



EUROPEAN COMMISSION

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

Single Market Enforcement

Notification of Regulatory Barriers

Notification Number : 2026/0346/ES (Spain)

Draft Royal Decree on the Security and Resilience of Electronic Communications Networks and Services and Certain Digital Infrastructures.

Date received : 08/07/2026

End of Standstill : 09/10/2026

Message

Message 001

Communication from the Commission - TRIS/(2026) 1822

Directive (EU) 2015/1535

Notification: 2026/0346/ES

Notification of a draft text from a Member State

Notification – Notifikation – 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.EN

1. MSG 001 IND 2026 0346 ES EN 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 - TELECOMS

5. Draft Royal Decree on the Security and Resilience of Electronic Communications Networks and Services and Certain Digital Infrastructures.

6. It aims to strengthen the security, resilience and continuity of electronic communications networks and services, their associated facilities and certain digital infrastructures in Spain.

7.

8. The Royal Decree aims to ensure the security, resilience and continuity of electronic communications networks and services, their associated facilities and certain digital infrastructures in Spain.

The objective is to ensure the provision of essential services in the event of security incidents, service interruptions or significant degradations, as well as to regulate the obligations to report such incidents to the authorities.

The obliged entities are operators of public electronic communications networks, providers of publicly available services, operators of associated facilities and digital infrastructures such as submarine cables, satellite systems, data processing centres (DPCs), content delivery networks (CDNs) and internet exchange points (IXPs), as well as, in certain respects, 112 emergency call centres and public warning systems. The essential nature of these networks and infrastructures in emergency situations is also recognised.

A 'National Security and Resilience Plan' has been drawn up, which will define the organisation of the crisis response and the institutional coordination mechanisms. It also lays down the obligation for obliged entities to draw up a 'general plan' for each obliged party and 'specific plans' for each type of network and specific services. They must include risk analyses, the identification of essential infrastructure, preventive measures, recovery mechanisms and action protocols for various scenarios, such as power cuts, natural disasters, fires, IT failures or cyber-attacks.

Specific obligations are introduced to ensure the continuity of telecommunications services. Operators shall take measures to minimise the impact of incidents and ensure the functioning of essential services, in particular emergency communications. In exceptional circumstances, they may prioritise certain types of traffic, such as emergency communications or voice and SMS services, whilst always respecting the principle of technological neutrality. In addition, minimum energy autonomy requirements are laid down for essential infrastructure and an obligation is imposed on mobile networks to progressively ensure a minimum of four hours' back-up power for a percentage of 75 % of the population within three years.

It includes a system for reporting significant incidents that are not considered cybersecurity incidents, the latter being regulated in the NIS2 Directive and the CER Directive. Operators shall notify the Secretariat of State of any significant incident within one hour of becoming aware of it, and shall subsequently provide regular updates for the duration of the disruption, followed by a final report once the service has been restored.

Specific measures are established for emergency communications through the 112 number and public warning systems. Both emergency call centres and operators must put in place redundancy and business continuity measures, draw up specific contingency plans and immediately report any disruption to these services, which are automatically classified as significant incidents.

The Royal Decree sets out measures and mechanisms for coordination with the regulations on cybersecurity and resilience for critical entities (the NIS2 Directive and the CER Directive), the establishment of a Security and Resilience Coordination Committee, and the future roll-out of digital platforms for incident management and communication. Overall, it represents a significant reinforcement of the security, continuity and oversight obligations applicable to the telecommunications sector and critical digital infrastructures.

9. The increasing digitalisation of the economy and public services has significantly increased the dependency on electronic communications networks and the digital infrastructures that support them. This situation has highlighted the



EUROPEAN COMMISSION

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

existence of vulnerabilities and risks that are not limited exclusively to the area of cybersecurity, but also affect the physical security and the ability of infrastructures to withstand and recover from adverse events. In this context, the regulation considers it necessary to strengthen the capacity for prevention, response and recovery in the event of incidents that could compromise the availability, integrity or functioning of electronic communications networks and services.

The explanatory memorandum to the Royal Decree highlights a number of recent events that have demonstrated the need to increase the resilience of these infrastructures. Among these, it mentions natural phenomena such as the volcanic eruption on La Palma in 2021 and the cold low-pressure system that affected various parts of Spain in 2024, as well as incidents of non-natural origin, such as the recent nationwide power outage. These events demonstrated that both extreme natural phenomena and technical or power failures can cause significant disruption to communications networks and jeopardise the continuity of essential services for the public and public authorities.

Furthermore, digital transformation is profoundly changing the architecture and functioning of telecommunications networks. The incorporation of technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), Big Data, cloud computing and service virtualisation has made it possible to improve efficiency, connectivity and economic development, but at the same time has increased the complexity of the systems and has generated new operational and security risks. Therefore, it considers it essential that the regulatory framework evolve to anticipate these risks and ensure appropriate levels of protection and resilience.

From a legal point of view, the initiative is mainly based on Article 63 of Law 11/2022, the General Telecommunications Act, on the integrity and security of electronic communications networks and services. Furthermore, it draws on existing legislation on 5G network security, in particular Royal Decree-Law 7/2022, Royal Decree-Law 12/2018 on the security of networks and information systems, and Royal Decree 443/2024 approving the National Security Framework for 5G Networks and Services. Notwithstanding the above, whilst these regulations have led to significant progress, it is necessary to develop a specific framework that comprehensively addresses the security and resilience of all electronic communications networks and services, as well as certain digital infrastructures.

Finally, the text explains that the new Royal Decree aims to act in a complementary way to the future Spanish legislation on cybersecurity and resilience of critical entities. Consequently, the obligations arising from the regulations transposing NIS2 and CER will continue to be fully applicable to cybersecurity incidents and those incidents that affect digital networks, services and infrastructures and that are not expressly regulated in this Royal Decree. The aim is thus to ensure consistency between the various regulatory instruments, to avoid regulatory overlaps and to establish a comprehensive protection system that strengthens the security, continuity and resilience of telecommunications and digital infrastructure essential to the functioning of Spanish society and the Spanish economy.

9a. The measure is suitable to achieve the pursued objective of strengthening the security, resilience and continuity of electronic communications networks and services and of certain digital infrastructures.

The experience gained in recent years has shown that telecommunications networks are essential infrastructures for the functioning of society, as evidenced during the COVID-19 pandemic, as well as in emergency situations arising from extreme natural events, power outages or security incidents that have affected the availability of services. In this scenario, the adoption of a specific regulatory framework is appropriate to strengthen the capacity to prevent, respond to and recover from incidents that may compromise the continuity of electronic communications.

The regulation implements the provisions contained in Article 63 of Law 11/2022, the General Telecommunications Act. It also complements and adapts the regulatory framework to technological developments and the new risks associated with digitalisation, network virtualisation, cloud computing, artificial intelligence and the IoT, the growing adoption of which increases exposure to vulnerabilities of both a physical and digital nature. In this regard, the Royal Decree is the appropriate instrument for specifying sectoral obligations that enable a comprehensive approach to the technical and operational particularities of the telecommunications sector.

The appropriateness of the measure is reflected in particular in the incorporation of preventive and planning mechanisms aimed at improving the preparedness of operators in crisis situations. The obligation to draw up 'General Plans' and 'Specific Plans' by network or service, together with the drawing up of a 'National Security and Resilience Plan' and a 'National Civil Emergency Plan', makes it possible to establish specific procedures for risk identification, prevention, response and recovery.

Similarly, the updating of incident reporting procedures is an appropriate measure to improve the monitoring and crisis management capacity of the competent authorities. Experience has shown the need to adapt the criteria, deadlines and



EUROPEAN COMMISSION

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

content of notifications to a more complex technological and operational reality.

Furthermore, the measure is well suited to strengthening the protection of particularly sensitive services, such as emergency communications via the 112 number and public warning systems, by imposing specific obligations regarding continuity, redundancy and notification on both operators and emergency call centres. This helps to ensure that these critical services are maintained even in situations where communications infrastructure is severely disrupted.

The establishment of cooperation mechanisms between public authorities and national and European authorities, as well as the creation of a permanent coordination committee involving the various stakeholders, is an appropriate means of promoting the exchange of information, institutional coordination and the adoption of best practice in the field of security and resilience.

Finally, the measure is consistent with the European regulatory framework arising from the NIS2 and CER Directives, ensuring proper coordination with future national transposition legislation and preventing regulatory gaps in a sector that is strategic for the economy and national security.

9b. The adoption of the Royal Decree responds to a real and proven need to strengthen the prevention, protection and recovery capacity of infrastructures that have become essential for the functioning of society, the economy and public services.

The increasing digitalisation of economic and social activities, coupled with a growing reliance on electronic communications networks and services, as well as events such as the volcanic eruption on La Palma, the cold low-pressure system that affected various parts of the country, or the recent power outage, have shown that electronic communications networks and services are exposed to a wide variety of risks that could seriously jeopardise the provision of essential services to citizens, businesses and public authorities. These incidents have highlighted the need to strengthen the resilience of digital infrastructure and improve the capacity to respond to emergencies and crises.

This measure is necessary to implement and give effect to Article 63 of Law 11/2022, the General Telecommunications Act, which sets out the obligation for operators to manage security risks appropriately and to ensure the integrity of their networks and services. It is essential to draw up regulations that set out in greater detail the obligations regarding planning, prevention, incident reporting, institutional coordination and supervision that operators and other relevant parties must fulfil.

Likewise, the need for the regulation is justified by the partial obsolescence of the regulatory framework currently in force for incident reporting. The existing procedures no longer adequately respond to the complexity of the incidents that may affect digital networks, services and infrastructures today. The updating of the types of incidents, communication procedures and reporting deadlines is necessary in order for the competent authorities to have sufficient and up-to-date information to coordinate a rapid and effective response to crisis situations.

It is also necessary to establish specific mechanisms to ensure the continuity of particularly critical services, such as emergency communications through the 112 number and public warning systems. Experience shows that any interruption of these services can have direct consequences on the protection of life, the physical integrity of people and emergency management. Consequently, the regulation imposes specific obligations regarding planning, redundancy and operational continuity on both operators and emergency call centres.

Furthermore, the measure is necessary to improve national and European cooperation mechanisms, and to establish a dedicated coordination committee to facilitate the exchange of information, the sharing of experiences and the establishment of common procedures for responding to incidents which, by their very nature, tend to affect multiple operators and infrastructure simultaneously.

Finally, it is necessary to ensure the coherence of the Spanish legal system with the new European regulatory framework derived from the NIS2 and CER Directives. These European instruments strengthen the obligations regarding security, risk management and resilience of critical infrastructure, and require Member States to develop effective mechanisms for the prevention, detection, response and recovery from incidents.

9c. The proposed measure does not impose an excessive or disproportionate burden in relation to the objectives pursued, since the obligations it introduces respond to the need to ensure the security, resilience and continuity of infrastructures that are essential for the functioning of society, the economy and public services.

The proportionality of the measure is evident, first and foremost, in the fact that many of the obligations set out are already part of the standard risk management and business continuity practices of telecommunications operators and digital infrastructure managers. Risk analyses, contingency plans, recovery protocols and oversight mechanisms are



EUROPEAN COMMISSION

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

standard elements in the management of critical infrastructure and essential services. The Royal Decree does not impose the creation of completely new structures, but rather systematises and homogenises certain obligations in order to ensure minimum standards common to all the obliged entities.

In addition, the measures envisaged are appropriate to the magnitude of the risks they intend to mitigate. In the face of these risks, the requirement to have security and resilience plans, backup mechanisms and early notification procedures in place is a reasonable and necessary response to minimise damage and speed up the restoration of services.

The regulation also incorporates mechanisms that allow the obligations to be tailored to the circumstances of each regulated entity. The specific plans should be drawn up taking into account the characteristics of each network, service or infrastructure, allowing operators to determine the most appropriate technical and organisational measures according to their specific risks. This flexibility avoids imposing uniform or rigid solutions that could generate unnecessary costs and favours an approach based on effective risk management.

As regards incident reporting, these obligations are justified by the need to have up-to-date and reliable information to coordinate the response to incidents that may affect a large number of users, operators or territories. Furthermore, the information required is that which operators are already required to collect and manage internally in order to resolve incidents and ensure the continuity of their services; it therefore does not impose a disproportionate administrative burden in relation to the benefits it brings in terms of coordination and responsiveness.

The Regulatory Impact Assessment Report also concludes that the economic impact resulting from the regulation is manageable and proportionate to the public interest it protects. Although the estimated financial cost to regulated entities is between EUR 45 million and EUR 90 million, this cost is primarily linked to investments aimed at strengthening the resilience of infrastructure and ensuring the continuity of essential services. In addition, the new administrative burdens are quantified at approximately EUR 19 276, a low figure compared to the volume of activity and the economic size of the operators concerned. Furthermore, the regulation does not entail any budgetary costs for public authorities, nor does it have any significant impact on competition.

For all these reasons, it can be concluded that the measure does not impose excessive burdens on the parties subject to it, but rather establishes obligations that are proportionate, reasonable and necessary to ensure a high level of security and resilience of electronic communications networks and services.

10. References to the basic texts:

11. No

12.

13. Yes

Strategic Interests of the Country

Electronic communications networks and services are essential infrastructure for national security, public services, emergency services, economic activity and territorial cohesion.

14. No

15. Yes

16.

TBT aspects: No

SPS aspects: No

European Commission

Contact point Directive (EU) 2015/1535

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