attiecas uz kritiskās infrastruktūras drošību, riska pārvaldību un noturību, un nosaka, ka dalībvalstīm ir jāizstrādā iedarbīgi mehānismi incidentu novēršanai, atklāšanai, reaģēšanai uz tiem un normālas darbības atjaunošanai.

9.c Ņemot vērā izvirzītos mērķus, ierosinātais pasākums nerada pārmērīgu vai nesamērīgu slogu, jo pienākumi, kurus tas paredz ieviest, atbilst nepieciešamībai nodrošināt sabiedrībai, ekonomikai un publiskajiem pakalpojumiem būtiskas infrastruktūras drošību, noturību un darbības nepārtrauktību.

Pasākuma samērīgumu pirmām un galvenām kārtām apliecina fakts, ka daudzi no paredzētajiem pienākumiem jau ietilpst telesakaru operatoru un digitālās infrastruktūras pārvaldītāju riska pārvaldības un darbības nepārtrauktības standarta praksē. Riska analīze, ārkārtas rīcības plāni, darbības atjaunošanas protokoli un uzraudzības mehānismi ir



EUROPEAN COMMISSION

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

kritiskās infrastruktūras un pamatpakalpojumu pārvaldības standarta elementi. Karaļa dekrēts neparedz izveidot pilnīgi jaunas struktūras, bet gan sistematizē un vienādo atsevišķus pienākumus, lai visām atbildīgajām iestādēm būtu nodrošināti vienoti minimālie standarti.

Turklāt plānotie pasākumi ir samērīgi, ņemot vērā milzīgos riskus, kuru mazināšanai tie ir paredzēti. Ņemot vērā šādus riskus, prasība izstrādāt un ieviest drošības un noturības plānus, rezerves mehānismus un agrīnās brīdināšanas procedūras ir saprātīga un nepieciešama rīcība, kas mazinās kaitējumu un ļaus ātrāk atsākt pakalpojumu sniegšanu. Regulējums ietver arī mehānismus, kas ļauj pielāgot pienākumus katra regulētā subjekta individuālajiem apstākļiem. Konkrēto plānu izstrādē būtu jāņem vērā katra tīkla, pakalpojuma vai infrastruktūras objekta īpatnības, lai operatori varētu noteikt savu konkrēto risku mazināšanai vispiemērotākos tehniskos un organizatoriskos pasākumus. Šāds elastīgums ļauj izvairīties no tādu vienotu vai striktu risinājumu ieviešanas, kas varētu radīt nevajadzīgas izmaksas, un atbalsta uz efektīvu riska pārvaldību balstītu pieeju.

Pienākumi, kas ir saistīti ar ziņošanu par incidentiem, ir pamatoti ar nepieciešamību pēc atjauninātas un uzticamas informācijas gadījumos, kad ir jākoordinē reaģēšana uz incidentiem, kuri var skart lielu skaitu lietotāju, operatoru vai teritoriju. Turklāt tiek prasīta informācija, kuru operatoriem jau tagad ir jāvāc un jāapstrādā iekšēji, lai novērstu incidentus un nodrošinātu pakalpojumu nepārtrauktību; tādējādi tā nerada nesamērīgu administratīvo slogu, ja ņem vērā šādas informācijas sniegtos ieguvumus koordinācijas un reaģēšanas spēju ziņā.

Regulējuma ietekmes novērtējuma ziņojumā arī secināts, ka regulējuma noteikumu radītā ekonomiskā ietekme ir pieļaujama un samērīga salīdzinājumā ar tām sabiedrības interesēm, kuru aizsardzība ir regulējuma mērķis. Lai gan aplēses rāda, ka regulētajiem subjektiem var rasties finansiālas izmaksas 45–90 miljonu EUR apmērā, šīs izmaksas galvenokārt ir saistītas ar investīcijām infrastruktūras noturības stiprināšanā un pamatpakalpojumu nepārtrauktības nodrošināšanā. Turklāt jaunais administratīvais slogs naudas izteiksmē ir aplēsts aptuveni 19 276 EUR apmērā, kas ir neliela summa, ja ņem vērā attiecīgo operatoru darbības apjomu un ekonomisko nozīmību. Šis regulējums arī neradīs nekādus budžeta izdevumus valsts iestādēm, un tam nav būtiskas ietekmes uz konkurenci.

Visu iepriekš minēto iemeslu dēļ var secināt, ka pasākums nerada pārmērīgu slogu personām, uz kurām tas attiecas, bet gan nosaka pienākumus, kas ir samērīgi, pamatoti un nepieciešami elektronisko sakaru tīklu un pakalpojumu drošības un noturības nodrošināšanai augstā līmenī.

10. Atsauces uz pamatdokumentiem:

11. Nē

12.

13. Jā

Valsts stratēģiskās intereses

Elektronisko sakaru tīkli un pakalpojumi ir valsts drošībai, publiskajiem pakalpojumiem, neatliekamās palīdzības dienestiem, saimnieciskajai darbībai un teritoriālajai kohēzijai būtiska infrastruktūra.

14. Nē

15. Jā

16.

TBT aspekts: Nē

SPS aspekts: Nē

Eiropas Komisijas

Direktīvas (ES) 2015/1535 kontaktpunkts

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