



EUROPEAN COMMISSION

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

Číslo oznámení : 2026/0346/ES (Spain)

Návrh královského výnosu o bezpečnosti a odolnosti sítí a služeb elektronických komunikací a určitých digitálních infrastruktur.

Datum přijetí : 08/07/2026

Ukončení odkladné lhůty : 09/10/2026

Message

Zpráva 001

Zpráva od Komise - TRIS/(2026) 1822

Směrnice (EU) 2015/1535

Oznámení: 2026/0346/ES

Oznámení návrhu znění od členského státu

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 - 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 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: 20261822.CS

1. MSG 001 IND 2026 0346 ES CS 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 - Telekomunikace

5. Návrh královského výnosu o bezpečnosti a odolnosti sítí a služeb elektronických komunikací a určitých digitálních infrastruktur.

6. Jeho cílem je posílit bezpečnost, odolnost a kontinuitu sítí a služeb elektronických komunikací, jejich souvisejících zdrojů a určitých digitálních infrastruktur ve Španělsku.

7.

8. Královský výnos usiluje o zajištění bezpečnosti, odolnosti a kontinuity sítí a služeb elektronických komunikací, jejich souvisejících zdrojů a určitých digitálních infrastruktur ve Španělsku.

Cílem je zajistit poskytování základních služeb v případě bezpečnostních incidentů, přerušení služeb nebo významného zhoršení jejich kvality, jakož i upravit povinnosti oznamování těchto incidentů správním orgánům.

Povinnými subjekty jsou provozovatelé veřejných sítí elektronických komunikací, poskytovatelé služeb dostupných veřejnosti, správci souvisejících zdrojů a digitální infrastruktury, jako jsou podmořské kabely, satelitní systémy, datová centra (CPD), síť pro distribuci obsahu (CDN) a internetové výměnné body (IXP), jakož i v určitých ohledech tísňová centra 112 a systémy veřejného varování. Dále se uznává zásadní charakter těchto sítí a infrastruktur v nouzových situacích.

Stanoví se vypracování „Národního plánu bezpečnosti a odolnosti“, který definuje organizaci reakce na krizi a mechanismy institucionální koordinace. Rovněž stanoví povinnost subjektů podléhajících této povinnosti vypracovat „obecný plán“ pro každý subjekt a „specifické plány“ podle typu sítě a konkrétních služeb. Tyto plány musí zahrnovat analýzu rizik, identifikaci klíčové infrastruktury, preventivní opatření, mechanismy obnovy a postupy pro různé scénáře, jako jsou výpadky elektrického proudu, přírodní jevy, požáry, selhání informačních systémů nebo kybernetické útoky. Zavádějí se konkrétní povinnosti k zajištění kontinuity telekomunikačních služeb. Provozovatelé budou muset přijmout opatření k minimalizaci dopadu incidentů a k zajištění fungování klíčových služeb, zejména nouzové komunikace. Ve výjimečných situacích budou moci upřednostnit určité typy datového provozu, jako jsou nouzová komunikace nebo hlasové služby a SMS, vždy při dodržení zásady technologické neutrality. Dále se stanovují minimální požadavky na energetickou soběstačnost pro klíčovou infrastrukturu a mobilním sítím se ukládá povinnost postupně zajistit minimální autonomii 4 hodin pro 75 % obyvatelstva ve lhůtě 3 let.

Zahrnuje systém oznamování významných incidentů, které nejsou považovány za incidenty v oblasti kybernetické bezpečnosti; ty jsou upraveny ve směrnici NIS2 a směrnici CER. Provozovatelé oznámí státnímu sekretariátu jakýkoli významný incident nejpozději do jedné hodiny od okamžiku, kdy se o něm dozvědí, a následně budou zasílat pravidelné aktualizace po dobu trvání narušení a závěrečnou zprávu po obnovení služby.

Stanovují se konkrétní opatření pro nouzovou komunikaci prostřednictvím čísla 112 a systémů veřejného varování. Jak centra pro přijímání tísňových volání, tak provozovatelé musí zavést opatření pro zajištění redundance a kontinuity, vypracovat konkrétní akční plány a neprodleně oznamovat jakékoli přerušení těchto služeb, které se automaticky považují za významné incidenty.

Královský výnos doplňuje opatření a mechanismy koordinace s předpisy o kybernetické bezpečnosti a odolnosti kritických subjektů (směrnice NIS2 a směrnice CER), zřízení Koordinační rady pro bezpečnost a odolnost a budoucí zavedení telematických platform pro řízení a hlášení incidentů. Celkově se jedná o významné posílení povinností v oblasti bezpečnosti, kontinuity a dohledu platných pro telekomunikační sektor a kritickou digitální infrastrukturu.

9. Rostoucí digitalizace ekonomiky a veřejných služeb výrazně zvýšila závislost na sítích elektronických komunikací a digitální infrastruktuře, která je podporuje. Tato situace poukázala na existenci zranitelností a rizik, která se neomezuje výlučně na oblast kybernetické bezpečnosti, ale dotýkají se také fyzické bezpečnosti a schopnosti infrastruktur odolávat nepříznivým událostem a zotavovat se z nich. V této souvislosti považuje předpis za nezbytné posílit schopnost prevence, reakce a zotavení v případě incidentů, které by mohly ohrozit dostupnost, integritu nebo fungování sítí a služeb elektronických komunikací.



EUROPEAN COMMISSION

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

Odůvodnění královského výnosu poukazuje na různé nedávné události, které prokázaly nutnost zvýšit odolnost těchto infrastruktur. Mezi nimi zmiňuje přírodní jevy, jako je sopečná erupce na ostrově La Palma v roce 2021 a studená tlaková níže, která v roce 2024 zasáhla různé části Španělska, jakož i jako incidenty nenaturálního původu, jako byl nedávný výpadek elektrické energie, který postihl celé území státu. Tyto události ukázaly, že jak extrémní přírodní jevy, tak technické či energetické poruchy mohou způsobit významné narušení komunikačních sítí a ohrozit kontinuitu služeb nezbytných pro občany i veřejnou správu.

Na druhou stranu digitální transformace zásadně mění architekturu a fungování telekomunikačních sítí. Zavádění technologií, jako je internet věcí (IoT), umělá inteligence (AI), Big Data, cloud computing a virtualizace služeb, umožnilo zlepšit efektivitu, konektivitu a hospodářský rozvoj, zároveň však zvýšilo složitost systémů a vyvolalo nová provozní a bezpečnostní rizika. Proto považuje za nezbytné, aby se regulační rámec vyvíjel tak, aby těmto rizikům předcházel a zajistil přiměřenou úroveň ochrany a odolnosti.

Z právního hlediska se návrh opírá především o článek 63 obecného zákona č. 11/2022 o telekomunikacích, který se týká integrity a bezpečnosti sítí a služeb elektronických komunikací. Dále vychází ze stávající právní úpravy v oblasti bezpečnosti sítí 5G, zejména z královského nařízení s mocí zákona č. 7/2022, královského nařízení s mocí zákona č. 12/2018 o bezpečnosti sítí a informačních systémů a královského výnosu č. 443/2024, kterým se schvaluje Národní bezpečnostní rámec pro sítě a služby 5G. Aniž je dotčeno výše uvedené, přestože tyto právní předpisy představují významný pokrok, je nezbytné vytvořit zvláštní rámec, který bude komplexně řešit bezpečnost a odolnost všech sítí a služeb elektronických komunikací a určitých digitálních infrastruktur.

Text dále vysvětluje, že cílem nového královského výnosu je doplnit připravovanou španělskou právní úpravu v oblasti kybernetické bezpečnosti a odolnosti kritických subjektů. Povinnosti vyplývající z právních předpisů provádějících směrnice NIS2 a CER proto zůstávají plně použitelné pro incidenty v oblasti kybernetické bezpečnosti i pro incidenty, které ovlivňují sítě, služby a digitální infrastruktury a nejsou výslovně upraveny tímto královským výnosem. Cílem je zajistit soudržnost jednotlivých právních nástrojů, zabránit překrývání regulačních požadavků a vytvořit komplexní systém ochrany, který posílí bezpečnost, kontinuitu a odolnost telekomunikací a digitálních infrastruktur nezbytných pro fungování španělské společnosti a hospodářství.

9a. Toto opatření je vhodné k dosažení sledovaného cíle, kterým je posílení bezpečnosti, odolnosti a kontinuity sítí a služeb elektronických komunikací a některých digitálních infrastruktur.

Zkušenosti získané v posledních letech ukázaly, že telekomunikační sítě představují infrastrukturu zásadního významu pro fungování společnosti, což se jasně projevilo během pandemie COVID-19 i při mimořádných událostech způsobených extrémními přírodními jevy, výpadky dodávek elektrické energie nebo bezpečnostními incidenty, které ovlivnily dostupnost služeb. V této souvislosti představuje přijetí zvláštního regulačního rámce vhodný prostředek k posílení schopnosti předcházet incidentům, reagovat na ně a obnovovat provoz po incidentech, které mohou narušit kontinuitu elektronických komunikací.

Tento právní předpis provádí ustanovení článku 63 obecného zákona č. 11/2022 o telekomunikacích. Současně doplňuje a přizpůsobuje regulační rámec technologickému vývoji a novým rizikům spojeným s digitalizací, virtualizací sítí, cloud computingem, umělou inteligencí a internetem věcí (IoT), jejichž stále širší využívání zvyšuje vystavení fyzickým i digitálním zranitelnostem. Královský výnos tak představuje vhodný nástroj pro stanovení zvláštních odvětvových povinností, které umožní komplexně řešit technické a provozní zvláštnosti telekomunikačního odvětví.

Vhodnost opatření se odráží zejména v zavedení preventivních mechanismů a plánovacích postupů zaměřených na zlepšení připravenosti provozovatelů na krizové situace. Povinnost vypracovat „obecné plány“ a „zvláštní plány“ pro jednotlivé sítě nebo služby spolu s vypracováním „Národního plánu bezpečnosti a odolnosti“ a „Národního civilního krizového plánu“ umožňuje zavést konkrétní postupy pro identifikaci rizik, prevenci, reakci na incidenty a obnovu. Rovněž aktualizace postupů oznamování incidentů představuje vhodné opatření ke zlepšení schopnosti příslušných orgánů vykonávat dohled a řídit krizové situace. Dosavadní zkušenosti ukázaly potřebu přizpůsobit kritéria, lhůty a obsah oznámení stále složitější technologické a provozní realitě.

Opatření je rovněž vhodné k posílení ochrany zvláště citlivých služeb, jako jsou tísňová volání prostřednictvím čísla 112 a systémy veřejného varování, neboť provozovatelům i střediskům pro příjem tísňových volání ukládá zvláštní povinnosti týkající se kontinuity provozu, redundance a oznamování. Přispívá tak k zajištění nepřetržitého poskytování těchto kritických služeb i v případě závažného narušení komunikační infrastruktury.

Vytvoření mechanismů spolupráce mezi orgány veřejné správy, vnitrostátními a evropskými orgány, jakož i zřízení stálé koordinační platformy za účasti různých zúčastněných stran představuje vhodný nástroj na podporu výměny informací,



EUROPEAN COMMISSION

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

institucionální koordinace a zavádění osvědčených postupů v oblasti bezpečnosti a odolnosti.

Navrhované opatření je konečně v souladu s evropským regulačním rámcem vyplývajícím ze směrnic NIS2 a CER, neboť zajišťuje odpovídající koordinaci s budoucími vnitrostátními prováděcími předpisy a předchází vzniku regulačních mezer v odvětví strategického významu pro hospodářství a národní bezpečnost.

9b. Přijetí královského výnosu reaguje na skutečnou a doloženou potřebu posílit schopnost předcházet rizikům, chránit a obnovovat infrastruktury, které se staly nezbytnými pro fungování společnosti, hospodářství a veřejných služeb.

Rostoucí digitalizace hospodářských a společenských činností spolu se stále větší závislostí na sítích a službách elektronických komunikací, stejně jako události, jako byla sopečná erupce na ostrově La Palma, studená tlaková níže, která zasáhly různé části území státu, nebo nedávný rozsáhlý výpadek dodávek elektrické energie, prokázaly, že sítě a služby elektronických komunikací jsou vystaveny velmi různorodým rizikům, která mohou vážně narušit poskytování služeb nezbytných pro občany, podniky i orgány veřejné správy. Tyto události poukázaly na potřebu posílit odolnost digitálních infrastruktur a zlepšit schopnost reagovat na mimořádné události a krizové situace.

Toto opatření je nezbytné k provedení a upřesnění článku 63 obecného zákona č. 11/2022 o telekomunikacích, který provozovatelům ukládá povinnost řádně řídit bezpečnostní rizika a zajišťovat integritu jejich sítí a služeb. Je nezbytné přijmout prováděcí právní úpravu, která přesněji vymezí povinnosti provozovatelů a dalších dotčených subjektů v oblasti plánování, prevence, oznamování incidentů, institucionální koordinace a dohledu.

Potřeba přijetí tohoto právního předpisu je dále odůvodněna částečnou zastaralostí stávajícího regulačního rámce pro hlášení incidentů. Dosavadní postupy již odpovídajícím způsobem nereagují na složitost incidentů, které mohou v současnosti ovlivnit sítě, služby a digitální infrastruktury. Aktualizace kategorií incidentů, postupů jejich oznamování a příslušných lhůt je nezbytná k tomu, aby příslušné orgány měly k dispozici dostatečné a aktuální informace umožňující koordinovat rychlou a účinnou reakci na krizové situace.

Rovněž je nezbytné zavést zvláštní mechanismy k zajištění kontinuity zvláště kritických služeb, jako jsou tísňová volání prostřednictvím čísla 112 a systémy veřejného varování. Zkušenosti ukazují, že jakékoli přerušení těchto služeb může mít přímé důsledky pro ochranu života, fyzické integrity osob a řízení mimořádných událostí. Z tohoto důvodu právní předpis ukládá provozovatelům i střediskům pro příjem tísňových volání zvláštní povinnosti v oblasti plánování, redundance a zajištění kontinuity provozu.

Opatření je dále nezbytné ke zlepšení mechanismů spolupráce na vnitrostátní i evropské úrovni prostřednictvím zřízení zvláštní koordinační platformy, která usnadní výměnu informací, sdílení zkušeností a stanovení společných postupů pro řešení incidentů, jež svou povahou zpravidla současně ovlivňují více provozovatelů a infrastruktur.

V neposlední řadě je opatření nezbytné k zajištění souladu španělského právního řádu s novým evropským regulačním rámcem vyplývajícím ze směrnic NIS2 a CER. Tyto evropské předpisy posilují povinnosti v oblasti bezpečnosti, řízení rizik a odolnosti kritických infrastruktur a vyžadují, aby členské státy vytvořily účinné mechanismy prevence, odhalování, reakce na incidenty a obnovy po incidentech.

9c. Navrhované opatření nepředstavuje nadměrnou ani nepřiměřenou zátěž vzhledem ke sledovaným cílům, neboť povinnosti, které zavádí, vycházejí z potřeby zajistit bezpečnost, odolnost a kontinuitu infrastruktur, které mají zásadní význam pro fungování společnosti, hospodářství a veřejných služeb.

Přiměřenost opatření se projevuje především tím, že řada stanovených povinností již tvoří součást běžné praxe provozovatelů telekomunikačních sítí a správců digitálních infrastruktur v oblasti řízení rizik a zajišťování kontinuity činností. Vypracovávání analýz rizik, plánů pro nepředvídané události, plánů obnovy nebo mechanismů dohledu představuje běžnou součást správy kritických infrastruktur a poskytování základních služeb. Královský výnos neukládá vytváření zcela nových organizačních struktur, ale systematizuje a harmonizuje určité povinnosti s cílem zajistit společné minimální standardy pro všechny povinné subjekty.

Navrhovaná opatření jsou rovněž přiměřená rozsahu rizik, která mají zmírnit. Vzhledem k těmto rizikům představuje požadavek na zavedení plánů bezpečnosti a odolnosti, záložních mechanismů a postupů včasného oznamování přiměřenou a nezbytnou reakci, která umožní minimalizovat škody a urychlit obnovu poskytování služeb.

Právní předpis rovněž obsahuje mechanismy umožňující přizpůsobit jednotlivé povinnosti konkrétní situaci každého povinného subjektu. Zvláštní plány musí být vypracovány s ohledem na charakteristiky jednotlivých sítí, služeb nebo infrastruktur, což provozovatelům umožňuje stanovit technická a organizační opatření nejvhodnější s ohledem na jejich konkrétní rizika. Tato flexibilita zabráňuje ukládání jednotných nebo příliš rigidních řešení, která by mohla vést ke zbytečným nákladům, a podporuje přístup založený na účinném řízení rizik.



EUROPEAN COMMISSION

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

Pokud jde o hlášení incidentů, jsou tyto povinnosti odůvodněny potřebou disponovat aktuálními a spolehlivými informacemi, které umožní koordinovat reakci na incidenty, jež mohou postihnout velký počet uživatelů, provozovatelů nebo území. Požadované informace navíc odpovídají údajům, které provozovatelé již shromažďují a spravují pro vlastní potřeby při řešení incidentů a zajišťování kontinuity svých služeb, takže nepředstavují nepřiměřenou administrativní zátěž vzhledem k přínosům v oblasti koordinace a schopnosti reagovat.

Zpráva o posouzení dopadů regulace dále dospívá k závěru, že hospodářské dopady vyplývající z navrhovaného právního předpisu jsou přijatelné a přiměřené chráněnému veřejnému zájmu. Přestože se náklady pro povinné subjekty odhadují na 45 až 90 milionů EUR, souvisejí především s investicemi zaměřenými na posílení odolnosti infrastruktur a zajištění kontinuity základních služeb. Nová administrativní zátěž se navíc odhaduje přibližně na 19 276 EUR, což představuje nízkou částku ve srovnání s rozsahem činností a ekonomickou velikostí dotčených provozovatelů. Právní předpis zároveň nevyvolává žádné rozpočtové náklady pro orgány veřejné správy ani významné dopady na hospodářskou soutěž. Lze proto uzavřít, že navrhované opatření neukládá povinným subjektům nadměrnou zátěž, ale stanoví přiměřené, odůvodněné a nezbytné povinnosti k zajištění vysoké úrovně bezpečnosti a odolnosti sítí a služeb elektronických komunikací.

10. Odkazy na základní texty:

11. Ne

12.

13. Ano

Strategické zájmy země

Sítě a služby elektronických komunikací představují infrastrukturu zásadního významu pro národní bezpečnost, veřejné a záchranné služby, hospodářskou činnost a územní soudržnost.

14. Ne

15. Ano

16.

Hledisko TBT: Ne

Hledisko SPS: Ne

Evropská komise

Kontaktní bod směrnice (EU) 2015/1535

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