



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Številka obvestila : 2026/0346/ES (Spain)

Osnutek kraljeve uredbe o varnosti in odpornosti elektronskih komunikacijskih omrežij in storitev ter nekaterih digitalnih infrastruktur.

Datum prejema : 08/07/2026

Konec mirovanja : 09/10/2026

Message

Sporočilo 001

Sporočilo Komisije - TRIS/(2026) 1822

Direktiva (EU) 2015/1535

Obvestilo: 2026/0346/ES

Uradno obvestilo o osnutku besedila države članice

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.SL

1. MSG 001 IND 2026 0346 ES SL 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 - Telekomunikacije

5. Osnutek kraljeve uredbe o varnosti in odpornosti elektronskih komunikacijskih omrežij in storitev ter nekaterih digitalnih infrastruktur.

6. Njen cilj je okrepiti varnost, odpornost in neprekinjeno delovanje omrežij in storitev elektronskih komunikacij, z njimi povezanih objektov ter nekaterih digitalnih infrastruktur v Španiji.

7.

8. Cilj kraljeve uredbe je zagotoviti varnost, odpornost in neprekinjeno delovanje omrežij in storitev elektronskih komunikacij, z njimi povezanih objektov ter nekaterih digitalnih infrastruktur v Španiji.

Cilj je zagotoviti izvajanje ključnih storitev v primeru varnostnih incidentov, prekinitev storitev ali znatnega poslabšanja kakovosti storitev ter urediti obveznosti glede poročanja o takšnih incidentih pristojnim organom.

Pooblaščen subjekti so operaterji javnih elektronskih komunikacijskih omrežij, ponudniki javno dostopnih storitev, operaterji povezanih objektov in digitalne infrastrukture, kot so podmorski kabli, satelitski sistemi, centri za obdelavo podatkov (data processing centres – DPC), omrežja za dostavo vsebin (content delivery networks – CDN) in stičišča omrežij (internet exchange points – IXP), v nekaterih pogledih pa tudi centri za klice v nujnih primerih prek številke 112 in sistemi javnega opozarjanja. Priznana je tudi ključna vloga teh omrežij in infrastruktur v izrednih razmerah.

Pripravljen je bil „nacionalni načrt za varnost in odpornost“, ki bo opredelil organizacijo odziva na krizne razmere ter mehanizme institucionalnega usklajevanja. Določa tudi obveznost pooblaščenih subjektov, da pripravijo „splošni načrt“ za vsako pooblaščen stranko in „posebne načrte“ za vsako vrsto omrežij in posebnih storitev. Vključevati morajo analize tveganj, opredelitev ključne infrastrukture, preventivne ukrepe, mehanizme za obnovo ter protokole ukrepanja za različne scenarije, kot so izpadi električne energije, naravne nesreče, požari, okvare informacijskih sistemov ali kibernetiski napadi.

Uvedene so posebne obveznosti za zagotovitev neprekinjenega delovanja telekomunikacijskih storitev. Operaterji morajo sprejeti ukrepe za zmanjšanje vpliva incidentov na najnižjo možno raven ter zagotoviti delovanje ključnih storitev, zlasti komunikacij v nujnih primerih. V izjemnih okoliščinah lahko dajo prednost določenim vrstam prometa, kot so komunikacije v nujnih primerih ali glasovne storitve in storitve SMS, pri čemer morajo vedno upoštevati načelo tehnološke nevtralnosti. Poleg tega so za osnovno infrastrukturo določene minimalne zahteve glede energetske avtonomije, mobilnim omrežjem pa je naložena obveznost, da v treh letih postopno zagotovijo vsaj štiriurno varnostno napajanje za delež 75 % prebivalstva.

Vključuje sistem za poročanje o pomembnih incidentih, ki se ne štejejo za kibernetiske incidente, pri čemer slednje urejata direktiva NIS2 in direktiva o odpornosti kritičnih subjektov. Operaterji morajo državni sekretariat obvestiti o vsakem pomembnem incidentu v roku ene ure od trenutka, ko se z njim seznanijo, ter nato med trajanjem motnje redno posredovati najnovejše informacije, po ponovni vzpostavitvi storitve pa morajo predložiti končno poročilo.

Določeni so posebni ukrepi za komunikacijo v nujnih primerih prek številke 112 in sistemov javnega opozarjanja. Tako centri za klice v nujnih primerih kot tudi operaterji morajo vzpostaviti ukrepe za zagotavljanje rezervnih zmogljivosti in neprekinjenega poslovanja, pripraviti konkretne načrte za izredne razmere ter nemudoma poročati o vseh motnjah v delovanju teh storitev, ki se avtomatično uvrščajo med pomembne incidente.

V kraljevi uredbi so določeni ukrepi in mehanizmi za usklajevanje s predpisi o kibernetiski varnosti in odpornosti kritičnih subjektov (direktiva NIS2 in direktiva o odpornosti kritičnih subjektov), ustanovitev usklajevalnega odbora za varnost in odpornost ter prihodnjo uvedbo digitalnih platform za obvladovanje incidentov in komunikacijo. Na splošno gre za znatno okrepitev obveznosti na področju varnosti, neprekinjenega delovanja in nadzora, ki veljajo za telekomunikacijski sektor in kritične digitalne infrastrukture.

9. Zaradi vse večje digitalizacije gospodarstva in javnih storitev se je znatno povečala odvisnost od elektronskih



EUROPEAN COMMISSION

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

komunikacijskih omrežij in digitalnih infrastruktur, ki jih podpirajo. To stanje je pokazalo, da obstajajo ranljivosti in tveganja, ki niso omejeni izključno na področje kibernetske varnosti, temveč vplivajo tudi na fizično varnost in zmožnost infrastruktur, da vzdržijo varnostne zaplete in si opomorejo po njih. V zvezi s tem je v uredbi navedeno, da je treba okrepiti zmogljivosti za preprečevanje incidentov, ki bi lahko ogrozili razpoložljivost, celovitost ali delovanje elektronskih komunikacijskih omrežij in storitev, odzivanje nanje in okrevanje po njih.

V pojasnjevalnih opombah kraljeve uredbe je izpostavljenih več nedavnih dogodkov, ki so pokazali, da je treba povečati odpornost teh infrastruktur. Med njimi navaja naravne pojave, kot sta izbruh vulkana na La Palmi leta 2021 in hladen sistem nizkega zračnega tlaka, ki je leta 2024 prizadel različne dele Španije, pa tudi dogodke nenaravnega izvora, kot je nedavni izpad električne energije po vsej državi. Ti dogodki so pokazali, da lahko tako izredni naravni pojavi kot tudi tehnične napake ali izpadi električne energije povzročijo znatne motnje v komunikacijskih omrežjih ter ogrozijo neprekinjeno delovanje ključnih storitev za javnost in javne organe.

Poleg tega digitalna preobrazba korenito spreminja arhitekturo in delovanje telekomunikacijskih omrežij. Vključitev tehnologij, kot so internet stvari, umetna inteligenca, velepodatki, računalništvo v oblaku in virtualizacija storitev, je omogočila izboljšanje učinkovitosti, povezanosti in gospodarskega razvoja, hkrati pa je povečala kompleksnost sistemov ter ustvarila nova operativna in varnostna tveganja. Zato vlada prepričanje, da je nujno, da se regulativni okvir razvija tako, da bo omogočal predvidevanje teh tveganj ter zagotavljal ustrezno raven zaščite in odpornosti.

S pravnega vidika pobuda temelji predvsem na členu 63 zakona št. 11/2022, splošnega zakona o telekomunikacijah, o celovitosti in varnosti elektronskih komunikacijskih omrežij in storitev. Poleg tega temelji na obstoječi zakonodaji o varnosti omrežij 5G, zlasti kraljevi uredbi z zakonsko močjo št. 7/2022, kraljevi uredbi z zakonsko močjo št. 12/2018 o varnosti omrežij in informacijskih sistemov ter kraljevi uredbi št. 443/2024 o odobritvi nacionalnega varnostnega okvira za omrežja in storitve 5G. Čeprav so ti predpisi privedli do znatnega napredka, je treba ne glede na navedeno razviti poseben okvir, ki bo celovito obravnaval varnost in odpornost vseh elektronskih komunikacijskih omrežij in storitev ter nekaterih digitalnih infrastruktur.

Nazadnje je v besedilu pojasnjeno, da naj bi nova kraljeva uredba dopolnjevala prihodnjo špansko zakonodajo o kibernetski varnosti in odpornosti kritičnih subjektov. Zato se bodo obveznosti, ki izhajajo iz predpisov, s katerimi se prenašata direktiva NIS2 in uredba o odpornosti kritičnih subjektov, še naprej v celoti uporabljale za kibernetske incidente in tiste incidente, ki vplivajo na digitalna omrežja, storitve in infrastrukturo ter niso izrecno urejeni v tej kraljevi uredbi.

Cilj je torej zagotoviti skladnost med različnimi regulativnimi instrumenti, preprečiti regulativna prekrivanja in vzpostaviti celovit sistem zaščite, ki krepi varnost, kontinuiteto in odpornost telekomunikacijske in digitalne infrastrukture, bistvene za delovanje španske družbe in španskega gospodarstva.

9a. Ukrep je primeren za doseganje zastavljenega cilja, in sicer okrepitve varnosti, odpornosti in neprekinjenega delovanja omrežij in storitev elektronskih komunikacij ter nekaterih digitalnih infrastruktur.

Izkušnje, pridobljene v zadnjih letih, so pokazale, da so telekomunikacijska omrežja bistvena infrastruktura za delovanje družbe, kot se je pokazalo med pandemijo COVID-19, pa tudi v izrednih razmerah, ki so posledica ekstremnih naravnih dogodkov, izpadov električne energije ali varnostnih incidentov, ki so vplivali na razpoložljivost storitev. V tem scenariju je sprejetje posebnega regulativnega okvira primerno za krepitev zmogljivosti za preprečevanje incidentov, ki bi lahko ogrozili neprekinjeno delovanje elektronskih komunikacij, ter odzivanje nanje in okrevanje po njih.

Z uredbo se izvajajo določbe iz člena 63 zakona št. 11/2022, tj. splošnega zakona o telekomunikacijah. Poleg tega dopolnjuje in prilagaja regulativni okvir tehnološkemu razvoju ter novim tveganjem, povezanim z digitalizacijo, virtualizacijo omrežij, računalništvom v oblaku, umetno inteligenco in internetom stvari (IoT), katerih vse večja uporaba povečuje izpostavljenost ranljivostim tako fizične kot digitalne narave. V tej zvezi je kraljeva uredba ustrezen instrument za opredelitev sektorskih obveznosti, ki omogočajo celovit pristop k tehničnim in operativnim posebnostim telekomunikacijskega sektorja.

Ustreznost ukrepa se odraža zlasti v vključitvi mehanizmov za preprečevanje in načrtovanje, namenjenih izboljšanju pripravljenosti operaterjev v kriznih razmerah. Obveznost priprave „splošnih načrtov“ in „posebnih načrtov“ za posamezno omrežje ali storitev, skupaj s pripravo „nacionalnega načrta za varnost in odpornost“ ter „nacionalnega načrta za civilne izredne razmere“, omogoča vzpostavitev posebnih postopkov za preprečevanje in odkrivanje tveganj ter odzivanje nanje in okrevanje po njih.

Prav tako je posodobitev postopkov za poročanje o incidentih ustrezen ukrep za izboljšanje zmogljivosti pristojnih organov za spremljanje in obvladovanje kriz. Izkušnje so pokazale, da je treba merila, roke in vsebino obvestil prilagoditi kompleksnejšim tehnološkim in operativnim razmeram.



EUROPEAN COMMISSION

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

Poleg tega je ta ukrep zelo primeren za okrepitev zaščite posebej občutljivih storitev, kot so centri za klice v nujnih primerih prek številke 112 in sistemi javnega opozarjanja, saj operaterjem in centrom za klice v nujnih primerih nalaga posebne obveznosti glede neprekinjenega delovanja, rezervnih zmogljivosti in obveščanja. To pomaga zagotoviti, da se te ključne storitve ohranijo tudi v primerih, ko je komunikacijska infrastruktura močno motena.

Vzpostavitev mehanizmov za sodelovanje med javnimi organi ter nacionalnimi in evropskimi organi ter ustanovitev stalnega usklajevalnega odbora, ki vključuje različne deležnike, je ustrezno sredstvo za spodbujanje izmenjave informacij, institucionalnega usklajevanja in sprejemanja najboljših praks na področju varnosti in odpornosti.

Nazadnje, ukrep je skladen z evropskim regulativnim okvirom, ki izhaja iz direktive NIS2 ter direktive o odpornosti kritičnih subjektov, saj zagotavlja ustrezno usklajevanje s prihodnjo nacionalno zakonodajo za prenos in preprečuje regulativne vrzeli v sektorju, ki je strateškega pomena za gospodarstvo in nacionalno varnost.

9b. Sprejetje kraljeve uredbe je odgovor na dejansko in dokazano potrebo po okrepitvi zmogljivosti za preprečevanje, zaščito in obnovo infrastruktur, ki so postale ključnega pomena za delovanje družbe, gospodarstva in javnih storitev. Vse večja digitalizacija gospodarskih in družbenih dejavnosti, skupaj z vse večjo odvisnostjo od elektronskih komunikacijskih omrežij in storitev, pa tudi dogodki, kot so izbruh vulkana na La Palmi, hladen sistem nizkega zračnega tlaka, ki je prizadel različne dele države, ali nedavni izpad električne energije, so pokazali, da so elektronska komunikacijska omrežja in storitve izpostavljena najrazličnejšim tveganjem, ki bi lahko resno ogrozila zagotavljanje ključnih storitev državljanom, podjetjem in javnim organom. Ti incidenti so poudarili potrebo po krepitvi odpornosti digitalne infrastrukture in izboljšanju zmogljivosti za odzivanje na izredne razmere in krize.

Ta ukrep je potreben za izvajanje in uveljavitev člena 63 zakona 11/2022, tj. splošnega zakona o telekomunikacijah, ki določa obveznost operaterjev, da ustrezno obvladujejo varnostna tveganja ter zagotovijo celovitost svojih omrežij in storitev. Nujno je treba pripraviti predpise, ki bodo podrobneje določali obveznosti glede načrtovanja, preprečevanja, poročanja o incidentih, institucionalnega usklajevanja in nadzora, ki jih morajo izpolnjevati operaterji in druge zadevne strani.

Prav tako je potreba po uredbi upravičena zaradi delne zastarelosti trenutno veljavnega regulativnega okvira za poročanje o incidentih. Obstoječi postopki se ne odzivajo več ustrezno na zapletenost incidentov, ki lahko danes vplivajo na digitalna omrežja, storitve in infrastrukturo. Posodobitev vrst incidentov, komunikacijskih postopkov in rokov za poročanje je potrebna, da imajo pristojni organi na voljo zadostne in najnovejše informacije za usklajevanje hitrega in učinkovitega odziva na krizne razmere.

Vzpostaviti je treba tudi posebne mehanizme za zagotovitev neprekinjenega delovanja posebej kritičnih storitev, kot so komunikacija v nujnih primerih prek številke 112 in sistemi javnega opozarjanja. Izkušnje kažejo, da lahko vsaka prekinitev teh storitev neposredno vpliva na varovanje življenja, fizično integriteto ljudi in obvladovanje izrednih razmer. Zato uredba tako operaterjem kot centrom za klice v nujnih primerih nalaga posebne obveznosti v zvezi z načrtovanjem, rezervnimi zmogljivostmi in neprekinjenim delovanjem.

Poleg tega je ta ukrep potreben za izboljšanje nacionalnih in evropskih mehanizmov sodelovanja ter za ustanovitev posebnega usklajevalnega odbora, ki bo olajšal izmenjavo informacij, izkušenj in vzpostavitev skupnih postopkov za odzivanje na incidente, ki zaradi svoje narave pogosto hkrati vplivajo na več operaterjev in infrastrukturo.

Nazadnje je treba zagotoviti skladnost španskega pravnega sistema z novim evropskim regulativnim okvirom, ki izhaja iz direktive NIS2 in direktive o odpornosti kritičnih subjektov. Ti evropski instrumenti krepijo obveznosti v zvezi z varnostjo, obvladovanjem tveganja in odpornostjo kritične infrastrukture ter od držav članic zahtevajo, da razvijejo učinkovite mehanizme za preprečevanje in odkrivanje incidentov ter odzivanje nanje in okrevanje po njih.

9c. Predlagani ukrep ne nalaga prekomernega ali nesorazmernega bremena v primerjavi s cilji, ki se z njim zasledujejo, saj obveznosti, ki jih uvaja, izhajajo iz potrebe po zagotavljanju varnosti, odpornosti in neprekinjenega delovanja infrastruktur, ki so bistvene za delovanje družbe, gospodarstva in javnih storitev.

Sorazmernost ukrepa se kaže predvsem v dejstvu, da so številne določene obveznosti že del standardnih praks obvladovanja tveganj in zagotavljanja neprekinjenega poslovanja pri telekomunikacijskih operaterjih in upravljavcih digitalne infrastrukture. Analize tveganj, načrti za izredne razmere, protokoli za obnovo in nadzorni mehanizmi so standardni elementi pri upravljanju kritične infrastrukture in ključnih storitev. Kraljeva uredba ne predpisuje vzpostavitve povsem novih struktur, temveč sistematizira in poenoti določene obveznosti, da bi zagotovila minimalne standarde, ki veljajo za vse zavezane subjekte.

Poleg tega so predvideni ukrepi primerni glede na obseg tveganj, ki naj bi jih zmanjšali. Glede na ta tveganja je zahteva



EUROPEAN COMMISSION

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

po vzpostavitvi načrtov glede varnosti in odpornosti, rezervnih mehanizmov ter postopkov za zgodnje obveščanje razumen in nujen ukrep za zmanjšanje škode in pospešitev ponovne vzpostavitve storitev.

Uredba vključuje tudi mehanizme, ki omogočajo prilagajanje obveznosti okoliščinam vsakega reguliranega subjekta. Posamezni načrti morajo biti pripravljeni ob upoštevanju značilnosti vsakega omrežja, storitve ali infrastrukture, kar bo operaterjem omogočilo, da določijo najprimernejše tehnične in organizacijske ukrepe v skladu s svojimi specifičnimi tveganji. Ta prožnost preprečuje vsiljevanje enotnih ali togih rešitev, ki bi lahko povzročile nepotrebne stroške, ter spodbuja pristop, ki temelji na učinkovitem obvladovanju tveganj.

Kar zadeva poročanje o incidentih, so te obveznosti utemeljene s potrebo po posodobljenih in zanesljivih informacijah za usklajevanje odziva na incidente, ki lahko prizadenejo veliko število uporabnikov, operaterjev ali ozemelj. Poleg tega gre za podatke, ki jih morajo operaterji že zdaj zbrati in upravljati interno, da bi reševali incidente in zagotovili neprekinjeno delovanje svojih storitev; zato to ne pomeni nesorazmernega upravnega bremena v primerjavi s koristmi, ki jih prinaša v smislu usklajevanja in odzivnosti.

V poročilu o oceni regulativnega učinka je ugotovljeno tudi, da je gospodarski učinek uredbe obvladljiv in sorazmeren z javnim interesom, ki ga varuje. Čeprav ocenjeni finančni stroški za regulirane subjekte znašajo med 45 milijoni EUR in 90 milijoni EUR, so ti stroški povezani predvsem z naložbami, namenjenimi krepitvi odpornosti infrastrukture in zagotavljanju neprekinjenega delovanja ključnih storitev. Poleg tega so nove upravne obremenitve ocenjene na približno 19 276 EUR, kar je nizka vrednost v primerjavi z obsegom dejavnosti in gospodarsko velikostjo zadevnih gospodarskih subjektov. Poleg tega ta uredba za javne organe ne pomeni nobenih proračunskih stroškov, prav tako pa nima nobenega pomembnega vpliva na konkurenco.

Zaradi vseh teh razlogov je mogoče sklepati, da ukrep ne nalaga pretiranih obremenitev strankam, za katere se uporablja, temveč določa obveznosti, ki so sorazmerne, razumne in potrebne za zagotovitev visoke ravni varnosti in odpornosti omrežij in storitev elektronskih komunikacij.

10. Sklici na osnovna besedila:

11. Ne

12.

13. Da

Strateški interesi države

Elektronska komunikacijska omrežja in storitve so bistvena infrastruktura za nacionalno varnost, javne storitve, storitve v nujnih primerih, gospodarsko dejavnost in ozemeljsko kohezijo.

14. Ne

15. Da

16.

Vidik TOT: Ne

Vidik SFS: Ne

Evropska komisija

Direktiva o kontaktni točki (EU) 2015/1535

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