



DRAFT ROYAL DECREE ON THE SECURITY AND RESILIENCE OF ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES AND CERTAIN DIGITAL INFRASTRUCTURES

I

The COVID-19 pandemic has powerfully highlighted the essential role played by electronic communications networks and services. Millions of people relied on them to continue working, access healthcare services and maintain their social relationships, among many other activities, in a context of lockdowns and restrictions.

In increasingly technology-driven societies and economies that are becoming ever more dependent on the growing and intensive use of electronic communications networks and services, this dependence has also highlighted a number of critical vulnerabilities relating to the security and integrity of electronic communications networks and services and digital infrastructures. This has created an urgent need to strengthen electronic communications networks and services, as well as certain digital infrastructures, and to make them more secure and resilient in the face of potential future incidents, not only in terms of cybersecurity but also in the physical environment. Thus, in recent years there have been a series of incidents that have tested the security and resilience of electronic communications networks and services. Some have been caused by natural events, such as the volcanic eruption on the island of La Palma on 19 September 2021, or the Isolated Upper-Level Low-Pressure System (DANA), which hit the Iberian Peninsula and the Balearic Islands—most severely affecting the Mediterranean coast—last October 2024. Others have been non-natural in origin, such as the recent power cut suffered by Spain.

The digital transformation driven by the technological progress achieved in the digitisation and virtualisation of services through the Internet of Things (IoT), Artificial Intelligence (AI), Big Data and Cloud Computing has radically transformed traditional telecommunications networks and electronic communications services. Whilst this transformation offers significant opportunities in terms of efficiency, connectivity, and economic and social development, it also introduces significant risks and vulnerabilities affecting digital infrastructures, for which the regulatory framework must anticipate and be adequately prepared.

The integrity and security of electronic communications networks and services is laid down in Article 63 of Law 11/2022 of 28 June (hereinafter the General Telecommunications Act). This Article is supplemented by the regulations on the security of fifth generation electronic communications networks and services, set out in Royal Decree-Law 7/2022 of 29 March on the requirements to ensure the security of



fifth generation electronic communications networks and services, and Royal Decree 443/2024 of 30 April approving the National Security Framework for 5G Networks and Services.

At European level, the integrity and security of digital infrastructures – including electronic communications networks and services – have also been regulated by Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (hereinafter the NIS2 Directive), as well as by Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (hereinafter the CER Directive). These directives strengthen the obligations imposed on operators and organisations to prevent, detect, respond to and recover from certain security incidents that may compromise the availability and reliability of digital infrastructures and electronic communications networks and services.

The NIS2 Directive establishes new regulations to ensure a high common level of cybersecurity across the European Union. Consequently, in line with and in coordination with the forthcoming legislation on cybersecurity and critical infrastructures transposing the NIS2 and CER Directives, it is considered necessary to adopt a Royal Decree establishing specific security and resilience obligations for the electronic communications networks and services sector and certain digital infrastructures. These obligations are to be consistent with the legislation on cybersecurity and critical infrastructures, in accordance with Article 63 of the General Telecommunications Act.

To ensure that this Royal Decree is consistent and coherent with current European legislation and with the regulatory texts resulting from the transposition of the existing draft legislation relating to the NIS2 Directive and the CER Directive, the obligations laid down in those Directives shall, in any event, apply to cybersecurity incidents and to those incidents affecting the sector of networks, electronic communications services and digital infrastructures which are not provided for in this Royal Decree.

II

Article 63 of the General Telecommunications Act establishes the need to ensure the integrity and security of electronic communications networks and services. Paragraph 1 stipulates that operators of public electronic communications networks and publicly available electronic communications services must appropriately manage security risks that may affect their networks and services, in order to ensure an adequate level of security and to prevent or minimise the impact of security incidents on users. To this end, they must adopt the appropriate technical and organisational measures they deem necessary. For its



part, paragraph 2 also includes the obligation of operators to ensure the integrity of telecommunications networks in order to safeguard the continuity of electronic communications services.

In line with the above, Chapter I of this Royal Decree defines its purpose and identifies the entities subject to the obligations laid down therein. Chapter II, in turn, sets out the various plans that obliged entities must draw up—general plans by operator and specific plans by service and type of incident—in order to ensure the security and resilience of electronic communications networks, electronic communications services and certain digital infrastructures.

Article 63(3) of the General Telecommunications Act requires operators providing public communications networks or publicly available electronic communications services to notify the current Ministry for Digital Transformation and the Civil Service of any security incidents that have had a significant impact on the provision of those networks or services. In this regard, Articles 20 to 23 of Order IET/1090/2014 of 16 June, regulating the conditions relating to service quality in the provision of electronic communications services (hereinafter the "Quality Order"), already lay down the criteria for determining what should be classified as a significant incident, whilst also establishing the notification obligations applicable to such incidents and the relevant time limits. However, technological developments, climate change and certain events that have occurred in recent years show us that in this respect the Quality Order has become outdated. It is now therefore appropriate to update the categories of incidents that must be taken into account in order to ensure the effective identification of risks and the planning of appropriate response measures to these events, which test the integrity and security of electronic communications networks and services.

The Quality Order also sets out the notification time limits and procedures for each type of incident. For the same reason mentioned above, it is considered that these time limits and procedures should be updated and adapted to the circumstances. Thus, on the one hand, the availability and handling—by both operators and the competent public bodies—of reliable and as up-to-date information as possible; and, on the other hand, an appropriate response to the management of the consequences arising from each incident, enabling the rapid restoration of the functionality of electronic communications networks, the continuity of service provision and the operational readiness of digital infrastructure, are not separate issues, but are clearly intertwined. They must therefore be addressed through a clear strengthening of time limits and the handling of structured and more detailed information whenever an incident occurs that affects network security or the normal functioning of electronic communications services, in order to facilitate the rapid recovery of networks and services. Accordingly, Chapter III of this Royal Decree sets out the new time limits and notification procedures for each type of security incident affecting electronic



communications networks and services, as well as certain digital infrastructures.

Similarly, paragraph 3 of the aforementioned Article 63 provides for the establishment of a mechanism for cooperation and information-sharing between the Ministry for Digital Transformation and the Civil Service and the competent national authorities of other Member States, as well as with the European Union Agency for Cybersecurity (ENISA). It also provides that the Ministry may inform the public or require operators to do so, if it considers that disclosure of the security incident is in the public interest. In accordance with this legal provision, Articles 24, 25 and 26 of this Royal Decree regulate the mechanisms for cooperation between the Ministry for Digital Transformation and the Civil Service and the competent national and European authorities in the field of security.

With a view to strengthening cooperation and coordination amongst all stakeholders and promoting the essential public-private cooperation in the planning, risk identification and joint management of incidents affecting an area of common interest, namely the security and resilience of electronic communications networks and services, the Second Additional Provision establishes a coordination board involving a wide range of stakeholders, to serve as a forum for dialogue, for sharing experiences and needs, and for establishing protocols and best practices in the event of future incidents such as those that have occurred in recent years, affecting the security of electronic communications networks and services and certain digital infrastructures.

Article 63(4) provides for a mechanism for informing users in the event of a security incident affecting the electronic communications services provided. This section has been set out in detail in Article 15 of this Royal Decree, which, in addition to the notification obligation, requires information to be provided on the estimated time for repair and the measures taken to mitigate this incident.

Article 63(5) sets out the inspection procedure and sanctioning regime, as well as the possibility to adopt additional measures to those identified in relation to the integrity and security of electronic communications networks and services. This section is set out in Chapter VII of this Royal Decree, as well as in Article 13, which empowers the Secretary of State for Telecommunications and Digital Infrastructures to impose new obligations and to issue recommendations, guidance or operational advice to obliged entities on the implementation of possible mitigating measures in relation to the contingency measures adopted during notified incidents or to reduce the risk of such incidents recurring.

For its part, the obligation set out in the General Telecommunications Act to provide the information necessary to assess the security and integrity of their services and networks—including documents on security policies—and the obligation to undergo a security audit carried



out by an independent body, at the obliged entity's own expense, and to make the results available to the Ministry for Digital Transformation and the Civil Service, are provided for in Article 23 of this Royal Decree.

Chapter IV sets out the obligations of centres receiving emergency calls and public warnings, and of the subjects bound by this Royal Decree, to ensure the highest possible availability of emergency services in the event of a catastrophic network failure or force majeure, and the obligation to take the necessary measures to ensure uninterrupted access to emergency services and the uninterrupted transmission of public warnings, in line with Article 63(6).

Chapter V of this Royal Decree regulates and implements the measures adopted in Article 4(6) of the General Telecommunications Act in relation to the assumption by the General State Administration of the direct management of certain publicly available electronic communications services, in order to ensure public security and national security or the fulfilment of public service obligations in accordance with Article 63(7).

Article 63(8),, concerning the protection of personal data and the safeguarding of digital rights, and its implementing regulations, are set out in Articles 27 and 28 of this Royal Decree.

III

This Royal Decree has been drafted and processed according to the principles for good regulation set out in Article 129 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations.

In particular, with regard to the principle of necessity, this regulation addresses the need to adopt certain measures that enhance the security and integrity of telecommunications networks, electronic communications services and certain digital infrastructures, in accordance with Article 63 of the General Telecommunications Act, in a manner that is consistent and coordinated with the national and European cybersecurity legislation. In this regard, it is considered necessary to establish an updated legal framework requiring obliged entities to have a security plan in place for each operator, service and type of incident, setting out the measures adopted for the prevention, detection and response to security incidents and risks in the event of an incident such as those that have occurred in recent years, whether natural or otherwise, with a view to restoring services as soon as possible. To this end, it is also considered necessary to set out in detail a clear and structured procedure for the notifications that obliged entities must submit to the Secretary of State for Telecommunications and



Digital Infrastructures when a significant incident occurs that affects the integrity of networks, certain digital infrastructures and the continuity of telecommunications services, in particular the emergency communications service via the 112 emergency number and public warning systems. This is so that both emergency services and policy-makers have, from the very outset, clear, reliable and as accurate information as possible on developments regarding the integrity of telecommunications networks, the provision of electronic communications services and certain digital infrastructures, so that they can take whatever decisions may be required as quickly as possible. It is also necessary to establish an enforcement and coordination procedure, as well as an inspection and penalty regime in the event of non-compliance with the obligations laid down in this Royal Decree.

With regard to the principle of proportionality, the conditions laid down in this regulation are proportionate to the objective pursued, namely ensuring the security and integrity of networks, electronic communications services and certain digital infrastructures. Obtaining information on significant incidents affecting the provision of electronic communications services is necessary to enable both the emergency services and policy-makers to take the decisions required, in the most effective manner possible to, among other things, save lives and prioritise the management of resources and public services in particularly critical situations.

The measures adopted in this Royal Decree comply with the principle of legal certainty, as they are aligned with and consistent with Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (CER Directive), and Article 63 of the General Telecommunications Act concerning the security and integrity of electronic communications networks and services.

With regard to the principle of transparency, the reasons justifying this regulation have been explained, and the public consultation and hearing procedures provided for in Article 133 of Law 39/2015 of 1 October have been carried out.

The procedure for the provision of information on technical regulatory standards and regulations relating to information society services, provided for in Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and rules on information society services, as well as Royal Decree 1337/1999 of 31 July regulating the provision of information in the field of technical standards and regulations and regulations relating to information society services, has also been followed.



Finally, the principle of efficiency is upheld, as this regulation sets out, in an up-to-date and structured manner, the content and time limits applicable to the notifications that telecommunications operators are already required to submit to the Secretary of State for Telecommunications and Digital Infrastructure when significant incidents occur that seriously affect the integrity of networks and the continuity of services provided via digital infrastructures.

IV

The draft has been notified by the National Commission on Markets and Competition, in accordance with Article 5(2)(a) of Law 3/2013 of 4 June 2013 establishing the National Commission on Markets and Competition.

This Royal Decree is issued by virtue of the exclusive competence of the State regarding telecommunications, as recognised in Article 149(1)(21) of the Spanish Constitution.

By virtue thereof, on the proposal of the Minister for Digital Transformation and the Civil Service, in agreement with the Council of State and after deliberation by the Council of Ministers at its meeting on xxx,

THE FOLLOWING IS DECREED:

CHAPTER I

General provisions

Article 1. Purpose

1. The purpose of this Royal Decree is to regulate the conditions and measures aimed at ensuring the security and resilience of electronic communications networks and services, their associated resources and certain digital infrastructures, in accordance with the provisions of Article 63 of Law 11/2022 of 28 June, the General Telecommunications Act, and Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems, or any legislation replacing them, particularly in the event of situations and incidents affecting network security, resulting in service interruptions or a significant degradation in service provision.



2. Furthermore, the purpose of this Royal Decree is to regulate the circumstances and requirements under which operators providing public communications networks or publicly available electronic communications services, together with the owners or operators of their associated facilities and certain digital infrastructures, must notify the Ministry for Digital Transformation and the Civil Service of any security incidents that have had a significant impact on the provision of those networks or services.

3. Network or service security is defined, in accordance with Definition 67 of Annex II to Law 11/2022 of 28 June, the General Telecommunications Law, as the ability of electronic communications networks and services to withstand, with a certain level of confidence, any action that compromises the availability, authenticity, integrity and confidentiality of such networks and services, of the data stored, processed or transmitted, and the security of the related services offered or accessible through such electronic communications networks and services.

4. Resilience of networks or services means the capacity of electronic communications networks and services to prevent, protect against, respond to, withstand, mitigate, absorb, adapt to and recover from an incident.

Article 2. Scope of application

1. This Royal Decree shall apply to owners and operators of public electronic communications networks located in Spain, to providers of publicly available electronic communications services provided in Spain, and to the owner or operator of any associated resource used to support the operation of public networks or the provision of any publicly available electronic communications service located or provided in Spain, including passive infrastructure used to host mobile communications access networks.

2. This Royal Decree also applies to the owners or operators of digital infrastructures located in Spain, including, among others, submarine cable infrastructure, satellite systems, content delivery networks (CDNs), data centres (DCs) or internet exchange points (IXPs), and any resources associated with such infrastructures, where they contribute to the operation of public electronic communications networks or the provision of publicly available electronic communications services.

For these purposes, owners and operators of public electronic communications networks and providers of publicly available electronic communications services shall identify the digital infrastructures that contribute to the operation of their own networks or the provision of their electronic communications services and shall communicate that



information to the Secretary of State for Telecommunications and Digital Infrastructure by 31 January of each calendar year.

Once owners and operators of public electronic communications networks and providers of publicly available electronic communications services have identified and notified the Secretary of State for Telecommunications and Digital Infrastructure of the digital infrastructures that contributes to the operation of their own networks or the provision of their electronic communications services, they must also notify the owners and operators of those digital infrastructures of this fact and, consequently, of the applicability of this Royal Decree.

3. For the purposes of this Royal Decree, the following are considered to be obliged parties: the owners and operators of the networks, electronic communications services, associated resources and digital infrastructures referred to in the preceding paragraphs where they fall within any of the following categories:

- a) Electronic communications operators whose total number of users in Spain, calculated across the same corporate group, in accordance with Article 42 of the Commercial Code, is 500,000 or more.
- b) Electronic communications operators whose annual turnover from the provision of public electronic communications networks or publicly available electronic communications services in Spain exceeds EUR 50 million, calculated across the same corporate group, in accordance with Article 42 of the Commercial Code. This figure may be updated or amended by order approved by the head of the Ministry for Digital Transformation and the Civil Service in the light of technical, economic and competitive developments in the market.
- c) Electronic communications operators on whom specific obligations have been imposed as operators with significant market power in a relevant market pursuant to the provisions of Article 18 of Law 11/2022 of 28 June.
- d) Electronic communications operators designated for the provision of universal telecommunications service or for the provision of public service obligations under the provisions of Articles 40 and 43, respectively, of Law 11/2022 of 28 June.
- e) Electronic communications operators that have been designated as critical operators or are the owners or operators of any critical infrastructure designated under the provisions of the legislation on the protection and resilience of critical entities.
- f) Electronic communications operators that provide the connectivity services to centres receiving emergency calls via the 112 emergency number and public warnings.
- g) Owners and operators of electronic communications networks providing wholesale services, digital infrastructures and associated facilities, including passive infrastructures used to host mobile communications access networks, which contribute to the



operation of the networks or the provision of electronic communications services provided by any of the obliged entities referred to in the preceding categories.

Given the dynamic nature of the electronic communications and digital infrastructure sector, the continuous process of technological innovation characteristic of those fields, and the continuous and successive regulatory, economic, commercial and competitive changes faced by market participants, the aforementioned provisions, criteria and requirements may be amended by an Order approved by the Minister for Digital Transformation and the Civil Service.

4. This Royal Decree applies to centres receiving emergency calls via the 112 emergency number and public warnings, in accordance with the provisions of Chapter IV.

5. This Royal Decree does not apply to the owners and operators of electronic communications networks, providers of electronic communications services and digital infrastructures linked to National Security and Defence.

6. The provisions of this Royal Decree shall be applied in a manner consistent with and in coordination with the National Security System, in accordance with Law 36/2015 of 28 September on National Security.

In particular, in the event of a security incident in the networks, electronic communications services and digital infrastructure that may give rise to a situation of interest to National Security, the instruments provided for under Law 36/2015 of 28 September on National Security may be activated.

7. The provisions of this Royal Decree shall be without prejudice to the application of the regulations on the security of fifth generation electronic communications networks and services, enshrined in Royal Decree-Law 7/2022 of 29 March on the requirements to ensure the security of fifth generation electronic communications networks and services and Royal Decree 443/2024 of 30 April approving the National Security Framework for 5G Networks and Services.

8. Similarly, the provisions of this Royal Decree shall be without prejudice to the application of the national or European legislation relating to the coordination and governance of cybersecurity in respect of specific cybersecurity incidents.

9. The provisions of this Royal Decree shall also be without prejudice to the application of national or European legislation relating to the protection and resilience of critical entities.



Article 3. Electronic communications networks and services, their associated resources and certain digital infrastructures as essential facilities and services in emergency situations.

1. All public electronic communications networks, publicly available electronic communications services, their associated resources, and the digital infrastructures that contribute to the operation of such networks or the provision of the aforementioned services, whether or not they are owned or operated by the entities subject to this Royal Decree, are classified as essential facilities and services in emergency situations arising from security incidents that affect network security, service interruptions or a significant degradation in the conditions under which the services are provided.

2. In such emergency situations, all public authorities, administrative bodies and the State Security Forces and Corps shall cooperate and contribute to facilitating the swiftest and most comprehensive possible restoration of the network's integrity and security, the resumption of service or the operational readiness of the infrastructure, or to facilitating its maintenance, in coordination with civil emergency planning and the protection planning for critical entities and infrastructures.

3. To this end, those authorities and bodies shall, within the scope of their respective powers, take the administrative, technical and operational measures necessary to ensure that such recovery and restoration take place as soon as possible, or that they are maintained as required.

Among other measures, safe-conduct passes and access permits will be issued to allow staff of operators, owners or managers of associated resources and digital infrastructures, and of companies contracted by them, to access the facilities and infrastructures for the purposes of repair, reconstruction or maintenance.

Similarly, these authorities and bodies shall prioritise and treat as a matter of urgency the processing of any procedure whose ultimate aim is to restore the integrity and security of the network, re-establish the service or the operational capability of the infrastructure, or facilitate its maintenance. Among other measures, provisional and temporary licences and permits—whether relating to town planning, land-use planning, environmental matters or any other area—may be granted, or may be replaced by responsible declarations, with a view to enabling operators and owners or managers of associated resources and digital infrastructures to restore the safety and operational capability of their facilities and infrastructures.

4. The State Security Forces and Corps shall provide whatever assistance and support that is necessary to enable the staff and



representatives of operators and owners or managers of associated resources and digital infrastructures, as well as the companies contracted by them, to carry out their activities and operations aimed at restoring the security and operational capability of the facilities and infrastructures or facilitating their maintenance.

5. In the specific case of a power cut, those facilities or infrastructures deemed by the operator to be essential at the first and intermediate levels, as set out in Article 7(4), shall be given priority in the restoration of the electricity supply.

6. Furthermore, in cases where the repair, reconstruction or maintenance of the facilities and infrastructures of electronic communications networks and services, associated resources and digital infrastructures requires the supply of fuel, priority shall be given to the supply of such fuel to the aforementioned facilities and infrastructures.

CHAPTER II

Planning to ensure the security and resilience of electronic communications networks and services, their associated resources and certain digital infrastructures

Article 4. National Plan for the security and resilience of electronic communications networks and services.

1. In order to ensure the security and resilience of electronic communications networks and services, their associated resources and certain digital infrastructures in Spain, the Ministry for Digital Transformation and the Civil Service shall approve, by means of a Ministerial Order, a National Security and Resilience Plan for Electronic Communications Networks and Services.

2. This National Security and Resilience Plan shall develop and coordinate a response and recovery plan for security incidents, setting out the objectives and measures applicable to the management of each category of security incident.

The Plan shall, in any event, include:

- a) The objectives of the measures and obligations set out in the National Plan for the Security and Resilience of Electronic Communications Networks and Services.
- b) The functions and responsibilities assigned to the various authorities with jurisdiction over security incidents affecting electronic communications networks and services, their



associated resources and certain digital infrastructures, taking into account, amongst other factors, whether they relate to critical infrastructures or cybersecurity incidents, in coordination with civil emergency planning and with the planning for the protection of critical entities and infrastructures.

- c) The procedures for managing crises caused by security incidents affecting electronic communications networks or services, and channels for the exchange of information both between the obliged entities and the public administration, and between public administrations.
- d) Anticipation and preparedness measures, which should include, amongst other things, training activities.
- e) The obliged entities, as well as the infrastructure involved.
- f) The procedures and mechanisms to ensure the participation and support of Spain in the coordinated management of large-scale security incidents affecting electronic communications networks and services at European Union level.
- g) The mechanisms for coordinating the Autonomous Communities' involvement in monitoring and updating the Plan.
- h) The territorial uniqueness of the Autonomous Communities of the Balearic Islands and the Canary Islands, and the Autonomous Cities of Ceuta and Melilla, in terms of issues related to submarine cables and satellite systems connecting their territories.

3. The National Security and Resilience Plan for Electronic Communications Networks and Services shall include procedures and mechanisms for crisis management, including the phases of prevention, detection, response, return to normality and evaluation, ensuring its integration and consistency with the plans and strategies of the National Security System.

4. The National Security and Resilience Plan shall be drawn up within one year of the entry into force of this Royal Decree and shall be updated every 2 years, with a view to adapting to new needs in the light of technological developments.

Article 5. Obligation to manage security risks appropriately.

1. In order to ensure the security and resilience of networks, electronic communications services and certain digital infrastructures, the obliged entities shall appropriately manage the security risks that may affect their networks or the electronic communications services they provide, their associated resources and certain digital infrastructures, with a view to preventing or minimising the impact of security incidents, both on users and on other networks, services and digital infrastructures, and shall, to this end, adopt appropriate technical and organisational measures.



2. Furthermore, operators shall ensure the greatest possible availability of publicly available electronic communications services and, in particular, of voice communications and internet access services provided over public electronic communications networks in the event of a catastrophic network failure or in cases of force majeure, and shall take all necessary measures to ensure uninterrupted access to emergency communications services and the uninterrupted transmission of public warnings.

Article 6. General Action Plan of each obliged entity to ensure the security and resilience of electronic communications networks and services.

1. In order to fulfil their obligation to prevent, detect and manage security risks appropriately, each of the obliged parties must draw up a General Action Plan.

2. This General Action Plan should include a risk analysis on the security of its network or the provision of electronic communications services, their associated resources or digital infrastructure, identifying whether they are essential networks or infrastructures, and identifying, in addition to the prevention and detection measures, the mechanisms and priorities in the measures to be adopted for the management and recovery of services in the event of a service interruption or significant degradation in the conditions under which the services are provided.

3. This Plan will also identify the buildings and facilities deemed essential and in respect of which specific and priority measures will be taken to ensure the security of the networks and the continuity of services.

Equally, the criteria taken into account to identify buildings and facilities as essential, as well as the specific and priority measures that have been taken in each building or facility to ensure the security of networks and the continuity of services, shall be detailed.

4. Every operator of public electronic communications networks and of publicly available electronic communications services that is classified as an obliged entity pursuant to the provisions of this Royal Decree must submit the General Action Plan to the Secretary of State for Telecommunications and Digital Infrastructures within a maximum period of six months from the entry into force of this Royal Decree, and it must be updated every two years.

Any owner or manager of an associated resource or digital infrastructure who is classified as an obliged entity pursuant to the provisions of this Royal Decree must submit the General Action Plan when required to do



so by the Secretary of State for Telecommunications and Digital Infrastructures, within the time limit specified in the request itself.

Article 7. Specific Plan for each obliged party for each network, service, associated resource or digital infrastructure used to ensure its security.

1. In addition to drawing up a General Action Plan, obliged entities are required to submit a Specific Plan for each of the networks, services, associated resources and digital infrastructures that they own or manage.

This specific plan must be submitted for each of the following types of digital networks, services and infrastructures:

- a) Fixed electronic communications networks and services,
- b) Mobile communications networks and services, including the passive infrastructures used to host mobile communications access networks.
- c) Digital messaging services,
- d) Networks supporting nationwide terrestrial broadcasting services for audiovisual communication, which are subject to coverage obligations.
- e) Submarine cables,
- f) Satellite systems,
- g) Certain digital infrastructures that contribute to the operation of public electronic communications networks and the provision of the electronic communications service, as previously identified by electronic communications operators, in accordance with Article 2(2) of this Royal Decree, such as Content Delivery Networks (CDN), Data Processing Centres (DPCs) and Internet Exchange Points (IXPs).

Given the dynamic nature of the electronic communications and digital infrastructure sectors, the constant process of technological innovation characteristic of these fields, and the continuous and successive regulatory, economic, commercial and competitive changes faced by market participants, the above provisions and classifications may be amended by an Order approved by the Minister for Digital Transformation and the Civil Service.

2. Furthermore, obliged entities are required to submit a Specific Plan for each type of incident, as determined by an Order approved by the Minister for Digital Transformation and the Civil Service. The following types of incidents are initially identified: serious disruption to the external network infrastructure; interruption of the electricity supply, a meteorological event causing serious impact on the network, service or



infrastructure, volcanic eruption, earthquake, flooding, fire, serious IT failure and major cyberattack.

3. In both specific plans, the obliged parties shall describe the priorities and measures for prevention, detection, as well as the measures to be adopted for the recovery of services in the event of interruption or significant degradation in the conditions under which those services are provided.

Specific plans may provide that, as measures aimed at properly managing the incident, the obliged party may take decisions to ensure the maintenance of the most basic and essential electronic communications services, enable communication to be maintained as widely as possible for different citizens and territories, and avoid traffic congestion. To this end, the plan may provide for, and the obliged party may, if necessary, implement measures such as prioritising certain types of traffic—such as that linked to emergency services, official communications or communications to official accounts—prioritising traffic consisting of voice calls and SMS messages over data transmission traffic, or temporarily suspending the use or operation of certain technologies or services that demand higher energy consumption or greater data transmission capacity. Under no circumstances may the obliged party discriminate against or disadvantage the traffic of any operator or agent within the same service or technology.

4. These specific plans will include estimates of the percentage of traffic and service availability for which, in the event of natural disasters or potential energy emergencies, the network infrastructure is capable of ensuring the continuity, operability and functioning of the service.

In particular, in the event of a power cut, the obliged party, under these specific plans, must identify, within the network, service, associated resource or digital infrastructure, those facilities or infrastructure elements that are considered essential due to their importance and impact on maintaining the service's operability and functioning. These essential first-level installations or infrastructures must guarantee their operability an interruption of the electricity supply for at least 24 hours; essential intermediate-level installations or infrastructures for at least 12 hours; and all other installations and infrastructures must guarantee their operability for at least 4 hours.

In the specific case of the access network of a mobile communications network through which publicly available electronic communications services are provided in harmonised European bands, this access network must be designed and equipped with its own generating equipment and electrical supply elements to ensure its operability and continuity of service as the ultimate objective for at least 4 hours for at least 75% of the population in Spain.



This ultimate objective must be achieved within three years of the entry into force of this Royal Decree and maintained thereafter. In order to achieve this ultimate objective, the access network must be designed and equipped with the appropriate power supply equipment to ensure operability and continuity of service for at least 4 hours for a minimum of 50% of the population in Spain before the end of the first year of this Royal Decree's entry into force, and for at least 4 hours for a minimum of 65% of the population in Spain before the end of the second year of this Royal Decree's entry into force.

In the design, planning and implementation of this strategy to maintain the operability of infrastructures and facilities and to ensure the continuity of service provision, the operator may use all base stations—whether fixed or portable—frequency bands, and technologies it deems appropriate. Furthermore it may prioritise all those locations, centres and facilities it considers appropriate based on their connection to the provision of public services and services of economic and social importance.

In implementing this strategy to maintain the operational readiness of infrastructures and facilities and to ensure the continuity of service provision, the various authorities and bodies, within the scope of their respective powers, may adopt the administrative, technical and operational measures necessary to facilitate the implementation of this strategy, such as prioritising and declaring the urgent need for the granting of licences and permits—whether relating to town planning, land-use planning, the environment or any other area—or allowing these to be replaced by responsible declarations.

Installations or infrastructures that are considered by the operator to be essential—at both the primary and intermediate levels—in the event of interruption to the electricity supply must be communicated to the transmission company and the electricity distribution companies so that they can be included in their electrical contingency plans.

Furthermore, the installations or infrastructures necessary to maintain the operability and functioning of submarine cables and satellite systems connecting any island of the Autonomous Communities of the Balearic Islands and the Canary Islands, or the Autonomous Cities of Ceuta and Melilla must also be communicated to the transmission company and the electricity distribution companies so that they can be included in their electricity contingency plans.

5. In the specific plans and in the design of mitigation and incident management measures for the possible consequences and damage that may be caused, the obliged party must incorporate the most advanced and innovative mechanisms and techniques in the detection and



prevention of risks and in the management of incidents that occur, in particular, those techniques linked to the use of artificial intelligence services that contribute to the planning, design and management of risks that make it possible to have and provide electronic communications networks and services, associated resources and safer and more resilient digital infrastructures.

6. Every operator of public electronic communications networks and of publicly available electronic communications services that is classified as an obliged entity pursuant to the provisions of this Royal Decree must submit these specific plans to the Secretary of State for Telecommunications and Digital Infrastructure within a maximum period of six months from the entry into force of this Royal Decree, and it must be updated every two years.

Any owner or manager of an associated resource or digital infrastructure who is classified as an obliged entity pursuant to the provisions of this Royal Decree must submit these specific plans when required to do so by the Secretary of State for Telecommunications and Digital Infrastructures, within the time limit specified in the request itself.

Article 8. Analysis and instructions of the plans of the obliged parties.

1. The Secretary of State for Telecommunications and Digital Infrastructure will examine the General Action Plan and the Specific Plans submitted by each obliged entity.

2. In the light of this analysis, the Secretary of State for Telecommunications and Digital Infrastructure may issue instructions and guidelines to amend both the General Action Plan and any of the Specific Plans submitted by each obliged entity, with a view to ensuring the security of electronic communications networks and services and digital infrastructures.

When adopting these instructions and guidelines, the Secretary of State for Telecommunications and Digital Infrastructure must provide adequate grounds, justifying them on the basis of the need to ensure the security and resilience of electronic communications networks and services, their associated resources and the digital infrastructure that contributes to their operation, to complement the risk analysis or the application of mitigation techniques that are generally accepted by the electronic communications and digital infrastructure sector and other obliged entities, and to implement those measures that have been specified in the routine and ad hoc audits which obliged entities are required to submit to under this Royal Decree.



Furthermore, when approving these instructions and guidelines, the Secretary of State for Telecommunications and Digital Infrastructure must take into account the costs associated with the various measures and solutions that may be imposed, having regard to the financial situation of the obliged party and the configuration of the network, service or infrastructure.

The instructions and guidelines shall be approved by the Secretary of State for Telecommunications and Digital Infrastructure following a hearing with the obliged party. They shall constitute the final administrative decision and may be challenged directly before the administrative courts.

3. The Secretary of State for Telecommunications and Digital Infrastructure may draw up templates for a General Action Plan and Specific Plans, to be followed and implemented by the obliged parties.

Article 9. National Civil Emergency Plan for electronic communications networks and services.

1. The Council of Ministers, on the proposal of the Ministry of the Interior and following a report from the Ministry for Digital Transformation and the Civil Service and the National Civil Protection Council, shall approve the National Civil Emergency Plan relating to electronic communications networks and services.

2. This Plan will analyse the various threats and exceptional circumstances that may affect community life and will set out a strategy for mobilising resources and assets relating to networks, electronic communications services and digital infrastructures, with a view to helping to overcome such exceptional circumstances and restore normal conditions as soon as possible.

The preparation of the Plan shall take into account the territorial uniqueness of the Autonomous Communities of the Balearic Islands and the Canary Islands, and the Autonomous Cities of Ceuta and Melilla, as regards the issues related to submarine cables and satellite systems connecting their territories.

3. Obligated entities are required to make available to the competent authorities the infrastructures, assets and resources that are necessary and required for this purpose in each situation arising from the implementation of this Plan.

4. This Plan must be updated every two years.



CHAPTER III

Notifications regarding security incidents affecting electronic communications networks and services, their associated resources and certain digital infrastructures

Article 10. Obligation to report security incidents that have had a significant impact on electronic communications networks and services, their associated resources and certain digital infrastructures.

1. Obligated entities are required to notify the Secretary of State for Telecommunications and Digital Infrastructure of any security incidents that have had a significant impact on the provision of networks or the provision of electronic communications services, or on the operability and functioning of associated resources and digital infrastructure.

2. In order to determine the significance of the impact of a security incident, the following parameters in particular shall be taken into account where available:

- a) The number of users affected by the security incident,
- b) The duration of the security incident,
- c) The geographical area affected by the security incident,
- d) The extent to which the operation of the network or service has been affected,
- e) The extent of the impact on economic and social activities.

3. In order to comply fully with this obligation to report significant security incidents, the entities subject to this requirement must ensure that all the necessary material and human resources are expressly and specifically made available to fulfil this obligation without undue delay, irrespective of the means and resources allocated to resolving the security incident and restoring normal operations.

Article 11. Definition of security incidents affecting networks or electronic communications services, their associated resources and certain digital infrastructures.

1. Security incidents are defined as incidents suffered by any obliged entity which affect electronic communications networks and services, their associated resources and digital infrastructures, and which result in an interruption to the electronic communications service or a significant degradation to the conditions of service provision, as defined below.

2. Incidents considered to be of minor significance.



These are incidents that result in a total interruption or a degradation in the operability or functioning of public electronic communications networks and the services provided through them, either directly or via any of the associated electronic communications networks, associated resources and identified digital infrastructure, affecting fewer than 25,000 lines for at least 1 hour, or the service supporting the nationwide terrestrial audiovisual broadcasting service for which coverage obligations are met, affecting fewer than 25,000 users for at least 1 hour.

These incidents are not subject to the notification referred to in Article 12, although they must be reported at the request of the Secretary of State for Telecommunications and Digital Infrastructure or when the platform or telematic service referred to in paragraph 2 of the fifth additional provision is set up.

3. Incidents considered significant.

These are incidents that result in a total disruption or a degradation of the operability or functioning of public electronic communications networks and the services provided through them, either directly or via any of the identified electronic communications networks, associated resources and digital infrastructures, which ultimately result in any of the following consequences:

- a) The incident affects 25,000 or more lines for more than one hour.
- b) The incident affects the support service for the nationwide terrestrial audiovisual broadcasting service, which is required to fulfil coverage obligations for 25,000 users or more for at least one hour. The number of users concerned shall refer to the users of the service areas of the transmission centres concerned.
- c) The incident affects several operators at the same time as a result of natural disasters or possible power supply interruptions affecting electronic communications services or services provided through digital infrastructures.
- d) The incident involves the interruption of the emergency communications service via the 112 emergency number or the public warning service, regardless of the number of lines affected.
- e) The incident affects more than 10% of the lines within the territory of any province, any island in the Autonomous Communities of the Balearic Islands and the Canary Islands, or in either of the Autonomous Cities of Ceuta and Melilla, for more than two hours.
- f) The incident involves a significant disruption or degradation of the service provided via an electronic communications network, associated resource or digital infrastructure, without



there being any immediate direct impact on lines or users of electronic communications services, or where it is not possible to determine such an impact, particularly in situations where there is a significant loss or degradation in the availability or operability of networks, infrastructure or alternative or redundant services, which undermines the security and resilience of the network or service in the face of future incidents.

- g) Any other incident that results in a significant disruption or degradation of the service provided and which, by affecting the normal conduct of certain economic or social activities or the provision of public services, or by having a significant social impact, is deemed as such by the Secretary of State for Telecommunications and Digital Infrastructure.

4. The incident begins as soon as the service begins to be interrupted or degraded. It ends the moment that all services have been re-established under normal operating conditions available for use.

5. The head of the Secretary of State for Telecommunications and Digital Infrastructure shall, by means of a resolution, determine:

- a) The procedure for calculating the number of lines or services affected,
- b) The definition of the threshold for disruption to service quality, above which the relevant notifications must be made, where there is no total interruption to the service,
- c) The determination of the conditions under which the interruption or significant degradation of the service provided must be notified, where there is no direct impact on lines or users of electronic communications services, or it is not possible to determine it.

6. Obligated entities shall be required to notify the Secretary of State for Telecommunications and Digital Infrastructure, in accordance with the procedure set out in Article 12, of any significant security incidents as referred to in paragraph 3.

Article 12. Notification.

1. Obligated entities facing a significant security incident shall, without undue delay, submit the following notifications to the Secretary of State for Telecommunications and Digital Infrastructure:

- a) Initial report

An initial notification must be submitted in all cases where the operator experiences a significant security incident as referred to in Article 11(3).



This notification must be sent by email to the Secretary of State for Telecommunications and Digital Infrastructure within a maximum of one hour of the obliged entity becoming aware of the incident. Should it not be possible to send the notification by email, the obliged entity must contact the Secretary of State for Telecommunications and Digital Infrastructure by whatever means are available, and the method for transmitting the notification and the information will be agreed upon.

The Secretary of State for Telecommunications and Digital Infrastructure shall have full and confidential access to all information relating to the security incident, provided that it relates to its respective responsibilities and powers.

The initial notification shall include at least the following:

- i) Information on the exact time of the start of the incident,
- ii) A brief description of the cause of the incident and, in particular, whether it is currently considered to be a cybersecurity incident, or any other type of incident, or a hybrid incident,
- iii) The affected services and, in particular, whether the incident affects the emergency communications service or the public warning service,
- iv) Contact person and contact details,
- v) Any other information that the liable party considers relevant.

b) Intermediate notifications

If, two hours after the initial notification by the obliged party, the reported incident has not been fully resolved, the obliged party must send, by email, within two hours of becoming aware of the incident and subsequently every 3 hours during the first 24 hours from the start of the incident, to the Secretary of State for Telecommunications and Digital Infrastructure, all necessary interim notifications to update the information contained in the initial notification and provide any additional information requested by the Secretary of State for Telecommunications and Digital Infrastructure.

In the intermediate notifications to be made to the Secretary of State for Telecommunications and Digital Infrastructure, the information reported in the initial notification shall be provided in more detail. A detailed description shall be provided of the incident and the digital infrastructures affected, the impact of the fault, whether the emergency communications service or public warning service has been restored, whether other operators are affected, an updated number of affected lines or users by service, a preliminary analysis of the cause of the fault, including whether the cause is internal or external and details thereof, whether it is due to system failure, network congestion, human error, malicious acts, natural phenomena, or third-party failures such as power



supply issues, cable theft or damage, earthquakes or floods, as well as any additional information that the operator may be able to report.

If the incident affects more than one obliged entity, the Secretary of State for Telecommunications and Digital Infrastructure shall specify, within the first 24 hours, the exact times for the submission of interim notifications.

In the first 24 hours of the start of the incident, interim notifications shall be sent at 9: 00, at 16:00 and at 21:00, by e-mail, until the final notification is made.

Without prejudice to the foregoing, the Secretary of State for Telecommunications and Digital Infrastructure may amend the periods of time and the times identified in the previous paragraph according to the impact and severity of the security incident that has occurred.

c) Final report

The operator shall notify the Secretary of State for Telecommunications and Digital Infrastructure of the termination of the incident, by email, as soon as it becomes aware of the restoration of the affected service.

Without prejudice to the foregoing, within a maximum of 24 hours of the operator notifying the resolution of the incident, it must send a final notification stating, in addition to the exact time of the incident's resolution, an update that is as detailed as possible regarding the latest information reported in the initial notification or in the interim notification, if one was issued.

d) Detailed Report

The detailed report shall be sent by email to the Secretary of State for Digital Infrastructure no later than 10 days after the notification by the operator of the completion of any of the significant incidents.

The detailed report must contain at least the following information:

- a) Detailed description of the incident:
 - i. Start and end times of the incident, Total duration of the incident,
 - ii. Type of incident and digital infrastructure affected (e.g. network failure, service disruption, server outage, data centres, etc.),
 - iii. Geographic area affected,
 - iv. Services affected (voice services, data services, fixed-line or mobile services, broadcasting services, satellite services, etc.).



b) Impact of incident:

- i. Access to the emergency response service via the 112 emergency number,
- ii. Impact on the public warning service,
- iii. Impact on customer service,
- iv. Other operators affected,
- v. Number of lines or users, depending on the service affected,
- vi. Different types of impact (e.g. interruption of telephone service, loss of connectivity, etc.).

c) Causes of the incident:

- i. Detailed analysis of the cause of the incident.
- ii. Detailed description of possible internal or external causes: system failures, network congestion, human errors, malicious acts, natural phenomena, third-party failures such as power supply failures, arson, theft or cable damage, earthquakes or floods, etc.

d) Contingency measures adopted during the first two hours following the start of the incident:

- i. Description of the contingency measures taken to mitigate the incident.
- ii. Communication to interested parties: Secretary of State for Telecommunications and Digital Infrastructure, communications with end users, and other bodies such as the Military Emergency Unit (hereinafter 'UME') or civil protection.

e) Recovery plans:

- i. Description of the progress made in restoring each of the services affected as a result of the contingency measures taken to mitigate the fault.
- ii. Measures to prevent similar incidents in the future.

f) Communication and contact person:

- i. The channels used to report any interruption or degradation of the service provided via digital infrastructures to users, the government, the civil protection services and the UME.
- ii. Contact person: first name, surname, email address and mobile phone number.



- g) Liability: possible liability of the operator in connection with the incident.
- h) Supporting documentation.

2. Without prejudice to the information requested in the previous section, the Secretary of State for Telecommunications and Digital Infrastructure may draw up and send to the obliged parties a specific notification form during the process of initial, interim and final notifications, requesting specific and additional information tailored to the particular security incident and in accordance with the needs and severity of the impact on the service.

3. Operators shall provide the Secretary of State for Telecommunications and Digital Infrastructure, within three months of the entry into force of this Royal Decree, with the contact details of the person or persons responsible for these notifications, so that further information may be requested if necessary. The contact details shall be updated at least once a year.

4. Obligated entities subject to a significant security incident requiring the performance of works or actions on public roads must inform the owner or manager of the road, without undue delay, of the need for action on that road, in order to coordinate its execution under safe conditions and as soon as possible, in accordance with the provisions of Article 123 of Royal Decree 899/2025 of 9 October approving the General Roads Regulation.

Article 13. Mitigation measures.

The Secretary of State for Telecommunications and Digital Infrastructure may issue recommendations, guidance or operational advice to obliged entities on the implementation of possible mitigating measures in relation to the contingency measures adopted during reported incidents, or to reduce the risk of such incidents recurring. These recommendations may be made public.

Article 14. Collaboration with other affected Member States.

1. Where appropriate, and in particular where a security incident affecting the network or the provision of electronic communications services, associated resources or digital infrastructure is likely to affect another Member State, the Secretary of State for Telecommunications and Digital Infrastructure shall inform the other Member State without undue delay.



2. The information forwarded to the other Member State shall include the information received by the obliged entities, whilst safeguarding, in accordance with European Union and national law, the commercial interests of the obliged entities and the confidentiality of the information provided.

Article 15. Information to natural and legal persons receiving services affected by a security incident in the electronic communications network or services.

Obliged entities must ensure that natural and legal persons who are recipients of electronic communications services are adequately informed, through public communications—such as publication on their websites—or through customer service channels and services, about the impact on their services, as soon as such communication or information can be provided following an incident affecting the provision of electronic communications services, as well as about the measures or solutions adopted to resolve the incident promptly.

Article 16. Notifications to other competent authorities in the event of significant security incidents affecting critical infrastructure and in relation to cybersecurity.

1. Where an obliged entity is the owner of a critical infrastructure in Spain, in the event of a significant security incident affecting the network or the provision of electronic communications services, it must notify the Ministry of the Interior, via the Secretary of State for Security, and the National Centre for the Protection of Critical Infrastructure (CNPIC), in accordance with the provisions of Law 8/2011 of 28 April, which establishes measures for the protection of critical infrastructure, and its implementing regulations.

2. In the event of a cybersecurity incident affecting Spain, depending on the type of organisation and the nature of the incident, the obliged party shall be required to notify the competent authorities designated for each case in the current cybersecurity regulations.

Article 17. Voluntary notification of relevant information.

1. Without prejudice to the mandatory notifications set out in this Royal Decree, obliged entities may, on a voluntary basis and at any time, notify the Secretary of State for Telecommunications and Digital Infrastructure of any other type of security incident—even if it is not considered significant—that results in the interruption or degradation of electronic communications services.



2. Mandatory notifications shall take precedence over voluntary notifications for the purposes of their management by the competent bodies.

Article 18. Information from the Secretary of State for Telecommunications and Digital Infrastructure to obliged entities and to centres receiving emergency calls and public warnings.

1. The Secretary of State for Telecommunications and Digital Infrastructure, where it deems it appropriate in view of the number of obliged entities affected, the type of incident and its repercussions, and in order to facilitate the flow of information to be provided by the obliged entities and access by those entities to the information most relevant to them, or to achieve better coordination in the resolution of the incident and the more rapid and effective restoration of service and infrastructure operability, shall provide information on the incident, its extent of impact, and the mitigating and resilience measures that may be adopted or are being adopted by other parties or obliged entities, whilst safeguarding the confidentiality of information and trade secrets pertaining to each obliged entity.

2. In addition, the Secretary of State for Telecommunications and Digital Infrastructure shall provide information to centres receiving emergency calls via the 112 emergency number and public warnings when the incident affects the origination, routing or reception of this type of communication or warnings.

CHAPTER IV

Emergency communications via the 112 emergency number and public warnings

Article 19. Obligation of centres receiving emergency calls via the 112 emergency number and public warnings.

1. Centres receiving emergency calls via the 112 emergency number and public warnings are obliged to ensure security and adopt measures to enable the routing of emergency calls and public warnings. To this end, they shall adopt such technical measures as they deem appropriate, including specific plans, strategies, redundancies and service alternatives, either through the operator providing the emergency communications routing service or through one or more other service providers.



2. The measures adopted by the centres receiving emergency calls referred to in the previous paragraph shall be submitted to the Secretary of State for Telecommunications and Digital Infrastructure within a maximum period of six months from the entry into force of this Royal Decree.

3. These measures, adopted by the centres receiving emergency calls via the 112 emergency number and public warnings, as well as any specific plans or contingency and alternative arrangements, shall be updated and submitted to the Secretary of State for Telecommunications and Digital Infrastructure every two years.

4. In cases where the provision of emergency call-handling services via the 112 emergency number and public warnings is carried out through contracts with third parties, the centres receiving the calls must review and, where necessary, update the measures adopted whenever there are changes to the service providers as a result of public procurement procedures. Once updated, these measures must be submitted to the Secretary of State for Telecommunications and Digital Infrastructure.

Article 20. Obligation of the obliged parties to ensure the continuity of service to centres receiving emergency calls via the 112 emergency number and public warnings.

1. Obligated entities are required to submit to the Secretary of State for Telecommunications and Digital Infrastructure, within 6 months of the entry into force of this Royal Decree, a specific plan, prepared in coordination with the reception centres, which includes the measures adopted to ensure the continuity of service and the transmission of emergency communications to centres receiving emergency calls via the 112 emergency number and public warnings, including, where appropriate, various redundancy mechanisms or other alternative arrangements that may be established to guarantee the continuity of the service.

2. This specific plan will be updated and submitted to the Secretary of State for Telecommunications and Digital Infrastructure every two years.

3. The Secretary of State for Telecommunications and Digital Infrastructure will examine the Specific Plan for service continuity to centres receiving emergency calls via the 112 emergency number and public warnings, as submitted by each obliged entity.

In the light of this analysis, the Secretary of State for Telecommunications and Digital Infrastructure may issue instructions and guidelines to bring about amendments to the Plan.



When adopting these instructions and guidelines, the Secretary of State for Telecommunications and Digital Infrastructure must provide adequate grounds, justifying them on the basis of the need to ensure the security and resilience of electronic communications networks and services, in order to ensure continuity of service to centres receiving emergency calls via the 112 emergency number and public warnings, to complement the risk analysis or the application of mitigation techniques that are generally accepted by the electronic communications and digital infrastructure sector and other obliged entities, and to implement those measures that have been specified in the ordinary and extraordinary audits which obliged entities are required to submit in accordance with the provisions of this Royal Decree.

Furthermore, when approving these instructions and guidelines, the Secretary of State for Telecommunications and Digital Infrastructure must take into account the costs associated with the various measures and solutions that may be imposed, having regard to the financial situation of the obliged party and the configuration of the network, service or infrastructure.

The instructions and guidelines shall be approved by the Secretary of State for Telecommunications and Digital Infrastructure, following a report from the emergency communications reception centre and after the regulated entity has been given the opportunity to be heard. They shall constitute a final administrative decision and may be challenged directly before the administrative courts.

Article 21. Notification obligation in the event of interruption of the emergency communications service via the 112 emergency number or the public warning service.

1. In the event of an interruption to the service routing emergency calls to the 112 emergency number or to the public warning service, both the centres receiving emergency calls via the 112 emergency number and public warnings, and the obliged parties, are required to notify the Secretary of State for Telecommunications and Digital Infrastructure of such an incident without delay, within a maximum of one hour of becoming aware of it.

2. In order to determine the impact of the interruption of the emergency communications service or the public warning service, the following parameters shall be taken into account:

- a) The number of users affected by the interruption of the emergency communications service via the 112 emergency number or the public warning service.
- b) The duration of the service interruption.



- c) The geographical area or areas affected by the service interruption.
- d) The extent of the impact on public safety.

3. In order to comply with the obligation to notify any interruption to the emergency communications service or the public warning service, centres receiving emergency calls via the 112 emergency number and public warnings, as well as the obliged parties, shall have the necessary material and human resources to fulfil the notification obligation in the event of an interruption to the emergency call service or the public warning service, regardless of the means and resources allocated to resolving the security incident and restoring normal service.

4. Interruptions to the emergency communications service via the 112 emergency number or the public warning service are considered significant incidents.

In this regard, centres responsible for receiving emergency calls via the 112 emergency number and public warnings, as well as obliged entities that experience an interruption to their emergency communications service or public warning service, must submit the following notifications to the Secretary of State for Telecommunications and Digital Infrastructure:

a) Initial report

The initial notification shall in any case be sent by the centres receiving emergency calls and public warnings, as well as by the obliged parties, in the event of any interruption of the emergency communication service or the public warning service.

This notification must be sent by email to the Secretary of State for Telecommunications and Digital Infrastructure within one hour of the reception centre or the obliged party becoming aware of it.

The initial notification shall include at least information on the exact time of the start of the incident, a brief description of the cause that gave rise to the incident, the geographical area affected, the number of estimated lines affected, contingency measures taken during the first hour that the emergency communications service or public warning service has been interrupted, plans envisaged for the recovery of the affected service, estimated duration of the incident and contact person and communications channels used to inform both users and the administration as well as any other relevant information.

b) Intermediate notifications

If, one hour after the initial notification, the emergency communications service or the public warning service has not been restored, both the



receiving centres and the obliged parties must submit to the Secretary of State for Telecommunications and Digital Infrastructure, by email, at the time the incident was first reported and subsequently every two hours, all necessary interim notifications to update the information contained in the initial notification and to provide any additional information requested by the Secretary of State for Telecommunications and Digital Infrastructure in the manner and within the timeframe specified.

Intermediate notifications shall be submitted until the final notification is made, without prejudice to the Secretary of State for Telecommunications and Digital Infrastructure's option to modify this period of time depending on the impact and severity of the security incident that has occurred.

In the intermediate notifications to be made to the Secretary of State for Telecommunications and Digital Infrastructure, the information reported in the initial notification shall be provided in more detail. A detailed description shall be provided of the incident and the networks, services, associated resources and digital infrastructures affected, the impact of the fault, whether other operators are affected, an update on the number of lines affected, a preliminary analysis of the cause of the fault, whether the cause is internal or external and details of the cause, whether it is due to system failure, network congestion, human error, malicious acts, natural phenomena, or third-party failures such as power supply issues, cable theft or breakage, earthquakes or floods, as well as any additional information that the operator may report.

c) Final report

As soon as they become aware that the emergency communications service or the public warning service has been restored, the reception centres and the designated entities shall notify the Secretary of State for Telecommunications and Digital Infrastructure by email.

Without prejudice to the foregoing, within a maximum of 24 hours of being notified that the incident has been resolved, the reception centres and the obliged parties shall send a final notification stating, in addition to the exact time at which the emergency communications service or the public warning service was restored, an update that is as detailed as possible regarding the latest information reported in the initial notification or in the interim notifications, if such notifications were issued.

d) Detailed Report

The detailed report shall be sent by email to the Secretary of State for Digital Infrastructure no later than 5 working days after the notification



of the restoration of the communications service to the emergency number or the public warning service.

The detailed report must contain at least the following information:

- i) Detailed description of the incident:
 - a. Start and end times of the incident. Total duration of the incident.
 - b. Type of incident (e.g. network failure, service disruption, server outage, data centres, etc.).
 - c. Geographic area affected.
- ii) Impact of incident:
 - a. Impact on the emergency communications service provided via the 112 emergency number.
 - b. Impact on the public warning service.
 - c. Other operators affected.
 - d. Number of lines or users affected.
- iii) Causes of the incident:
 - a. Detailed analysis of the cause of the incident.
 - b. Detailed description of possible internal or external causes: System failures, network congestion, human error, malicious acts, natural phenomena, failures by third parties such as the electricity supply, arson, theft or cable breakage, earthquakes or floods, etc.
- iv) Contingency measures adopted starting one hour after the start of the incident:
 - a. Description of the contingency measures taken to mitigate the incident involving the interruption to the emergency communications service or the public warning service.
 - b. Communication to interested parties: Secretary of State for Telecommunications and Digital Infrastructure, communication to end users, other units such as UME or civil protection.
- v) Recovery plans:
 - a. A description of the progress made in restoring each of the services affected as a result of the contingency measures implemented to mitigate the incident.
 - b. Measures to prevent similar incidents in the future.



vi) Communication and contact person:

- a. Channels used to notify users, the authorities, civil protection and the UME of any disruption to the emergency communications service or the public warning service.
- b. Contact person: First name, surname, email address and mobile phone number.

vii) Responsibility: Potential liability of the obliged party in relation to the incident.

viii) Supporting documentation.

5. The Secretary of State for Telecommunications and Digital Infrastructure may establish and issue a specific notification form during the initial, interim and final notification stages following an interruption to the emergency communications service or the public warning service, requesting specific and additional information, tailored to the needs and severity of the service disruption.

6. Centres responsible for receiving emergency calls via the 112 emergency number and public warnings, and the obliged entities, shall provide the Secretary of State for Telecommunications and Digital Infrastructure, within three months of the entry into force of this Royal Decree, with the contact details of the person responsible for these notifications, so that further information may be requested if necessary. The contact details must be updated once a year.

CHAPTER V

Assumption by the General State Administration of the direct management of certain publicly available electronic communications services, in order to ensure public security and national security or the fulfilment of public service obligations.

Article 22. Assumption of the direct management of certain publicly available electronic communications services, in order to ensure public security and national security or the fulfilment of public service obligations.

1. By virtue of the provisions of Article 4(6) of Law 11/2022 of 28 June, the Government may, on an exceptional and temporary basis, agree that the General State Administration shall ensure the direct management of certain publicly available electronic communications services, other than number-independent interpersonal communications



services or the operation of certain public electronic communications networks, in order to safeguard public security and national security, as those networks and services are defined in Annex II to Law 11/2022 of 28 June. Networks and services operated or provided exclusively on a self-provision basis shall be excluded.

2. This exceptional and temporary power of direct management may extend to any infrastructure, associated resource, or element or level of the network or service deemed necessary to preserve or restore public safety and national security. Under no circumstances may such intervention constitute a violation of the fundamental rights and civil liberties recognised by the legal system.

3. In the event of non-compliance with public service obligations, in accordance with the provisions of Law 11/2022, of 28 June, the Government may, on an exceptional and temporary basis, agree, subject to a mandatory report from the National Commission on Markets and Competition, that the General State Administration shall assume the direct management of the corresponding services or the operation of the corresponding networks. In the latter case, the Government may, subject to the same conditions, intervene in the provision of electronic communications services.

Prior to assuming the direct management or intervening in electronic communications services that may affect access to or operation of emergency communications via the 112 emergency number or public warning systems, the Government shall cooperate with the competent Autonomous Communities in the management of those emergency communications and public warning services, in order to assess the impact of the measure on their operations and ensure appropriate institutional coordination.

4. The decisions to take over or intervene in the direct management of the service and to intervene in or operate the networks referred to in the preceding paragraphs shall be adopted by the Government either at its own initiative or at the request of a competent Public Authority. In the latter case, the Public Authority concerned must have powers in the field of security or in relation to the provision of the public services affected by the abnormal functioning of the electronic communications network or service.

5. If the procedure is initiated at the request of an authority other than the State, the relevant authority shall be regarded as an interested party and may issue an opinion prior to the final decision.

6. The decisions to assume direct management of the service and to intervene in it or to intervene or operate the networks referred to in this paragraph must be notified by the Government to the competent judicial authority within 24 hours. That authority shall, within 48 hours,



determine whether such decisions are compatible with the fundamental rights and public freedoms recognised in the legal system, and annul them if they are not.

7. The rules contained in this article shall be without prejudice to the provisions of the specific legislation on telecommunications relating to public order, public security, national defence and national security.

CHAPTER VI

Supervision and cooperation

Article 23. Supervision and enforcement of security and resilience obligations applicable to electronic communications networks and services, their associated resources and certain digital infrastructures.

1. The Secretary of State for Telecommunications and Digital Infrastructure shall act as the competent authority in Spain for receiving the notifications referred to in Chapter III of this royal decree, as well as for supervising the security and resilience obligations relating to electronic communications networks and services, their associated resources and certain digital infrastructures, and shall take the necessary measures to ensure compliance with the obligations set out in this royal decree. In adopting these measures, the Secretary of State for Telecommunications and Digital Infrastructure may establish supervision methodologies to prioritise these functions using a risk-based approach.

2. In particular, the role of the Secretary of State for Telecommunications and Digital Infrastructure, as the competent authority, is to monitor and verify compliance by obliged entities with the obligations set out in this Royal Decree, including, amongst others, the submission of general plans by each obliged entity, specific plans and obligations to report security incidents affecting the network and electronic communications services, their associated resources and certain digital infrastructures, as well as any other obligation imposed by the Secretary of State pursuant to this Royal Decree.

3. When carrying out those tasks, obliged entities may be required to provide all relevant information necessary to assess the security of electronic communications networks and services.

4. The obliged entities may also be required to commission, at their own expense, an external audit to verify compliance with the obligations laid down in this Royal Decree.



5. The obliged entities shall collaborate in this supervision by facilitating inspection actions, providing all information required to that effect, and implementing orders or instructions issued, where appropriate, to remedy the deficiencies identified.

6. Any supervisory or enforcement measures imposed by the Secretary of State for Telecommunications and Digital Infrastructure in relation to compliance by obliged entities with the obligations imposed on them under this Royal Decree shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

7. The Secretary of State for Telecommunications and Digital Infrastructure, as the competent authority in the exercise of its supervisory functions, may adopt at least the following measures in relation to obliged entities:

- a) On-site inspections and remote supervision, which may include random checks conducted out by qualified professionals.
- b) Periodic and targeted security audits, where applicable, conducted by an independent third party, in accordance with the procedures determined by the competent authority. These security audits will be carried out every two years. They will be based on risk assessments, their results will be reported to the Secretary of State for Telecommunications and Digital Infrastructure, and their costs will be borne by the audited organisation.
- c) Extraordinary audits, in particular where justified by the occurrence of a significant incident or where there is evidence, indications or information suggesting non-compliance by an obliged entity. The costs of these audits will be borne by the audited entity.
- d) Security analysis based on objective, non-discriminatory, fair and transparent risk assessment criteria, with the cooperation of the Secretariat of State for Telecommunications and Digital Infrastructures where necessary.
- e) Requests for information necessary to assess the measures adopted by the obliged entity in relation to compliance with the obligation to submit information.
- f) Requests to access data, documents and information necessary to carry out their supervisory tasks.

8. In exercising its enforcement powers, the Secretary of State for Telecommunications and Digital Infrastructure may, at the very least:

- a) Issue a warning to obliged entities in the event of non-compliance.
- b) Adopt binding instructions, which shall set out the measures necessary to prevent or remedy an incident, the deadlines for implementing those measures and notifying their



- implementation, or an order requiring the obliged entities to remedy the deficiencies or infringements identified.
- c) Where appropriate, order the obliged entities to cease conduct that infringes this legislation and desist from repeating that conduct.
 - d) Require obliged entities to ensure compliance with the obligations laid down in this Royal Decree, including the obligations to submit their general and specific plans, as well as the obligation to notify security incidents as set out in Articles 12 and 21 within the specified time limits.
 - e) Require obliged entities to inform, in the circumstances set out in this Royal Decree, the natural or legal persons to whom they provide services or carry out activities, of any interruption or degradation of the electronic communications service provided to them, as well as of any measures taken to ensure the prompt restoration of the service.
 - f) Order obliged entities to implement the corrective measures or recommendations issued by the Secretariat of State for Telecommunications and Digital Infrastructures within the time limit specified by that authority.
 - g) Designate a supervising officer to oversee, for the period to be determined, the compliance of the obliged entities with their obligations.
 - h) Exercise the power to impose sanctions in the cases and under the conditions set out in Law 11/2022 of 28 June and in this Royal Decree, and to conduct administrative proceedings in all cases.

9. Where the enforcement measures adopted prove ineffective in achieving their intended objectives, the Secretary of State for Telecommunications and Digital Infrastructure shall set a deadline for the obliged parties to take the necessary steps to remedy the shortcomings or comply with the requirements, without prejudice to any liabilities that may arise. If these measures are not adopted within the specified time limit, the Secretary of State for Telecommunications and Digital Infrastructure shall have the power to:

- a) Temporarily suspend or request the competent authorities, in accordance with current regulations, to suspend temporarily the authorisation relating to part or all of the services or activities provided by the obliged party.
- b) Request that competent bodies, courts or tribunals, in accordance with the legal system, to temporarily prohibit any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising management functions.



Temporary suspensions or prohibitions that are imposed shall be applied only until the obliged entity takes the necessary measures to remedy the deficiencies or comply with the requirements established by the Secretary of State for Telecommunications and Digital Infrastructure. The imposition of such temporary suspensions or prohibitions shall be subject to appropriate safeguards in accordance with the general principles of the legal system.

10. Furthermore, in respect of matters not expressly regulated in this article, the supervisory and enforcement measures set out in national and European legislation on the coordination and governance of cybersecurity and on the resilience of critical infrastructure operators shall apply.

Article 24. Cooperation at national level.

1. The Secretary of State for Telecommunications and Digital Infrastructure shall carry out the following tasks in the field of national cooperation:

- a) In order to ensure the effective fulfilment of its functions and obligations, the Secretary of State for Telecommunications and Digital Infrastructure shall cooperate and collaborate with public bodies and agencies with responsibilities in the areas of national security, national defence, public safety, public security, digital administration and the protection of personal data, as well as with any other entity with competence within the scope of this Royal Decree in matters relating to the security of electronic communications networks and services.
- b) It shall cooperate and regularly exchange information with competent authorities designated pursuant to the regulation on the identification of critical entities, risks, cyber threats and ICT-related incidents, as well as on risks, threats and non-cyber incidents affecting essential entities identified as critical entities, and on measures taken in response thereto. It shall also share information in relation to ICT-related incidents and cyber threats with competent authorities in the areas of electronic identification and trust services for electronic transactions in the internal market, digital operational resilience of the financial sector, and electronic communications.
- c) It shall cooperate with the competent authorities in the sectors subject to the specific cybersecurity regulations in order to harmonise the regulations.



2. The Secretary of State for Telecommunications and Digital Infrastructure shall inform the Secretary of State for Security of the Ministry of the Interior of any incidents affecting national strategic operators that are of interest for improving the protection of critical infrastructure, within the framework of Law 8/2011 of 28 April regulating such infrastructure.

3. The Secretary of State for Telecommunications and Digital Infrastructure shall also inform the National Commission on Markets and Competition of any security incidents that affect or may affect the specific obligations imposed by that Commission on the relevant markets through ex ante regulation.

Article 25. Cooperation with the Autonomous Communities.

1. Mechanisms for mutual cooperation will be developed to enable both the Secretary of State for Telecommunications and Digital Infrastructure and the Autonomous Communities to exercise the functions and powers assigned to them by law, with a view to achieving the best possible coordination in the exercise of these powers, thereby contributing to the common objective of ensuring the swiftest and most effective resolution of incidents and the fastest and fullest restoration of the security of the networks, the continuity of the services and the operability of the infrastructures referred to in this Royal Decree.

2. In particular, the Secretary of State for Telecommunications and Digital Infrastructure shall establish the appropriate channels for the transmission of information so that the Autonomous Communities may receive information as quickly as possible regarding significant incidents affecting electronic communications networks and services and certain digital infrastructures, in particular those networks, services and infrastructures located within their territories.

3. The Secretary of State for Telecommunications and Digital Infrastructure shall also develop the appropriate cooperation mechanisms to enable the Autonomous Communities to contribute to setting the objectives, practices and instruments designed to strengthen the security and resilience of public electronic communications networks, publicly available electronic communications services and their associated resources, and the digital infrastructures that contribute to their operation and the provision of those services.

Article 26. Cooperation at European Union level.

1. The Secretary of State for Telecommunications and Digital Infrastructure will cooperate at European Union level by representing



Spain in political and strategic forums and working groups on network security, electronic communications services and digital infrastructure.

2. Once a year, the Secretary of State for Telecommunications and Digital Infrastructure shall submit to the Commission and to ENISA a summary report on the notifications received and the measures taken in accordance with this royal decree.

Article 27. Cooperation in terms of the incidents that affect personal data.

1. The Secretary of State for Telecommunications and Digital Infrastructure shall cooperate closely with the Spanish Data Protection Agency and, where appropriate, with the independent supervisory authorities of the Autonomous Communities, to deal with incidents that give rise to personal data breaches, informing them of any incidents that might compromise the security of personal data and should be reported, as well as their development.

2. This is without prejudice to the tasks assigned to data controllers in relation to reports of possible breaches in the protection of personal data in accordance with the provisions of Organic Law 3/2018 of 5 December 2018 on the protection of personal data and the guarantee of digital rights and, where applicable, Organic Law 7/2021 of 26 May 2021 on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties.

3. The provisions of this Article shall be without prejudice to the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Organic Law 3/2018 of 5 December 2018 on Protection of Personal Data and Guarantee of Digital Rights, and its implementing regulations.

Article 28. Authorisation for releasing personal data.

1. If the reporting of incidents or their management, analysis or resolution requires the communication of personal data, the processing thereof shall be restricted to what is strictly appropriate and relevant and limited to what is necessary in relation to the purpose, of the actions indicated, pursued in each case.

2. The release of said data for such purposes shall only be deemed authorised in the following cases:

- a) From the obliged entities to the Secretary of State for Telecommunications and Digital Infrastructure or bodies



designated by it to carry out supervisory and enforcement functions.

- b) Between the Secretary of State for Telecommunications and Digital Infrastructure and the bodies designated by it to carry out supervisory and enforcement functions.
- c) Between the Secretary of State for Telecommunications and Digital Infrastructure and the European or international national regulatory authorities.
- d) Between the single point of contact and the single points of contact in other Member States of the European Union.

CHAPTER VII

Inspection and penalty regime relating to the security and continuity of electronic communications networks and services, their associated resources and digital infrastructures

Article 29. Inspection function.

The inspection function in relation to the security of electronic communications networks and services, their associated resources and digital infrastructures shall be exercised by the Ministry for Digital Transformation and the Civil Service through the Secretary of State for Telecommunications and Digital Infrastructure.

Article 30. Inspection powers.

1. The Inspection Services of the Secretary of State for Telecommunications and Digital Infrastructure may carry out the inspections they deem necessary in order to verify compliance by the obliged entities with the obligations laid down in this Royal Decree. For this purpose, these Inspection Services may collect any additional data they deem necessary, as well as carry out their own measurements and checks of the operators' networks and information systems.

2. The obliged entities shall be obliged to make available to the inspection personnel any books, records and documents, whatever their form or medium, together with any technical resources that the personnel deem necessary, including software, computer programmes and magnetic, optical or any other type of files. For this purpose, the inspection personnel may make or obtain copies of such materials.

3. Furthermore, they must provide, upon request, any documentation required by the inspection personnel to determine the ownership of the



equipment or the origin of transmissions, activities, or the content or services provided via electronic communications networks.

4. The obliged entities shall submit to inspections carried out by inspection personnel. Any refusal or obstruction in to appearing for inspection proceedings for which a summons has been issued, in carrying out the technical tests or supplementary procedures required, or in providing the information or documentation requested shall be penalised, in accordance with the following articles of this title, as obstruction of the inspection function.

5. Inspection personnel shall, for the purposes of performing the duties provided for in this Article, have access free of charge to all public registers, in particular the Property and Commercial Registers. Access to information held in the register shall be provided electronically, in the manner set out in the relevant regulations.

Article 31. Liability for infringements.

Administrative liability for infringement of the provisions contained in this Royal Decree shall be incurred by the natural or legal person that carries out or is materially responsible for the activity constituting the alleged infringement.

Section 32. Serious offences.

Any breach by the obliged entities of any of the obligations set out in this Royal Decree that is directly related to the integrity and security of the provision of electronic communications services or the supply of electronic communications networks, and, in particular, the obligations to draw up and submit the general and specific plans established in this Royal Decree, and the obligations relating to the notification of incidents provided for therein, shall be regarded as a serious infringement pursuant to Article 107(22) of Law 11/2022 of 28 June, without prejudice to the commission of any other possible infringements that may be committed and which are defined in Articles 106, 107 and 108 of Law 11/2022 of 28 June, which shall be penalised in accordance with the provisions of Title VIII of the aforementioned Law.

Article 33. Sanctions.

1. For the commission of serious offences as defined in Article 107(22) of Law 11/2022 of 28 June, the offender shall be liable to a fine of up to two million euros, in accordance with Article 109 of Law 11/2022 of 28 June.



2. For the commission of other offences set out in Articles 106, 107 and 108 of Law 11/2022 of 28 June, the offender shall be subject to the penalties laid down in Article 109 of Law 11/2022 of 28 June.

Article 34. Criteria for determining the amount of the sanction.

1. The amount of the sanction imposed shall be graduated taking into account, in addition to the provisions of Article 29 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, the following:

- a) The severity of the offences previously committed by the subject to whom the penalty is imposed;
- (b) the damage caused, such as the degradation to the service and the cost of rectifying it;
- c) Voluntary compliance with the precautionary measures that, where appropriate, are imposed in the sanctioning procedure;
- d) Refusal to provide, or obstruction of access to, the information or documentation requested;
- e) The cessation of the infringing activity, prior to or during the processing of the penalty proceedings;
- (f) The impact on protected legal interests relating to public order, public safety and national security, or the rights of users;
- g) Active and effective cooperation with the competent authority in detecting or proving the infringing activity.

2. In the case of an infringement consisting of providing misleading, incorrect or incomplete information, either knowingly or through gross negligence, for the purposes of drawing up the reports provided for in the Royal Decree, the amount of the sanction shall be determined taking into account, amongst other criteria, the harm caused to competition, to users or to the public administration.

Article 35. Precautionary measures.

The Secretary of State for Digital Transformation and the Civil Service may adopt precautionary measures pursuant to Articles 111 and 112 of Law 11/2022 of 28 June, with a view to bringing about the cessation of the alleged infringements and ensuring compliance with the provisions of this Royal Decree.

Article 36. Statute of limitations.

1. Serious offences shall be time-barred after two years, in accordance with Article 113 of Law 11/2022 of 28 June.



The limitation period for infringements shall be calculated from the date on which the infringement was committed. The limitation period shall be interrupted by the initiation, with the knowledge of the person concerned, of disciplinary proceedings. The limitation period shall start to run again if the disciplinary proceedings are halted for more than 1 month for reasons not attributable to the alleged offender.

In the event of a continuing infringement, the limitation period shall begin to run on the date on which the infringing activity ceases or, where applicable, on the date of the last act by which the infringement is completed. However, the infringement shall be deemed to continue for as long as the telecommunications equipment or installations that are the subject of the proceedings are not made available to the Administration or until there is conclusive evidence that they cannot be used.

2. Sanctions shall be subject to a limitation period of 2 years for very serious offences. The prescription period for sanctions shall be counted from the day after the final ruling imposing the sanction becomes enforceable or the period for appealing it has expired. The limitation period shall be interrupted by the commencement of the enforcement procedure, with notification sent to the interested party, and shall restart if the latter is halted for more than 1 month for reasons not attributable to the accused.

Article 37. Powers to impose penalties.

The power to impose sanctions to ensure compliance with the obligations set out in this Royal Decree lies with the Secretary of State for Telecommunications and Digital Infrastructure, in accordance with Article 114 of Law 11/2022 of 28 June.

First additional provision. Regulations on the coordination and governance of cybersecurity and on the resilience of critical entities.

1. This Royal Decree shall apply to the security incidents described in Article 11. For all other security incidents, the relevant national or European regulations on the coordination and governance of cybersecurity and on the resilience of critical entities will apply.

2. Without prejudice to the foregoing, the parties subject to this Royal Decree shall be subject to national or European legislation relating to the coordination and governance of cybersecurity and the resilience of critical entities in respect of matters not provided for or regulated in this Royal Decree.



Second additional provision. Coordination Committee for the Security and Resilience of Electronic Communications Networks and Services.

1. In order to facilitate collaboration, coordination, cooperation, the exchange of information and the participation of all stakeholders involved in the security and resilience of electronic communications networks and services, and to contribute to the continuous improvement of the capacity to respond to significant incidents, the Coordination Committee for the Security and Resilience of Electronic Communications Networks and Services is hereby established.

The Committee will act as a body for strategic and technical cooperation, a forum for dialogue and consultation, and a platform for drawing up proposals, recommendations and best practices in the field of security and resilience, without assuming any direct operational coordination functions in incident management.

2. The Coordination Committee for the Security and Resilience of Electronic Communications Networks and Services comprises representatives from the Ministry for Digital Transformation and the Civil Service, the Ministry of the Interior, the Ministry of Defence, the Department of National Security, the Autonomous Communities, the Spanish Federation of Municipalities and Provinces, the National Commission for Markets and Competition, and the most representative associations of electronic communications operators, digital infrastructure providers, telecommunications equipment manufacturers, and consumers and users. The specific composition of the committee will be determined by order of the Minister for Digital Transformation and the Civil Service.

3. The Coordination Committee for the Security and Resilience of Electronic Communications Networks and Services shall adopt its rules of organisation and operation.

4. The Committee may propose the carrying out of tests, drills and practical exercises with the aim of verifying the effectiveness of the measures and obligations established regarding the security and resilience of electronic communications networks and services, drawing conclusions on the implementation of these measures, and proposing ways to improve the security and resilience of these networks and services.

Third additional provision. Amendment of contracts entered into between operators providing public electronic communications networks or publicly available electronic communications



services and the owners or operators of their associated resources, electronic communications networks providing wholesale services, and certain digital infrastructures.

1. Compliance with the obligations set out in this Royal Decree may give rise to the amendment of contracts entered into between, on the one hand, operators providing public electronic communications networks or publicly available electronic communications services and, on the other hand, the owners or operators of their associated resources, electronic communications networks providing wholesale services, and certain digital infrastructures.

2. In the event that no agreement is reached on the need for, or the technical, financial or operational terms of, the amendment to the relevant contract between electronic communications operators, or between electronic communications operators and the owners or operators of associated resources, any of the parties may refer the matter to the National Commission on Markets and Competition, in accordance with the provisions of Article 28 of Law 11/2022 of 28 June.

The National Commission on Markets and Competition, in the decision resolving the dispute, in accordance with the provisions of the aforementioned Article 28 of Law 11/2022 of 28 June, shall seek to achieve the objectives set out in Article 3 of the aforementioned Law. In particular, with regard to the allocation of costs that may arise from compliance with the obligations set out in Article 7(4) relating to electricity supply infrastructure intended to ensure the operational continuity and uninterrupted provision of electronic communications services, it shall establish the appropriate measures to ensure that such cost allocation is fair, reasonable and proportionate.

Fourth additional provision. Adaptation of the ex ante regulation.

In the event that compliance with the provisions of this Royal Decree requires an amendment to the terms under which the specific obligations required by virtue of the ex ante regulation approved pursuant to the provisions of Chapter IV of Title II of Law 11/2022 of 28 June have been imposed, the National Commission on Markets and Competition shall have a period of one year, commencing on the date on which the regulated operator informs the Commission of the need to amend and adapt that ex ante regulation to the provisions of this Royal Decree.

Fifth additional provision. Technological adaptation of the transmission of security incident notifications.



1. The head of the Ministry for Digital Transformation and the Civil Service may, by order, decide that the transmission by email of notifications of significant security incidents pursuant to Articles 12 and 21 may be replaced or supplemented by other means or channels of transmission or communication, including transmission via a telematic platform or service that may be established for this purpose by the Ministry for Digital Transformation and the Civil Service or in accordance with the provisions of national or European legislation.

2. Furthermore, the Minister for Digital Transformation and the Civil Service may, by order, decide that security incidents of minor significance must be reported through an online platform or service, to which the various public administrations within whose territory the affected networks are located shall have access. This order will specify the online platform or service to be used, its terms of use and the date on which it will come into effect.

Sole repealing provision. Regulatory repeal.

1. Chapter VI of Order IET/1090/2014 of 16 June, which regulates the conditions relating to the quality of service in the provision of telecommunications services, concerning events that cause a significant degradation of service quality, is hereby repealed.

2. Furthermore, any provisions of equal or lower legal force than this Royal Decree that are contrary to its provisions are hereby repealed.

First final provision. Attribution of powers.

This Royal Decree is issued by virtue of the exclusive competence of the State regarding telecommunications, as recognised in Article 149(1)(21) of the Spanish Constitution.

Second final provision. Regulatory implementation and application.

1. The head of the Ministry for Digital Transformation and the Civil Service shall, within the scope of their powers, issue any provisions necessary to implement the provisions of this Royal Decree.

2. The head of the Ministry of Digital Transformation and the Civil Service and the head of the Secretary of State for Telecommunications and Digital Infrastructures shall, within the scope of their powers, approve all measures necessary for the application of the provisions of this Royal Decree.



Third final provision. Entry into force.

This Royal Decree shall enter into force on the day after its publication in the Official State Gazette.

In Madrid on xx xxxx 2026

The Minister for Digital Transformation
and the Civil Service

ÓSCAR LÓPEZ ÁGUEDA