



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Нотификационен номер : 2026/0346/ES (Spain)

Проект на Кралски указ относно сигурността и устойчивостта на електронни съобщителни мрежи и услуги, както и някои цифрови инфраструктури.

Дата на получаване : 08/07/2026

Край на период на прекъсване : 09/10/2026

Message

Съобщение 001

Съобщение от Комисията - TRIS/(2026) 1822

Директива (ЕС) 2015/1535

Нотификация 2026/0346/ES

Нотификация на проект на текст от държава членка

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.BG

1. MSG 001 IND 2026 0346 ES BG 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 - Далекосъобщения

5. Проект на Кралски указ относно сигурността и устойчивостта на електронни съобщителни мрежи и услуги, както и някои цифрови инфраструктури.

6. С него се цели да се укрепят сигурността, устойчивостта и непрекъснатостта на електронни съобщителни мрежи и услуги, свързани с тях съоръжения и някои цифрови инфраструктури в Испания.

7.

8. Целта на кралския указ е да се гарантират сигурността, устойчивостта и непрекъснатостта на електронни съобщителни мрежи и услуги, свързани с тях съоръжения и някои цифрови инфраструктури в Испания. Целта е да се гарантира предоставянето на съществени услуги в случай на инциденти, свързани със сигурността, прекъсвания на услугите или значително влошаване на качеството, както и да се регламентират задълженията за докладване на такива инциденти пред компетентните органи.

Задължените субекти са оператори на обществени електронни съобщителни мрежи, доставчици на обществено достъпни услуги, оператори на свързани съоръжения и цифрови инфраструктури, като например подводни кабели, спътникови системи, центрове за обработка на данни, мрежи за доставка на съдържание и точки за обмен в интернет, както и, в някои отношения, центрове за спешни повиквания на номер 112 и системи за предупреждение на населението. Признава се също така съществения характер на тези мрежи и инфраструктури при извънредни ситуации.

Изготвен е „План за национална сигурност и устойчивост“, с който ще се определи организацията на реакцията при кризи и механизмите за институционална координация. С него също така се определя задължението на задължените субекти да изготвят „общ план“ за всяка задължена страна и „специфични планове“ за всеки вид мрежа и специфични услуги. Те трябва да включват анализи на рисковете, идентифицирането на съществената инфраструктура, превантивни мерки, механизми за възстановяване и протоколи за действие за различни сценарии, като прекъсвания на електрозахранването, природни бедствия, пожари, информационно-технологични повреди или кибератаки.

Въвеждат се специфични задължения за осигуряване на непрекъснатостта на телекомуникационните услуги. Операторите предприемат мерки за свеждане до минимум на въздействието на инцидентите и гарантират функционирането на съществените услуги, по-специално на спешните повиквания. При изключителни обстоятелства те могат да дадат приоритет на някои видове трафик, като например спешни повиквания или услуги за гласови съобщения и текстови съобщения, като винаги се спазва принципът на технологична неутралност. В допълнение са определени минимални изисквания за енергийна автономност за съществената инфраструктура, а на мобилните мрежи се налага задължението в рамките на три години постепенно да осигурят резервно електрозахранване за минимум четири часа за 75 % от населението.

В него се включва система за докладване на значителни инциденти, които не се считат за киберинциденти, като последните са регламентирани в Директивата МИС 2 и Директивата за УКС. Операторите следва да уведомят Държавния секретариат за всеки значителен инцидент в рамките на един час от момента, в който научат за него, и впоследствие да предоставят редовни актуализации за целия период на прекъсването, след което да представят окончателен доклад, след като услугата бъде възстановена.

Въвеждат се специфични мерки за комуникация при извънредни ситуации чрез номер 112 и системите за предупреждение на населението. Както централите за спешни повиквания, така и операторите трябва да въведат мерки за предоставяне на резервност и осигуряване на непрекъснатост на дейността, да изготвят специфични планове за действие при извънредни ситуации и незабавно да докладват за всяко прекъсване на тези услуги, които автоматично се класифицират като значителни инциденти.

С кралския указ се определят мерки и механизми за координация с наредбите относно киберсигурността и



EUROPEAN COMMISSION

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

устойчивостта на критичните субекти (Директивата МИС 2 и Директивата за УКС), създаването на Координационен комитет по сигурността и устойчивостта и бъдещото въвеждане на цифрови платформи за управление на инциденти и комуникация. Като цяло това представлява значително засилване на задълженията, свързани със сигурността, непрекъснатостта и надзора, приложими за далекосъобщителния отрасъл и критичните цифрови инфраструктури.

9. С нарастващата цифровизация на икономиката и обществените услуги значително се увеличава зависимостта от електронните съобщителни мрежи и от цифровите инфраструктури, които ги подпомагат. Тази ситуация извежда на преден план наличието на уязвимости и рискове, които не се ограничават изключително до областта на киберсигурността, а засягат и физическата сигурност, както и способността на инфраструктурите да издържат на и да се възстановяват от неблагоприятни събития. В този контекст с наредбата се счита за необходимо да се укрепи способността за превенция, реакция и възстановяване в случай на инциденти, които биха могли да застрашат достъпността, целостта или функционирането на електронни съобщителни мрежи и услуги.

В обяснителния меморандум към кралския указ се изтъкват редица скорошни събития, които са показали необходимостта от повишаване на устойчивостта на тези инфраструктури. Наред с тях, в него се посочват природни явления като вулканичното изригване на остров Ла Палма през 2021 г. и атмосферния фронт с ниско налягане, който засегна различни части на Испания през 2024 г., както и инциденти, които нямат произход, свързан с природата, като например неотдавнашното прекъсване на електрозахранването в цялата държава. Тези събития показаха, че както екстремните природни явления, така и техническите неизправности или прекъсванията в електрозахранването могат да причинят значителни смущения в съобщителните мрежи и да застрашат непрекъснатостта на съществените услуги за гражданите и публичните органи.

Освен това цифровата трансформация променя дълбоко архитектурата и функционирането на далекосъобщителните мрежи. Включването на технологии като интернет на нещата, изкуствен интелект, големи информационни масиви, компютърни услуги „в облак“ и виртуализация на услугите даде възможност за подобряване на ефективността, свързаността и икономическото развитие, но същевременно увеличи сложността на системите и породиха нови оперативни рискове и рискове за сигурността. Поради това се счита, че е от съществено значение регулаторната рамка да се развива, за да се предвидят тези рискове и да се гарантират подходящи равнища на защита и устойчивост.

От правна гледна точка инициативата се основава предимно на член 63 от Закон № 11/2022, Общия закон за далекосъобщенията, относно целостта и сигурността на електронни съобщителни мрежи и услуги. Освен това се води до съществуващото законодателство в областта на сигурността на 5G мрежите, по-специално на Кралския указ-закон № 7/2022, Кралския указ-закон № 12/2018 относно сигурността на мрежите и информационните системи, както и Кралския указ № 443/2024 за одобряване на Националната рамка за сигурност на 5G мрежите и услугите. Независимо от горепосоченото, макар че тези наредби доведоха до значителен напредък, е необходимо да се разработи специфична рамка, която изчерпателно да обхваща сигурността и устойчивостта на всички електронни съобщителни мрежи и услуги, както и някои цифрови инфраструктури.

Накрая в текста се обяснява, че с новия кралски указ се цели да се допълни бъдещото испанско законодателство в областта на киберсигурността и устойчивостта на критичните субекти. Следователно задълженията, произтичащи от наредбите за транспониране на МИС 2 и УКС, ще продължат да се прилагат изцяло за киберинцидентите и инцидентите, които засягат цифровите мрежи, услуги и инфраструктури и които не са изрично регламентирани в настоящия кралски указ. Целта е следователно да се осигури съгласуваност между различните регулаторни инструменти, да се избегнат регулаторни припокривания и да се създаде всеобхватна система за защита, която укрепва сигурността, непрекъснатостта и устойчивостта на далекосъобщителната и цифровата инфраструктура, които са от съществено значение за функционирането на испанското общество и испанската икономика.

9а. Мярката е подходяща за постигане на преследваната цел за укрепване на сигурността, устойчивостта и непрекъснатостта на електронни съобщителни мрежи и услуги, както и някои цифрови инфраструктури. Опитът, натрупан през последните години, показва, че далекосъобщителните мрежи са съществена инфраструктура за функционирането на обществото, както стана ясно по време на пандемията от COVID-19, а също така в извънредни ситуации, възникнали вследствие на екстремни природни явления, прекъсвания на



EUROPEAN COMMISSION

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

електрозахранването или инциденти, свързани със сигурността, които са засегнали достъпността на услугите. В този сценарий е целесъобразно да се приеме специфична регулаторна рамка, за да се укрепи способността за превенция, реакция и възстановяване след инциденти, които могат да застрашат непрекъснатостта на електронните съобщения.

С наредбата се прилагат разпоредбите, съдържащи се в член 63 от Закон № 11/2022, Общия закон за далекосъобщенията. Освен това с нея се допълва и адаптира регулаторната рамка към технологичните промени и новите рискове, свързани с цифровизацията, виртуализацията на мрежите, компютърните услуги „в облак“, изкуствения интелект и интернета на нещата, чието все по-широко приене увеличава уязвимостта както от физически, така и от цифров характер. В тази връзка кралският указ е подходящият инструмент за определяне на секторни задължения, които позволяват цялостен подход към техническите и оперативните особености на далекосъобщителния отрасъл.

Целесъобразността на мярката е отразена по-специално в включването на механизми за превенция и планиране, насочени към подобряване на готовността на операторите в кризисни ситуации. Задължението за изготвяне на „общи планове“ и „специфични планове“ по мрежи или услуги, заедно с изготвянето на „Национален план за сигурност и устойчивост“ и „Национален план за гражданска готовност при извънредни ситуации“, дава възможност за установяване на специфични процедури за идентификация на рисковете, превенция, реакция и възстановяване.

По същия начин актуализирането на процедурите за докладване на инциденти е подходяща мярка за подобряване на способността на компетентните органи да осъществяват мониторинг и управляват кризи. Опитът показва необходимостта от адаптиране на критериите, сроковете и съдържанието на нотификациите към по-сложната технологична и оперативна действителност.

Освен това мярката е подходяща за укрепване на защитата на особено чувствителни услуги, като например спешните повиквания чрез номер 112 и системите за предупреждение на населението, чрез налагане на специфични задължения по отношение на непрекъснатостта, дублирането и уведомяването както на операторите, така и на центровете за спешни повиквания. Това спомага за гарантирането на непрекъснатостта на тези критични услуги дори в ситуации, при които съобщителната инфраструктура е сериозно нарушена. Установяването на механизми за сътрудничество между публичните органи и националните и европейските органи, както и създаването на постоянен координационен комитет, включващ различните заинтересовани страни, е подходящо средство за насърчаване на обмена на информация, институционалната координация и приемането на най-добри практики в областта на сигурността и устойчивостта.

И накрая, мярката е в съответствие с европейската регулаторна рамка, произтичаща от Директивата МИС 2 и Директивата за УКС, като гарантира подходяща координация с бъдещото национално законодателство в областта на транспонирането и предотвратява регулаторните пропуски в отрасъл, който е стратегически за икономиката и националната сигурност.

96. Приемането на кралския указ е отговор на действителна и доказана необходимост от укрепване на способността за превенция, защита и възстановяване на инфраструктурите, които са станали от съществено значение за функционирането на обществото, икономиката и обществените услуги.

Увеличаващата се цифровизация на икономическите и социалните дейности, съчетана с все по-голямата зависимост от електронни съобщителни мрежи и услуги, както и събития като вулканичното изригване на остров Ла Палма и атмосферния фронт с ниско налягане, който засегна различни части на държавата, или неотдавнашното прекъсване на електрозахранването, показаха, че електронни съобщителни мрежи и услуги са изложени на широк спектър от рискове, които биха могли сериозно да застрашат предоставянето на съществени услуги на гражданите, предприятията и публичните органи. Тези инциденти подчертаха необходимостта от укрепване на устойчивостта на цифровата инфраструктура и подобряване на способността за реакция при извънредни ситуации и кризи.

Тази мярка е необходима за прилагането и привеждането в действие на член 63 от Закон № 11/2022, Общия закон за далекосъобщенията, с който се определя задължението на операторите да управляват рисковете за сигурността по подходящ начин и да гарантират целостта на техните мрежи и услуги. От съществено значение е да се изготвят наредби, в които да се определят по-подробно задълженията по отношение на планирането, превенцията, докладването на инциденти, институционалната координация и надзора, които операторите и другите заинтересовани страни трябва да изпълняват.



EUROPEAN COMMISSION

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

По същия начин необходимостта от наредбата е обоснована от частичното остаряване на действащата понастоящем регулаторна рамка за докладване на инциденти. Съществуващите процедури вече не отговарят по подходящ начин на сложността на инцидентите, които могат да засегнат цифровите мрежи, услуги и инфраструктури понастоящем. Актуализирането на видовете инциденти, процедурите за комуникация и сроковете за докладване е необходимо, за да разполагат компетентните органи с достатъчна и актуална информация, с която да координират бърза и ефективна реакция при кризисни ситуации.

Необходимо е също така да се установят специфични механизми, за да се гарантира непрекъснатостта на особено критичните услуги, като например спешните повиквания чрез номер 112 и системите за предупреждение на населението. Опитът показва, че всяко прекъсване на тези услуги може да има преки последици за опазването на живота, физическата неприкосновеност на хората и управлението на извънредни ситуации. Следователно с наредбата се налагат специфични задължения по отношение на планирането, предоставянето на резервност и оперативната непрекъснатост както на операторите, така и на центровете за спешни повиквания.

Освен това тази мярка е необходима за подобряване на механизмите за сътрудничество на национално и европейско равнище, както и за създаване на специален координационен комитет, който да улеснява обмена на информация, споделянето на опит и установяването на общи процедури за реакция при инциденти, които по тяхната същност обикновено засягат едновременно множество оператори и обекти на инфраструктурата. И накрая, необходимо е да се гарантира съгласуваността на испанската правна система с новата европейска регулаторна рамка, произтичаща от Директивите МИС2 и за УКС. С тези европейски инструменти се укрепват задълженията по отношение на сигурността, управлението на риска и устойчивостта на критичната инфраструктура, и се изисква от държавите членки да разработят ефективни механизми за превенция, откриване, реакция и възстановяване от инциденти.

9в. С предложената мярка не се налага прекомерна или непропорционална тежест по отношение на преследваните цели, тъй като въведените с нея задължения отговарят на необходимостта да се гарантират сигурността, устойчивостта и непрекъснатостта на инфраструктурите, които са от съществено значение за функционирането на обществото, икономиката и обществените услуги.

Пропорционалността на мярката се проявява преди всичко в това, че много от предвидените задължения вече са част от стандартните практики за управление на риска и осигуряване на непрекъснатост на дейността на далекосъобщителните оператори и управителите на цифрова инфраструктура. Анализите на рисковете, плановете за действие при извънредни ситуации, протоколите за възстановяване и механизмите за надзор са стандартни елементи при управлението на критичната инфраструктура и съществените услуги. С кралския указ не се налага създаването на изцяло нови структури, а по-скоро се систематизират и уеднаквяват някои задължения, с цел да се гарантират минимални стандарти, общи за всички субекти, подлежащи на това задължение.

В допълнение предвидените мерки са подходящи по отношение на мащаба на рисковете, които те целят да намалят. Предвид тези рискове изискването за наличие на плановете за сигурност и устойчивост, механизми за предоставяне на резервност и процедури за ранно уведомяване е разумна и необходима мярка за свеждане до минимум на щетите и ускоряване на възстановяването на услугите.

Наредбата включва също така механизми, които позволяват задълженията да бъдат съобразени с конкретните обстоятелства на всеки регулиран субект. Специфичните плановете следва да се изготвят, като се отчитат характеристиките на всяка мрежа, услуга или инфраструктура, което ще позволи на операторите да определят най-подходящите технически и организационни мерки в зависимост от специфичните рискове, с които те се сблъскват. С тази гъвкавост се позволява да се избегне налагането на еднообразни или твърди решения, които биха могли да доведат до ненужни разходи, както и се насърчава подходът, основан на ефективно управление на риска.

Що се отнася до докладването на инциденти, тези задължения са обосновани от необходимостта да се разполага с актуална и надеждна информация, за да се координира реакцията при инциденти, които могат да засегнат голям брой ползватели, оператори или територии. Освен това изискваната информация е именно тази, която операторите вече са длъжни да събират и управляват вътрешно, за да разрешават инциденти и да осигуряват непрекъснатостта на техните услуги; следователно с нея не се налага непропорционална административна тежест в сравнение с ползите, които носи по отношение на координацията и способността за



EUROPEAN COMMISSION

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

реакция.

В доклада за оценка на регулаторното въздействие се прави също така заключението, че икономическото въздействие, произтичащо от наредбата, е управляемо и пропорционално на обществения интерес, който се защитава с нея. Въпреки че очакваните финансови разходи за регулираните субекти са между 45 и 90 млн. евро, тези разходи са свързани предимно с инвестиции, насочени към укрепване на устойчивостта на инфраструктурата и гарантиране на непрекъснатостта на съществените услуги. В допълнение новите административни тежести се оценяват на приблизително 19 276 EUR, което е ниска стойност в сравнение с обема на дейността и икономическия размер на съответните оператори. Освен това наредбата не води до каквито и да било бюджетни разходи за публичните органи, нито оказва значително въздействие върху конкуренцията.

Поради всички тези причини може да се направи заключението, че с мярката не се налага прекомерна тежест на страните, по отношение на които се прилага, а по-скоро се установяват задължения, които са пропорционални, разумни и необходими, за да се гарантира високо равнище на сигурност и устойчивост на електронни съобщителни мрежи и услуги.

10. Препратки към основните текстове:

11. Не

12.

13. Да

Стратегически интереси на страната

Електронни съобщителни мрежи и услуги представляват жизненоважна инфраструктура за националната сигурност, обществените услуги, службите за спешна помощ, икономическата дейност и териториалното сближаване.

14. Не

15. Да

16.

Аспект ОТС: Не

Аспект СПС: Не

Европейска Комисия

Контактна точка Директива (ЕС) 2015/1535

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