



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Broj notifikacije : 2026/0346/ES (Spain)

Nacrt Kraljevske uredbe o sigurnosti i otpornosti elektroničkih komunikacijskih mreža i usluga te određenih digitalnih infrastruktura.

Datum zaprimanja : 08/07/2026

Prestanak razdoblja mirovanja : 09/10/2026

Message

Poruka 001

Priopćenje Komisijev- TRIS/(2026) 1822

Direktiva (EU) 2015/1535

Obavijest: 2026/0346/ES

Obavijest o nacrtu teksta iz 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 - 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.HR

1. MSG 001 IND 2026 0346 ES HR 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 - Telekomunikacije

5. Nacrt Kraljevske uredbe o sigurnosti i otpornosti elektroničkih komunikacijskih mreža i usluga te određenih digitalnih infrastrukture.

6. Cilj joj je ojačati sigurnost, otpornost i kontinuitet elektroničkih komunikacijskih mreža i usluga, s njima povezane opreme i određene digitalne infrastrukture u Španjolskoj.

7.

8. Kraljevskom se uredbom nastoji osigurati sigurnost, otpornost i kontinuitet elektroničkih komunikacijskih mreža i usluga, s njima povezane opreme i određene digitalne infrastrukture u Španjolskoj.

Cilj je osigurati pružanje osnovnih usluga u slučaju sigurnosnih incidenata, prekida usluga ili značajnih pogoršanja, kao i regulirati obveze prijavljivanja takvih incidenata nadležnim tijelima.

Obveznici su operatori javnih elektroničkih komunikacijskih mreža, pružatelji javno dostupnih usluga, operatori povezane opreme i digitalne infrastrukture kao što su podmorski kabeli, satelitski sustavi, centri za obradu podataka, mreže za isporuku sadržaja i točke za razmjenu internetskog sadržaja, kao i, u određenim aspektima, pozivni centri za hitne slučajeve 112 i sustavi upozoravanja javnosti. Prepoznata je i osnovna priroda tih mreža i infrastruktura u izvanrednim situacijama.

Izrađen je „Plan nacionalne sigurnosti i otpornosti“, koji će definirati organizaciju odgovora na krize i institucionalne mehanizme koordinacije. Propisuje se i obveza obveznim subjektima da za svaku obvezanu stranu izrade „opći plan“, a za svaku vrstu mreže i određene usluge „specifične planove“. Moraju uključivati analize rizika, utvrđivanje osnovne infrastrukture, preventivne mjere, mehanizme oporavka i akcijske protokole za različite scenarije, kao što su nestanka struje, prirodne katastrofe, požari, kvarovi u području IT-a ili kibernetički napadi.

Uvode se posebne obveze kako bi se osigurao kontinuitet telekomunikacijskih usluga. Operatori poduzimaju mjere kako bi se utjecaj incidenata sveo na najmanju moguću mjeru i kako bi se osiguralo funkcioniranje ključnih usluga, posebno komunikacija prema hitnim službama. U iznimnim okolnostima mogu dati prednost određenim vrstama prometa, kao što su komunikacije prema hitnim službama ili glasovne i SMS usluge, uvijek poštujući načelo tehnološke neutralnosti. Osim toga, utvrđuju se najmanji zahtjevi u pogledu energetske autonomije za osnovnu infrastrukturu, a za pokretne mreže uvodi se obveza postupnog osiguravanja rezervne snage od najmanje četiri sata za 75 % stanovništva u roku od tri godine.

Uključuje sustav za izvješćivanje o značajnim incidentima koji se ne smatraju kibersigurnosnim incidentima, a potonji se uređuje u Direktivi NIS2 i Direktivi CER. Operatori obavješćuju Državno tajništvo o svakom značajnom incidentu u roku od jednog sata od saznanja o tom incidentu, a nakon toga redovito ažuriraju informacije tijekom trajanja prekida, nakon čega slijedi završno izvješće nakon ponovne uspostave usluge.

Uspostavljene su posebne mjere za hitne komunikacije putem broja 112 i sustava za javno upozoravanje. I centri za primanje hitnih poziva i operatori moraju uspostaviti mjere redundancije i kontinuiteta poslovanja, izraditi posebne planove za nepredvidive situacije i odmah prijaviti sve poremećaje tih usluga, koji se automatski klasificiraju kao značajni incidenti.

Kraljevskom se uredbom utvrđuju mjere i mehanizmi za koordinaciju s propisima o kibersigurnosti i otpornosti kritičnih subjekata (Direktiva NIS2 i Direktiva o otpornosti kritičnih subjekata), osnivanje koordinacijskog odbora za sigurnost i otpornost te buduće uvođenje digitalnih platformi za upravljanje incidentima i komunikaciju. Općenito, riječ je o znatnom jačanju obveza u pogledu sigurnosti, kontinuiteta i nadzora koje se primjenjuju na telekomunikacijski sektor i kritičnu digitalnu infrastrukturu.

9. Sve veća digitalizacija gospodarstva i javnih usluga znatno je povećala ovisnost o elektroničkim komunikacijskim mrežama i digitalnim infrastrukturama koje ih podržavaju. Ta je situacija ukazala na postojanje ranjivosti i rizika koji nisu ograničeni isključivo na područje kibersigurnosti, već utječu i na fizičku sigurnost i sposobnost infrastruktura da se odupru nepovoljnim događajima i oporave od njih. U tom se kontekstu smatra da je u Uredbi potrebno ojačati kapacitete za



EUROPEAN COMMISSION

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

prevenciju, odgovor i oporavak u slučaju incidenata koji bi mogli ugroziti dostupnost, cjelovitost ili funkcioniranje elektroničkih komunikacijskih mreža i usluga.

U obrazloženju Kraljevske uredbe ističe se niz nedavnih događaja koji su ukazali na potrebu za povećanjem otpornosti te infrastrukture. Među njima se spominju prirodne pojave poput vulkanske erupcije na La Palmi 2021. i hladnog ciklona koji je 2024. pogodio različite dijelove Španjolske, kao i događaji neprirodnog podrijetla, poput nedavnog nestanka struje diljem države. Ti su događaji pokazali da ekstremne prirodne pojave i tehnički kvarovi ili prekidi opskrbe električnom energijom mogu uzrokovati znatne poremećaje u komunikacijskim mrežama i ugroziti kontinuitet ključnih usluga za javnost i javna tijela.

Nadalje, digitalna transformacija iz temelja mijenja arhitekturu i funkcioniranje telekomunikacijskih mreža. Uvođenje tehnologija kao što su Internet stvari (IoT), umjetna inteligencija (AI), veliki podaci (Big Data), računarstvo u oblaku i virtualizacija usluga omogućilo je poboljšanje učinkovitosti, povezanosti i gospodarskog razvoja, ali je istodobno povećalo složenost sustava i stvorilo nove operativne i sigurnosne rizike. Stoga smatra da je ključno da se regulatorni okvir razvije kako bi se predvidjeli ti rizici i osigurale odgovarajuće razine zaštite i otpornosti.

S pravnog stajališta inicijativa se uglavnom temelji na članku 63. Zakona 11/2022 (Opći zakon o telekomunikacijama) o integritetu i sigurnosti elektroničkih komunikacijskih mreža i usluga. Nadalje, temelji se na postojećem zakonodavstvu o sigurnosti 5G mreža, posebno na Kraljevskoj uredbi sa zakonskom snagom 7/2022, Kraljevskoj uredbi sa zakonskom snagom 12/2018 o sigurnosti mreža i informacijskih sustava i Kraljevskoj uredbi 443/2024 kojom se odobrava nacionalni sigurnosni okvir za 5G mreže i usluge. Unatoč navedenom, iako su ova pravila dovela do značajnog napretka, potrebno je razviti poseban okvir koji sveobuhvatno obuhvaća sigurnost i otpornost svih mreža i usluga elektroničke komunikacije, kao i određene digitalne infrastrukture.

Naposljetku, u tekstu se objašnjava da se novom Kraljevskom uredbom nastoji dopuniti buduće španjolsko zakonodavstvo o kibernsigurnosti i otpornosti kritičnih subjekata. Stoga će se obveze koje proizlaze iz propisa kojima se prenose Direktiva NIS2 i Uredba o otpornosti kritičnih subjekata i dalje u potpunosti primjenjivati na kiberincidente i incidente koji utječu na digitalne mreže, usluge i infrastrukture i koji nisu izričito uređeni ovom Kraljevskom uredbom. Stoga je cilj osigurati dosljednost između različitih regulatornih instrumenata, izbjeći regulatorna preklapanja i uspostaviti sveobuhvatan sustav zaštite kojim se jačaju sigurnost, kontinuitet i otpornost telekomunikacijske i digitalne infrastrukture ključne za funkcioniranje španjolskog društva i španjolskog gospodarstva.

9.a Mjera je prikladna za postizanje željenog cilja jačanja sigurnosti, otpornosti i kontinuiteta elektroničkih komunikacijskih mreža i usluga te određenih digitalnih infrastrukture.

Iskustvo stečeno posljednjih godina pokazalo je da su telekomunikacijske mreže ključna infrastruktura za funkcioniranje društva, što je postalo očito tijekom pandemije bolesti COVID-19, kao i u hitnim situacijama koje su nastale uslijed ekstremnih prirodnih događaja, prekida napajanja ili sigurnosnih incidenata koji su utjecali na dostupnost usluga. U tom je scenariju donošenje posebnog regulatornog okvira primjereno za jačanje kapaciteta za sprječavanje incidenata koji mogu ugroziti kontinuitet elektroničkih komunikacija, odgovor na njih i oporavak od njih.

Uredbom se provode odredbe iz članka 63. Zakona 11/2022, Općeg zakona o telekomunikacijama. Njime se dopunjuje i prilagođava i regulatorni okvir tehnološkom razvoju i novim rizicima povezanim s digitalizacijom, virtualizacijom mreže, računalstvom u oblaku, umjetnom inteligencijom i internetom stvari, čije sve veće prihvaćanje povećava izloženost fizičkim i digitalnim ranjivostima. U tom je pogledu Kraljevska uredba odgovarajuć instrument za preciziranje sektorskih obveza koje omogućuju sveobuhvatan pristup tehničkim i operativnim specifičnostima telekomunikacijskog sektora.

Primjerenost mjere posebno se ogleda u uključivanju preventivnih mehanizama i mehanizama planiranja usmjerenih na poboljšanje pripravnosti subjekata u kriznim situacijama. Obveza izrade „Općih planova” i „Specifičnih planova” za mrežu ili uslugu, zajedno s izradom „Nacionalnog plana sigurnosti i otpornosti” i „Nacionalnog plana za civilne hitne situacije”, omogućuje uspostavljanje specifičnih postupaka za identifikaciju rizika, prevenciju, odgovor i oporavak.

Slično tome, ažuriranje postupaka izvještavanja o incidentima prikladna je mjera za poboljšanje sposobnosti nadležnih tijela za nadzor i upravljanje krizama. Iskustvo je pokazalo da je kriterije, rokove i sadržaj obavijesti potrebno prilagoditi složenijoj tehnološkoj i operativnoj stvarnosti.

Nadalje, mjera je dobro prilagođena jačanju zaštite osobito osjetljivih usluga, kao što su hitne komunikacije putem broja 112 i sustavi za javno upozoravanje, nametanjem posebnih obveza u pogledu kontinuiteta, redundantnosti i obavještavanja kako operaterima, tako i centrima za hitne pozive. To pomaže osigurati da se te ključne usluge održavaju čak i u situacijama kad je komunikacijska infrastruktura ozbiljno narušena.

Uspostava mehanizama suradnje između javnih vlasti i nacionalnih i europskih vlasti, kao i osnivanje stalnog



EUROPEAN COMMISSION

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

koordinacijskog odbora koji uključuje različite dionike, prikladno je sredstvo za poticanje razmjene informacija, institucionalne koordinacije i donošenja najboljih praksi u području sigurnosti i otpornosti.

Konačno, mjera je u skladu s europskim regulatornim okvirom koji proizlazi iz Direktiva NIS2 i CER, osiguravajući pravilnu koordinaciju s budućim nacionalnim zakonodavstvom o transpoziciji i sprječavajući regulatorne praznine u sektoru koji je strateški za gospodarstvo i nacionalnu sigurnost.

9.b Donošenjem Kraljevske uredbe odgovara se na stvarnu i dokazanu potrebu za jačanjem kapaciteta za sprječavanje, zaštitu i oporavak infrastruktura koje su postale ključne za funkcioniranje društva, gospodarstva i javnih usluga. Rastuća digitalizacija gospodarskih i društvenih aktivnosti, u kombinaciji sa sve većom ovisnošću o elektroničkim komunikacijskim mrežama i uslugama, kao i događaji poput erupcije vulkana na La Palmi, hladnog ciklona koji je pogodio različite dijelove države ili nedavnog nestanka struje, pokazali su da su elektroničke komunikacijske mreže i usluge izložene širokom rasponu rizika koji bi mogli ozbiljno ugroziti pružanje ključnih usluga građanima, poduzećima i javnim vlastima. Ti su incidenti istaknuli potrebu za jačanjem otpornosti digitalne infrastrukture i poboljšanjem kapaciteta za odgovor na hitne situacije i krize.

Ta je mjera potrebna za provedbu i primjenu članka 63. Zakona 11/2022, Općeg zakona o telekomunikacijama, kojim se utvrđuje obveza operatora da na odgovarajući način upravljaju sigurnosnim rizicima i da osiguraju integritet svojih mreža i usluga. Ključno je sastaviti propise kojima se detaljnije utvrđuju obveze u pogledu planiranja, sprječavanja, izvješćivanja o incidentima, institucionalne koordinacije i nadzora koje gospodarski subjekti i druge relevantne strane moraju ispuniti. Isto tako, potreba za uredbom opravdana je djelomičnom zastarjelošću regulatornog okvira koji je trenutačno na snazi za izvješćivanje o incidentima. Postojeći postupci više ne odgovaraju složenosti incidenata koji danas mogu utjecati na digitalne mreže, usluge i infrastrukturu. Ažuriranje vrsta incidenata, postupaka komunikacije i rokova izvješćivanja potrebno je kako bi nadležne vlasti imale dovoljno i ažurnih informacija za koordinaciju brzog i učinkovitog odgovora na krizne situacije.

Potrebno je i uspostaviti posebne mehanizme kako bi se osigurao kontinuitet posebno ključnih usluga, kao što su komunikacija prema hitnim službama putem broja 112 i sustavi javnog upozoravanja. Iskustvo pokazuje da svaki prekid tih usluga može imati izravne posljedice na zaštitu života, fizički integritet ljudi i upravljanje kriznim situacijama. Sukladno tome, propis nameće operaterima i centrima za hitne pozive posebne obveze u pogledu planiranja, redundantnosti i operativnog kontinuiteta.

Nadalje, mjera je potrebna za poboljšanje nacionalnih i europskih mehanizama suradnje te za osnivanje posebnog koordinacijskog odbora koji će olakšati razmjenu informacija i iskustava te uspostavu zajedničkih postupaka za odgovor na incidente koji po svojoj prirodi obično istodobno pogađaju više operatora i infrastrukture.

Naposlijetku, potrebno je osigurati usklađenost španjolskog pravnog sustava s novim europskim regulatornim okvirom koji proizlazi iz direktiva NIS2 i CER. Tim se europskim instrumentima jačaju obveze u pogledu sigurnosti, upravljanja rizicima i otpornosti kritične infrastrukture te se od država članica zahtijeva da razviju učinkovite mehanizme za sprečavanje, otkrivanje, odgovor i oporavak od incidenata.

9.c Predloženom mjerom ne nameće se prekomjerno ili nerazmjerno opterećenje u odnosu na ciljeve koji se žele postići jer se obvezama koje se njome uvode odgovara na potrebu za osiguravanjem sigurnosti, otpornosti i kontinuiteta infrastruktura koje su ključne za funkcioniranje društva, gospodarstva i javnih usluga.

Proporcionalnost mjere očita je, prije svega, u činjenici da su mnoge od navedenih obveza već dio standardnih praksi upravljanja rizikom i osiguranja kontinuiteta poslovanja telekomunikacijskih operatera i upravitelja digitalne infrastrukture. Analize rizika, planovi za nepredviđene situacije, protokoli oporavka i mehanizmi nadzora standardni su elementi u upravljanju kritičnom infrastrukturom i osnovnim uslugama. Kraljevskom se uredbom ne nalaže stvaranje potpuno novih struktura, nego se sistematiziraju i homogeniziraju određene obveze kako bi se osigurali minimalni zajednički standardi za sve obveznike.

Osim toga, predviđene su mjere primjerene opsegu rizika koje namjeravaju ublažiti. S obzirom na te rizike, zahtjev da se uspostave planovi za sigurnost i otpornost, rezervni mehanizmi i postupci ranog obavješćivanja razuman je i nužan odgovor kako bi se šteta svela na najmanju moguću mjeru i ubrzala obnova usluga.

Pravilnik uključuje i mehanizme koji omogućuju prilagodbu obveza okolnostima svakog reguliranog subjekta. Posebni planovi trebali bi se izraditi uzimajući u obzir značajke svake mreže, usluge ili infrastrukture, čime bi se operatorima omogućilo da odrede najprikladnije tehničke i organizacijske mjere u skladu sa svojim specifičnim rizicima. Tom se fleksibilnošću izbjegava uvođenje jedinstvenih ili krutih rješenja koja bi mogla stvoriti nepotrebne troškove i pogoduje



EUROPEAN COMMISSION

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

pristupu koji se temelji na učinkovitom upravljanju rizikom.

Kad je riječ o izvješćivanju o incidentima, te su obveze opravdane potrebom za ažuriranim i pouzdanim informacijama za koordinaciju odgovora na incidente koji mogu utjecati na velik broj korisnika, operatora ili područja. Nadalje, potrebne su informacije koje su operatori ionako obvezni prikupljati i interno obrađivati kako bi riješili incidente i osigurali kontinuitet svojih usluga; stoga ne nameće nerazmjerno administrativno opterećenje u odnosu na koristi koje donosi u pogledu koordinacije i operativnosti.

Izvršće o procjeni regulatornog utjecaja zaključuje i da je gospodarski utjecaj koji proizlazi iz regulative upravljiv i proporcionalan javnom interesu koji štiti. Iako procijenjeni financijski trošak za regulirane subjekte iznosi od 45 milijuna EUR do 90 milijuna EUR, taj je trošak prvenstveno povezan s ulaganjima usmjerenima na jačanje otpornosti infrastrukture i osiguravanje kontinuiteta osnovnih usluga. Osim toga, nova administrativna opterećenja kvantificirana su na približno 19 276 EUR, što je nizak iznos u usporedbi s obujmom djelatnosti i gospodarskom veličinom predmetnih subjekata. Nadalje, Uredba ne podrazumijeva nikakve proračunske troškove za javne vlasti, niti ima značajan utjecaj na konkurenciju.

Iz svih navedenih razloga može se zaključiti da mjera ne nameće pretjerana opterećenja strankama na koje se odnosi, već uspostavlja obveze koje su proporcionalne, razumne i nužne za osiguranje visoke razine sigurnosti i otpornosti mreža i usluga elektroničke komunikacije.

10. Upućivanje na temeljne tekstove:

11. Ne

12.

13. Da

Strateški interesi zemlje

Elektroničke komunikacijske mreže i usluge ključna su infrastruktura za nacionalnu sigurnost, javne usluge, hitne službe, gospodarsku aktivnost i teritorijalnu koheziju.

14. Ne

15. Da

16.

Sa stajališta TBT-a: Ne

Sa stajališta SPS-a: Ne

Europska komisija

Služba za kontakt Direktive (EU) 2015/1535

E-pošta: grow-dir2015-1535-central@ec.europa.eu