REPORT ON THE REGULATORY IMPACT ANALYSIS OF THE PRELIMINARY DRAFT LAW ON CYBERSECURITY COORDINATION AND GOVERNANCE

1. EXECUTIVE SUMMARY SHEET

Proposing Ministries/Bodies	• Ministry of the Interior • Presidency of the Government • Ministry of Defence • Ministry for the Digital Transformation and the Civil Service	**Date**	November 2024
Title of the Regulation	Law on Cybersecurity Coordination and Governance		
Type of report	☑ Normal ☐ Abbreviated		
TIMELINESS OF THE PROPOSAL			
Subject	Transposition of 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.		
Objectives	- To create a single national competent authority for cybersecurity. - To define a uniform criterion for determining which entities are included within the scope classified as essential entities and important entities. - To establish a catalogue of measures necessary for cybersecurity risk-management. - To strengthen the procedure for reporting incidents that disrupt or are likely to disrupt provision of the services of essential and important entities. - To create the role of the Information Security Officer. - To strengthen the regulations governing the exchange of information on cybersecurity. - To establish an institutional and coordination framework between the competent authorities.		

Main alternatives considered	No other alternatives could be considered when it became imperative to transpose 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.
CONTENT AND LEGAL ANALYSIS	
Type of regulation	Law
Structure of the Regulation	The preliminary draft is structured in an explanatory note, 50 articles divided into 7 chapters, 8 additional provisions, 3 transitional provisions and 5 final provisions.
Reports received and to be received	The preliminary draft is the result of a long process of reflection and close collaboration with the various management centres of the Ministry of the Interior: The Secretariat of State for Security (Directorate General for Coordination and Studies) and the General Technical Secretariat, which has already reported. In accordance with the first paragraph of Article 26(5) of Law 50/1997 of 27 November 1997, a **report will be received** from the following Ministries: • Ministry of Defence • Ministry for the Digital Transformation and the Civil Service • Ministry of Transport and Sustainable Mobility • Ministry of Science, Innovation and Universities • Ministry for the Ecological Transition and the Demographic Challenge • Ministry of Industry and Tourism • Ministry of Agriculture, Fisheries and Food • Ministry of Territorial Policy and Democratic Memory • Ministry of Health • Ministry of the Presidency of the Government (Department of National Security). The following will also be received: • Report of the Office of Coordination and Regulatory Quality (Article 26(9) of Law 50/1997 of 27 November 1997) Other reports or opinions: • The Spanish Data Protection Agency. • The Council of State. **Similarly, a report from the Ministry of Territorial Policy and Democratic Memory is pending, in accordance with the sixth subparagraph of Article 26(5).**

Hearing process	A prior public consultation process was conducted between 21 September and 17 October 2023, as provided for in Article 133 of Law 39/2015 of 1 October 2015 and Article 26 of Law 50/1997 of 27 November 1997, in which various observations were received. Furthermore, it will have to go through the public information and hearing process.	
IMPACT ANALYSIS		
COMPLIANCE WITH THE DISTRIBUTION OF POWERS	Issued under the provisions of Article 149(1) 29 of the Spanish Constitution, which grants the State exclusive competence in matters of public safety. As such, the constitutional distribution of powers is respected.	
ECONOMIC AND BUDGETARY IMPACT	**General impact on the economy.**	It has a positive economic impact on the economic sector upon which obligations are imposed.
	With regard to competition	☒ The Regulation has no significant impact on competition. ☐ The Regulation has positive effects on competition. ☐ The Regulation has negative effects on competition.
	With respect to administrative burdens	☐ It entails a reduction in administrative burdens Estimated quantification: ☒ It incorporates new administrative burdens Estimated quantification: ☐It does not affect administrative burdens.
	With respect to budgets, the Regulation: ☐ Affects State budgets. ☐ Affects the budgets of other regional administrations.	☒ Implies an expense. ☐ Implies an income.

GENDER IMPACT	The Regulation has the following gender impact:	☐ Negative ☒ None ☐ Positive
IMPACT ON CHILDHOOD, ADOLESCENTS AND FAMILIES	The Regulation has the following impact on childhood, adolescence and family:	☐ Negative ☒ None ☐ Positive
IMPACT ON THE PROTECTION OF PERSONAL DATA	The Regulation has the following impact on the protection of personal data:	☐ Negative ☐ None ☒ Positive
OTHER IMPACTS CONSIDERED	There are no other significant impacts.	
EX POST EVALUATION	Not applicable	

2.- TIMELINESS OF THE PROPOSAL.

2.1. Rationale.

Since the entry into force of Directive (EU) 2016/1148, considerable progress has been made in increasing the Union's level of cyber resilience. The revision of said Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change of mindset. It has led to the implementation of national cybersecurity frameworks through the definition of national security strategies for networks and information systems, the establishment of national capacities and the implementation of regulatory measures covering the critical entities and infrastructures identified by each Member State. Directive (EU) 2016/1148 has also facilitated cooperation at Union level through the establishment of the Cooperation Group and the network of information security incident response teams. Despite these achievements, the revision of Directive (EU) 2016/1148 has revealed some inherent shortcomings that prevent current and emerging challenges in the field of cybersecurity from being effectively addressed.

The security of networks and information systems has become a crucial aspect of everyday life thanks to the speed of the digital transformation and the interconnectedness of society, including in cross-border exchanges. This progress has resulted in an expansion of the range of cyber threats, with the consequent emergence of new challenges that require appropriate, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impacts of incidents are increasing and represent a serious threat to the functioning of network and information security systems. As a result, incidents can disrupt economic activities in the internal market, generate financial losses, undermine user confidence and cause extensive damage to the Union's economy and society. Cybersecurity preparedness and effectiveness are therefore more essential than ever if the internal market is to function correctly. Moreover, cybersecurity is an essential factor enabling many critical sectors to successfully participate in the digital transformation and take full advantage of the economic, social and sustainable benefits of digitalisation.

Any requirements imposed by one Member State that differ from, or even contradict, those applied by another Member State may substantially affect these cross-border activities. Furthermore, inadequately designed or implemented cybersecurity requirements in one Member State are likely to have an impact on the level of cybersecurity in other Member States, especially given the intensity of cross-border exchanges. The revision of Directive (EU) 2016/1148 has revealed significant differences in the manner of its application by the Member States, particularly regarding its scope, the parameters of which were left largely to the discretion of the Member States. Directive (EU) 2016/1148 similarly afforded Member States broad discretion regarding the implementation of the security and incident reporting obligations laid down therein. Consequently, those obligations were applied in significantly different ways in each Member State. There are similar differences in the way that the provisions of Directive (EU) 2016/1148 concerning supervision and enforcement have been applied.

All these differences lead to fragmentation of the internal market and may have detrimental effects on its functioning, with particular regard to the cross-border provision of services and the level of cyber resilience, due to the implementation of disparate measures. Ultimately, these differences could lead to greater vulnerability to cyber threats for some Member States, the effects of which could be felt across

the Union. The objective of this Directive is to eliminate such pronounced divergences between Member States, notably by defining minimum standards for the functioning of a coordinated regulatory framework, establishing mechanisms enabling the competent authorities of each Member State to cooperate effectively, updating the list of sectors and activities subject to cybersecurity obligations and ensuring the availability of effective remedies and the enforcement measures that are essential to ensuring effective compliance with those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

Given the intensification and increasing sophistication of cyber threats, Member States should endeavour to ensure that entities excluded from the scope of this Directive achieve a high level of cybersecurity and support the implementation of equivalent cybersecurity risk-management measures that reflect the sensitive nature of said entities.

With these objectives, 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) was published, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148, subject to transposition. It sets **17 October 2024** as the deadline for its transposition into national law by the Member States.

On behalf of the Ministry of Foreign Affairs, European Union and Cooperation, the Ministry of the Interior was designated as responsible for the transposition and the Presidency of the Government, the Ministry of Defence and the Ministry for Digital Transformation as competent.

2.2. Purposes and objectives pursued.

The main objective pursued is to comply with the provisions of the Directive that is being transposed, and more specifically:

The Preliminary Draft Law on Cybersecurity Coordination and Governance transposes 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), amending Regulation (EU)

910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 and Royal Decree-Law 12/2018 of 7 September 2018 on the security of information networks and systems. The NIS2 Directive seeks to overcome certain shortcomings of the NIS1 Directive by providing a more comprehensive framework of both technical and regulatory obligations to strengthen network and information security in the European Union.

The aspect of this preliminary draft Law that stands out as most innovative and among the most significant is the creation of a National Cybersecurity Department, which will overcome the current dispersion of competence in cybersecurity matters by becoming the sole competent national authority in the matter, for the direction, promotion and coordination of all of the activities provided for in this Law, as a single point of contact to ensure cross-sectoral and cross-border cooperation with other competent authorities, as well as the national cybersecurity crisis management authority, and assuming the function of management and coordination of the supervisory authorities and sectoral contact points in the development of their execution and supervision functions, as well as of the reference national computer security incident response teams (CSIRTs).

It also establishes a uniform criterion for determining which entities fall within the scope of this Regulation, for the purposes of compliance with the measures for managing cybersecurity risks, which are classified into two categories: essential entities and important entities, depending on the degree of criticality of their sectors and the type of service they provide, as well as their size and turnover.

The security requirements are reinforced with a list of specific measures, including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing and the effective use of encryption. As regards the measures for cybersecurity risk-management and reporting obligations, this part provides for an individualised risk assessment by the different entities and details the specific actions that they should carry out to ensure and raise the security levels of their network and information systems and prevent the risk of incidents, as well as for the obligation to report significant incidents that occur in their operation or in the provision of their services. In the same vein, the legislation transposing Directive 2023/2557 on the resilience of critical entities introduces coordination

mechanisms that this Department also undertakes to transpose.

The incident reporting introduced in NIS1 is significantly strengthened, with a detailed and comprehensive incident reporting procedure to ensure that reporting takes place within a common European Union framework. More precise provisions are included on the reporting process, the content and deadlines and, in order to comply with the reporting obligations, the National cyber incident reporting and monitoring platform (*Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes*) will be used, which will enable the various players to exchange technical information and monitor incidents.

It also includes the person responsible for information security, as a person or body designated by the essential and important entities, who is responsible for the functions of contact person and technical coordinator for the matters covered by this Law. In this context, it highlights consideration of the person responsible for information security of essential entities through the reform of Law 5/2014, of 4 April 2014 on Private Security.

Finally, a detailed penalties regime is established that includes effective, proportionate and dissuasive penalties, taking into account the specific circumstances of the case. Penalties imposed upon essential entities may reach up to €10 000 000 or a maximum of 2% of the total annual worldwide turnover for the previous financial year. In addition to economic penalties, it also provides for the possibility of other corrective measures, such as continuous monitoring, security audits and the imposition of specific measures to address identified weaknesses in cybersecurity systems.

2.3. Adherence to the principles of sound regulation.

Here follows an analysis of the adherence of the Regulation to the principles of sound regulation set out in Article 129 of Law 39/2015 of 1 October 2015 on Common Administrative Procedures in Public Administration.

On the one hand, this legislation is necessary for the transposition of the NIS2 Directive, Article 41 of which provides that Member States shall, by 17 October 2024 at the latest, adopt and publish the provisions necessary to

comply with this Directive.

It is effective legislation for achieving its desired objectives, as follows.

- To create a single national competent authority for cybersecurity with management and coordination functions.
- To designate the supervisory authorities, with executive functions.
- To define a uniform criterion for determining which entities are included within the scope classified as essential entities and important entities.
- To establish a catalogue of measures necessary for cybersecurity risk-management.
- To strengthen the procedure for reporting incidents that disrupt or are likely to disrupt provision of the services of essential and important entities.
- To create the role of the Information Security Officer.
- To strengthen the legislation and obligations relating to the exchange of information on cybersecurity.
- To establish an institutional and coordination framework between the competent authorities.

With regard to the principle of legal certainty, it is legislation with the status of a law, whose processing and integration into the legal system enjoys the guarantees that protect legislation with this status.

This preliminary draft is also consistent with the principle of proportionality required in the development of any law. It provides for a large number of guarantees that are necessary in order to ensure that any possible impacts on the rights that may be involved, as well as the obligations imposed upon the entities and persons concerned, are proportionate, timely, minimal and sufficient, in terms of meeting the objectives pursued, namely to ensure the unhindered provision of services essential to the maintenance of vital social functions and economic activities within the internal market.

Finally, it also complies with the requisite principle of transparency, having already gone through the prior public consultation procedure and then subsequently

the other procedures that guarantee public participation.

2.4. Alternatives.

The Directive being transposed includes regulation of network and information system security through a cybersecurity coordination and governance model. Article 41 of that Directive requires Member States to adopt the laws, regulations and administrative provisions necessary to comply with that Directive and sets a time frame for them to do so.

The purpose of this Law is to transpose 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 into Spanish law.

In addition, the preliminary draft provides very detailed regulation of the National Cybersecurity Department, which will act as a single point of contact to ensure cross-sectoral cooperation with supervisory authorities and sectoral contact points at national level, as well as liaison work ensuring cross-border cooperation with competent authorities in other Member States and the European Union Agency for Cybersecurity (ENISA).

Therefore, ruling out this possibility, the only possible alternative is the adoption of a law that transposes the provisions of that Directive into Spanish law.

With regard to the status of the law, taking into account that it is legislation that does not affect fundamental rights, the transposition does not require the adoption of a law with organic status, as required under Article 81(1) of the Spanish Constitution.

3.- CONTENT, LEGAL ANALYSIS AND DESCRIPTION OF THE PROCESS.

I. Content.

The preliminary draft is divided into 49 articles, broken down into 7 chapters, as well as 8 additional provisions, 3 transitional provisions, a derogatory provision and 4 final provisions, which include both those aspects that must be developed as provided for in the NIS2 Directive and those others that, it has been considered

appropriate to address without specific provision, since they offer opportunities and advantages in cybersecurity protection actions.

o Chapter I.

This chapter regulates the objective and subjective purpose and scope of application of the law and defines the criteria for identifying essential and important entities. It includes the main definitions to be applied and known, so that all actors involved in interpreting it are aware of the basic elements for understanding the meaning and scope of each provision.

In this regard, the aim is to achieve a high common level of cybersecurity through the adoption of a national cybersecurity strategy and the designation or establishment of competent authorities, a cybersecurity crisis management authority, a single point of contact for cybersecurity (hereinafter 'single point of contact') and computer security incident response teams (CSIRTs), together with a catalogue of measures for cybersecurity risk-management and reporting obligations for the entities regulated by this Law, and rules and obligations relating to the exchange of cybersecurity information and monitoring and enforcement obligations.

The Law applies to public or private entities within the high criticality sectors and other critical sectors listed in Annexes I and II thereto, where they are considered to be medium-sized or large enterprises when they employ 50 or more persons and which have an annual turnover and/or an annual balance sheet total of €10 million or more. It also applies to entities included among the types indicated in Annexes I or II of the Law, regardless of their size:

a) When the services provided are provided by public electronic communications network providers or publicly available electronic communications services, trust service providers, domain name registries and providers of domain name system services;
b) When the entity is the only provider in Spain of a service that is essential to the maintenance of critical social or economic activities;
c) When disruption of the service provided by the entity could have a significant impact on public safety, public order or public health;

d) When disruption of the service provided by the institution could induce significant systemic risks, particularly in sectors in which such a disruption could have cross-border implications;
e) When the entity is a public sector entity, as defined in Article 2 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector;
f) In the case of those critical entities complying with the regulations applicable to measures for the protection of critical infrastructure;
g) In the case of universities and research centres in matters or research projects relating to high criticality and other critical sectors;
h) In the case of companies in which 25% or more of their capital or voting rights are controlled, directly or indirectly, by one or more public bodies and which are identified as such by the competent authority, unless it can be considered a related company;
i) In the case of any other entity that the relevant competent authority identifies as an essential entity by applying the criteria of this Article and issuing a reasoned resolution to this effect.

- **Chapter II.**

Chapter II establishes the national, strategic and institutional framework for network and information system security, with the aim of achieving and maintaining a high level of cybersecurity. To this end, it determines the minimum content to be addressed by the National Cybersecurity Strategy, highlighting, inter alia: the definition of objectives and priorities, particularly with regard to the sectors mentioned in Annexes I and II of the Law; the relationship of authorities and stakeholders involved in implementing the National Cybersecurity Strategy; a governance framework to achieve the objectives and priorities defined in the cybersecurity strategy; a governance framework clarifying the roles and responsibilities of stakeholders, underpinning cooperation and coordination between stakeholders at national level; a mechanism for the identification of relevant assets; assessment of cybersecurity risks; identification of measures to ensure preparedness, response capacity and incident recovery, including cooperation between the public and private sectors; and a plan of measures needed to raise citizens' overall level of cybersecurity awareness.

The main innovation and most significant aspect of this chapter is its provision for the creation of a National Cybersecurity Department, which will

overcome the current dispersion of competence in cybersecurity matters by becoming the sole competent national authority in the matter for the promotion and coordination of all of the activities provided for in this Law, as a single point of contact to ensure cross-sectoral and cross-border cooperation with other sectoral authorities, as well as the national cybersecurity crisis management authority and reference national computer security incident response team.

In addition, it specifies the functions to be carried out by the National Cybersecurity Department, including, in particular, management and supervision functions such as promoting and approving, where appropriate, the use of standards, guides, specifications, technical instructions and any provisions on network and information system security, and informing the public about incidents affecting more than one supervisory authority, where the dissemination of such information is necessary in order to prevent an incident or manage one that has already occurred.

Likewise, it sets out the functions of the supervisory authorities in detail; which of them will be, within the framework of their competences, responsible for supervision and execution functions such as: establishing communication channels with essential and important entities, including the National cyber incident reporting and monitoring platform; receiving and following up on reports of incidents presented within the framework of this Law through the reference national CSIRTs; informing the public about certain incidents, participating, on a voluntary basis, in peer reviews or proposing mandatory cybersecurity risk-management measures for entities included in the scope of this Regulation.

The supervisory authorities shall be:

a) The Ministry of Defence, through the National Cryptologic Centre, for essential and important entities that, being non-critical entities, fall within the scope of Law 40/2015 of 1 October 2015 on the Public Sector Legal Framework;

b) The Ministry for the Digital Transformation and the Civil Service, through the State Secretariat for Telecommunications and Digital Infrastructure and the State Secretariat for Digitalisation and Artificial Intelligence, for essential and important entities in the digital infrastructure and digital service provider sectors, as well as important entities in the other sectors, which have not been designated as critical entities;

c) The Ministry of the Interior, through the Cybersecurity Coordination Office of the Secretary of State for Security, for critical entities and essential entities of the sectors not included in points (a) or (b), as well as for all essential and important entities in the private security sector.

In addition, it provides for the creation of specialised points of contact that would be responsible, inter alia, for providing the National Cybersecurity Department with the information necessary to create compliance standards that are able to take into account the possible specificities of each sector.

As regards the reference national cybersecurity incident response teams (CSIRTs), it specifies that in the area of network and information system security, they are as follows:

1st CCN-CERT, of the National Cryptological Centre (CCN), which will be responsible for the reference community consisting of the entities considered essential or important in accordance with this Law that are included within the scope of Law 40/2015 of 1 October 2015.

2nd INCIBE-CERT, of the National Cybersecurity Institute of Spain, which will be responsible for the reference community consisting of the entities considered important in accordance with this Law and which are not included in the scope of Law 40/2015 of 1 October 2015.

3rd ESPDEF-CERT, of the Ministry of Defence Joint Cyberspace Command (*Mando Conjunto del Ciberespacio*), which will cooperate with CCN-CERT and INCIBE-CERT in situations where they need it to do so and, necessarily, in situations relating to incidents affecting the Ministry of Defence and entities with an impact on national defence, in which case they will coordinate with the Ministry any aspects liable to affect national defence, the Ministry of Defence or the operational readiness of the armed forces; without prejudice to the provisions of this article for incidents affecting critical entities.

However, for incidents involving entities classified as critical under Law xxxx, CSIRT-MIR-PJ (the cyber incident response centre of the Ministry of the Interior) of the Cybersecurity Coordination Office (OCC) will operate in conjunction with the relevant reference CSIRT.

- **Chapter III.**

Chapter III regulates cybersecurity risk-management measures and reporting obligations. This part provides for an individualised risk assessment by the different entities and details the specific actions that they should carry out to ensure and raise the security levels of their network and information systems and prevent the risk of incidents within the framework of the National Security Scheme and equivalent European and international technical standards.
On the other hand, institutions are required to report significant incidents that occur within their operations or in the provision of their services. In order to comply with the reporting obligations, the National cyber incident reporting and monitoring platform shall be made available to all actors involved, enabling technical information to be exchanged and incidents to be monitored.

Essential and important entities shall designate a person, unit or collegiate body as information security officer, to exercise the functions of point of contact and technical coordination with the National Cybersecurity Department and the reference national CSIRTs. This information security officer shall act as a point of contact with the National Cybersecurity Department for supervision of the security requirements for information networks and systems, and as a special point of contact for coordination of incident management with the reference national CSIRTs.

In terms of incident reporting, consideration is being given to the growing scale and sophistication of incidents, as well as the fact that they represent a serious threat to the functioning of network and information systems, potentially disrupting economic activities in the internal market and generating large financial losses, which can contribute to undermining users' confidence and cause major damage to the economy and society of the Union.

Given the above, a multi-stage approach to the reporting of significant incidents is advocated, in order to strike a balance between, on the one hand, agile reporting that reduces the possible spread of significant incidents and, on the other hand, thorough reporting that draws valuable lessons from each incident in order to improve cyber resilience, from individual entities right through to entire sectors.

In addition, the new Regulation advocates the establishment of single channels facilitating the communication of cyber incidents, thereby promoting implementation of the National cyber incident reporting and monitoring platform, which had already been included in the previous regulations, but is in the process of being finalised.

Cyber incident preparedness and effectiveness are therefore more essential than ever if the internal market is to function correctly.

- **Chapter IV.**

The main emphasis in Chapter IV is on imposing the obligation to create and regularly update a list of providers of cross-border digital infrastructure services.

The National Cybersecurity Department shall create and maintain a register containing a list of all such entities. To this end, the supervisory authorities shall require DNS service providers, top-level domain name registries, entities providing domain name registry services, cloud computing service providers, data centre service providers, content distribution network providers, managed service providers and managed security service providers, providers of online marketplaces, online search engines and social media service platforms, to submit certain information, as well as any changes thereto within 3 months of the date on which the change occurred.

- **Chapter V.**

At the same time, Chapter V enshrines the voluntary exchange of relevant information between entities, with the aim of strengthening the level of cybersecurity and preventing, detecting, responding to, recovering from or reducing the impact of incidents, as well as the reporting of incidents for which no reporting obligation is established to the reference national CSIRT.

- **Chapter VI.**

Chapter VI is dedicated to the regulation of supervisory and enforcement functions in respect of essential and important entities, as well as cross-border cooperation.

- **Chapter VII.**

This chapter provides for the penalties regime. It regulates disciplinary liability, powers to impose penalties, criteria for progressive penalties, the classification of offences, classified as very serious, serious and minor, the applicable penalties for each type of offence, the consequences for public authorities of committing offences, the limitation of offences and penalties, and the penalties procedure.

- **Additional provisions**

- One
  - Dedicated to the creation of the National Cybersecurity Department as the single national competent authority for cybersecurity.
- Two
  - Contains the regime applicable to the Bank of Spain, the European Central Bank and the European System of Central Banks, in accordance with the legislation in force.
- Three
  - Provides that the supervisory authorities and the reference national CSIRTs will inform the head of the Secretary of State for Economic Affairs and Business Support, through the General Secretariat of the Treasury and International Finance, of any incidents that might have significant impacts on the essential services of the financial system.
- Four
  - In relation to the National cyber incident reporting and monitoring platform, refers to the common platform provided for in Article 19(4) of Royal Decree-Law 12/2018 and developed by Article 11 of Royal Decree 43/2021.
- Five
  - Addresses the database of security incidents of a criminal nature, assigning responsibility for the processing of this database to the Directorate-General for Coordination and Studies of the Secretariat of State for Security.
- Six
  - Provides for the safeguarding of essential State interests and

functions, such that the obligations of the law will not involve providing any information whose disclosure would be contrary to the essential interests of Spain in terms of national security, public security or national defence.

- Seven
  - Provides that the State Secretariat for Digitalisation and Artificial Intelligence of the Ministry for the Digital Transformation and the Civil Service will represent Spain on the Administrative Board of the European Cybersecurity Industrial, Technology and Research Competence Centre, established by Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.
- Eight
  - Designates the national cybersecurity certification authority (*Autoridad Nacional de Certificación de la Ciberseguridad*).

o Transitional provisions

- One: Regulates communication obligations.
- Two: Addresses the register of entities. The National Cybersecurity Council, through the Permanent Cybersecurity Commission as a working group supporting the Council, chaired by the Department of National Security, will draw up the list of essential and important entities referred to in the law.
- Three: Regulates the transitional regime

o Repealing provision

Royal Decree-Law 12/2018 of 7 September 2018 on the security of information networks and systems, as well as Royal Decree 43/2021 of 26 January 2021 implementing Royal Decree-Law 12/2018 of 7 September 2018 on the security of information networks and systems, are repealed, with the exception of the National Cyber-incident Reporting and Management Instruction contained in its annex, which shall remain in force until expressly amended, replaced or repealed. Similarly, any provisions of equal or lower rank that are contrary to the provisions of this Law are repealed.

o Final provisions

- One: Relating to the title of competence.
- Two: Amends Article 2(9) and Article 3(2) of Law 5/2014 of 4 April 2014 on Private Security.
- Three: Empowers certain ministerial departments to develop the regulatory aspect of the Regulation.
- Four: Transposes the NIS2 Directive into Spanish law.
- Five: Envisages the entry into force of the Regulation.

2. Legal analysis.

2.1. Correlation table.

Below is a correlation table of the provisions of the NIS2 Directive and those of the preliminary draft organic law.

DIRECTIVE NIS2	PRELIMINARY DRAFT LAW
Article 1. Aim.	**Article 1.** Aim.
Article 2. Scope.	**Article 3.** Scope.
Article 3. Essential and important entities.	**Article 4.** Essential and important entities.
Article 4. Sector-specific Union legal acts.	
Article 5. Minimum harmonisation.	**Sixth additional provision.** Safeguarding of essential State interests and functions
Article 6. Definitions.	**Article 2.** Definitions
Article 7. National cybersecurity strategy.	**Article 5.** National cybersecurity strategy.
Article 8. Competent authorities and single points of contact.	**Article 6.** Competent authority. **Article 7.** Single point of contact.
Article 9. National cyber crisis management frameworks.	**Article 8.** National cyber crisis management framework.
Article 10. Computer security incident response teams (CSIRTs).	**Article 9.** Reference national computer security incident response team (CSIRT).
Article 11. Requirements, technical capabilities and tasks of CSIRTs.	**Article 10.** Requirements, technical capabilities and tasks of reference national CSIRTs.

Article 12. Coordinated vulnerability disclosure and a European vulnerability database.	**Article 11.** Coordinated vulnerability disclosure.
Article 13. Cooperation at national level.	**Article 12.** Cooperation at national level.
Article 14. Cooperation Group.	**Article 13.** Cooperation at European Union level.
Article 15. CSIRTs network.	**Article 13(3).** Cooperation at European Union level.
Article 16. European cyber crisis liaison organisation network (EU-CyCLONe).	**Article 13(2).** Cooperation at European Union level.
Article 17. International cooperation.	**Article 13.** Cooperation at European Union level.
Article 18. Report on the state of cybersecurity in the Union.	
Article 19. Peer reviews.	**Article 13(4).** Cooperation at European Union level.
Article 20. Governance.	**Article 14.** Governance.
Article 21. Cybersecurity risk-management measures.	**Article 15.** General cybersecurity risk-management measures.
Article 22. Union level coordinated security risk assessments of critical supply chains.	**Article 15(3).** General cybersecurity risk-management measures.
Article 23. Reporting obligations.	**Article 18.** Reporting obligations.
Article 24. Use of European cybersecurity certification schemes.	**Article 33.** Use of European cybersecurity certification schemes.
Article 25. Standardisation.	
Article 26. Jurisdiction and territoriality.	**Article 3.** Scope.
Article 27. Registry of entities.	**Article 26.** Registry of entities.
Article 28. Database of domain name registration data.	**Article 27.** Database of domain name registration data.
Article 29. Cybersecurity information-sharing arrangements.	**Article 28.** Cybersecurity information-sharing arrangements.
Article 30. Voluntary notification of relevant information.	**Article 29.** Voluntary notification of relevant information.
Article 31. General aspects concerning supervision and enforcement.	**Article 30.** General aspects concerning the supervision of essential and important entities.
Article 32. Supervisory and enforcement measures in relation to essential entities.	**Article 31.** Supervisory and enforcement measures in relation to essential entities.
Article 33. Supervisory and enforcement measures in relation to important entities.	**Article 32.** Supervisory and enforcement measures in relation to important entities.
Article 34. General conditions for imposing administrative fines on essential and important entities.	**Article 35 et seq.** Legal authority to impose penalties.

Article 35. Infringements entailing a personal data breach.	**Article 24.** Cooperation in terms of the incidents that affect personal data.
Article 36. Penalties.	**Article 40.** Penalties.
Article 37. Mutual assistance.	**Article 34.** Cross-border cooperation.

2.2. Periodic obligations contained in the Directive.

The Directive provides for a number of time frames and deadlines to be respected by all Member States, both for the transposition of the Directive into their respective domestic legislation and for the drawing up and submission of annual statistical reports that will serve as a basis for the Commission to inform the Parliament and the Council.

Article 41 sets 17 October 2024 as the deadline for transposition of the Directive.

Article 4 of the Directive provides that 'By 17 April 2025 and every two years thereafter, the competent authorities shall notify... the Commission and the Cooperation Group of the number of listed essential and important entities... for each sector and subsector referred to in Annex I or II; and the type of service that they provide...'.

It similarly provides that Member States should communicate their strategies and substantial updates thereof to the Commission. The Commission should prepare a summary report of the strategies communicated by the Member States to serve as a basis for exchanges in order to identify best practices and issues of common interest.

Article 9 provides that 'Within three months of the designation or establishment of the cyber crisis management authority, each Member State shall notify the Commission of the identity of its authority and of any subsequent changes thereto. Member States shall submit to the Commission and to the European cyber crisis liaison organisation network (EU-CyCLONe) relevant information relating to the requirements regarding their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans. Member States may exclude information where and to the extent that such exclusion is necessary for their national security'.

Article 10 provides that ‘Each Member State shall notify the Commission without undue delay of the identity of the CSIRT... [and] of their respective tasks in relation to essential and important entities’.

Article 16 provides that ‘By 17 July 2024 and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work’.

These communication obligations are included in the First transitional provision. Specifically, the National Cybersecurity Council shall, through the Department of National Security, by 17 April 2025, notify:

- The Commission and the European Union Cooperation Group of the number of essential and important entities for each sector and subsector referred to in Annex I or II; and

- The Commission of relevant information on the number of essential and important entities identified, the sector and sub-sector identified in Annex I or II to which they belong, the type of service they provide and the provision under which they were identified.

These notifications will then be updated every two years through the National Cybersecurity Department.

The National Cybersecurity Council, through the Department of National Security, after approval by the Permanent Cybersecurity Commission, shall notify the European Commission of the identity of its cybersecurity crisis management authority and any subsequent amendments thereto within three months of the entry into force of this Law. In addition, within three months of its adoption, it shall submit to the European Commission and the European cyber crisis liaison organisation network (EU-CyCLONe) the relevant information concerning the requirements of the Large-scale Cybersecurity Incident and Crisis Response Plan, being able to exclude information where and to the extent necessary for national security.

Likewise, the National Cybersecurity Council, through the National Security Department, after approval by the Permanent Cybersecurity Commission, shall notify

the European Commission without undue delay of the identity of the national reference CSIRTs designated pursuant to Article 10, and any subsequent changes to the notification.

3. Processing.

This Regulation is among those included in the Annual Regulatory Plan for 2024. The preliminary draft was drawn up after a long process of reflection.

The various management centres of the Ministry of the Interior have been actively involved in the preparation of the text.

A prior public consultation procedure was carried out between 21 September and 17 October 2023, provided for in Article 133 of Law 39/2015 of 1 October and in Article 26 of Law 50/1997 of 27 November, in which various comments were received from the following entities: Chamber of Commerce, Spanish Confederation of Business Organisations (CEOE), DigitalES, ESYS Foundation, Vodafone, Cotec and Ametic.

The various entities consider it positive to move forward on a common framework in relation to the cybersecurity of the Member States and provide specific observations aimed at: reinforcing the need to establish unified security standards and certification systems at European level; applying a risk-based approach prioritising supervisory tasks; and implementing supply chain security based on objective and non-discriminatory facts and criteria, clear and accurate incident reporting procedures and the existence of a one-stop shop for incident reporting. All these issues have been addressed in the preliminary draft that is being processed.

In accordance with the first paragraph of Article 26(5) of Law 50/1997 of 27 November 1997, a **report will be received** from the following Ministries:

- Ministry of Defence
- Ministry for the Digital Transformation and the Civil Service
- Ministry of Transport and Sustainable Mobility
- Ministry of Science, Innovation and Universities
- Ministry for the Ecological Transition and the Demographic Challenge
- Ministry of Industry and Tourism
- Ministry of Agriculture, Fisheries and Food
- Ministry of Territorial Policy and Democratic Memory

- Ministry of Health
- Ministry of the Presidency of the Government (Department of National Security).

In addition, a report must be obtained from:

- **The Ministry of Territorial Policy and Democratic Memory (Article 26(5)(6) of Law 50/1997 of 27 November 1997);**
- The Office of Coordination and Regulatory Quality (Article 26(9) of Law 50/1997 of 27 November 1997);
- The Spanish Data Protection Agency.

In addition, the mandatory opinion of the Council of State must be obtained.

Upon completion of these processes, the preliminary draft will be submitted to the Council of Ministers for approval as a draft law and subsequent presentation to the Congress of Deputies.

This Regulation is valid for an indefinite period and will enter into force one month after its publication in the Official State Gazette. This derogates from the general rule laid down in Article 23 of Law 50/1997 of 27 November 1997, according to which the validity of regulations imposing new obligations on natural or legal persons engaged in an economic or professional activity shall begin on 2 January or 1 July following their approval. However, the second paragraph of Article 23 itself provides for certain situations in which this general rule does not apply, such as where compliance with the deadline for transposition of a directive is required, as is the case in this Law.

4.- IMPACT ANALYSIS

4.1. Economic and budgetary impact.

4.1.1 Impact on prices

Essential and important entities must implement a series of appropriate and proportionate technical, organisational and security measures to ensure compliance with the law.

In this context, essential entities shall designate a person, unit or collegiate body

as security officer to exercise the functions of contact point and technical coordination with the National Cybersecurity Department and with the reference national CSIRTs. In the event that the information security officer is a collegiate unit or body, a representative natural person shall be designated, as well as a replacement for them who will assume their duties in the event of absence, vacancy or illness. Essential entities shall notify the National Cybersecurity Department of their designation of the Security Officer within three months of acquiring the status of essential entities. They shall also report any subsequent appointments and dismissals affecting their nomination within one month of their occurrence.

In essential entities, the person responsible for information security, their representative natural person if they are a collegiate body and their replacement, regardless of the technical capacity and training requirements, must obtain the status of accredited personnel within the framework of Organic Law 2/1986 of 13 March on Security Forces and Law 5/2014 of 4 April on Private Security and in the manner established by regulation. In the case of essential entities that are also considered critical under Law XXXXXXX, this obligation will be similarly extended to the rest of the cybersecurity personnel.

The measures included in the Regulation seek to improve network and information system security, entities' responses to cyberattacks and, as has been analysed, a governance framework is established, of which the information security policy is an essential piece. Similarly, the security requirements are reinforced with a list of measures, including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing and the effective use of encryption. Supply chain protection measures for key information and communication technologies are also strengthened.

In this context, the economic effort devoted to implementation of these security measures should be considered as an investment, since it generates positive returns as a result of reducing the impact of security incidents.

4.1.2 Impact on productivity.

The measures will have a positive impact on productivity. Enhanced appropriate and proportionate technical, organisational and security measures to guarantee security, along with more effective management of security incident risks, will reduce the adverse impact of these incidents on the services, resulting in higher productivity in

service provision.

4.1.3 Impact on employment.

The measures will have a positive effect on employment, since the obligations regarding human resources dedicated to network and information system security are being strengthened.

4.1.4 Impact on innovation

These appropriate and proportionate technical, organisational and security measures will have a positive effect on innovation. Affected entities must be able to prevent, protect against, respond to, resist, and recover from hybrid attacks, natural disasters, terrorist threats and public health emergencies.

4.1.5 Impact on consumers

The measures will have a positive impact on consumers. Increases in productivity and innovation in the provision of services will help to boost the markets of the different sectors concerned, resulting in an increase in consumer demand for these services.

4.1.6 Impact on European and other economies.

The measures will have a positive impact on the European economy. Given that the draft develops the national Regulation transposing 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, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148, whose objective is to adapt to the rapidly changing range of threats, with the adoption of measures to improve the network and information security systems of essential and important entities within the scope of the Regulation.

4.1.7 Impact on competition and market unity.

The draft has a neutral impact on competition on the various markets involved and complies with the provisions of Law 20/2013 of 9 December 2013 on guaranteeing market unity. On the other hand, the obligations on critical entities are defined according

to the principle of proportionality, with equal impact on all operators in each sector that meet certain criteria; specification of these criteria falls to the authorities in the relevant sector and scope.

4.1.8 Budgetary impact.

A) From an expenditure point of view.

- **Impact on entities (Annex 1)**

In order to assess the economic impact that transposition of the NIS2 Directive has on companies, a complex process has been carried out that is detailed below. First, an estimate was made of the number of entities obliged by the Regulation according to the data collected by the National Statistical Institute, together with the reports collected by the Secretariat of State for Security in the exercise of its functions as competent authority under RDL 12/2018, based on categorisation of the entities by number of employees.

Although, within the essential entities, a distinction was drawn between those that were within the scope of NIS1 (300) and those that were not (1 519); as a result of this process a total of 1 819 essential entities and 3 941 important entities were identified.

An estimate was then made (below), of the average cost for each entity of assuming obligations arising from the transposition of the NIS2 Directive, which was €179 562.50 for important entities, and €2 153 250.00 for essential entities.

However, taking into account that the NIS1 Directive transposed into our legal system by Royal Decree 43/2021 and repealed by NIS2 already imposed certain obligations on certain companies in the field of cybersecurity, which they were fulfilling, the starting point for implementation of NIS2 would not be zero, so work has been carried out to estimate this concept with the intention of applying it to the total cost calculation as a corrective index.

In this regard, the following average percentages for prior implementation of the NIS2 requirements have been identified according to the type of entity:

- Important entities: 27%
- Essential entities not previously regulated by NIS1: 48%
- Essential entities previously regulated by NIS1: 95%

Thus, once these percentages are applied to the average cost per entity, the amounts reflected in the corrected average cost per entity column are obtained.

In view of the above, and as a result of applying the correction indices shown in the table to the average cost, the figures shaded in grey in the last column have been obtained, representing a total of €2 249 696 603.13, which would be approximately the total cost of fully implementing the Regulation throughout the Spanish business world.

TYPE OF ENTITY	APPROXIMATE NUMBER OF ENTITIES	AVERAGE COST/ENTITY	%AVERAGE PREVIOUS IMPLEMENTATION OF REQUIREMENTS	CORRECTED AVERAGE COST/ENTITY	CORRECTED TOTAL COST
IMPORTANT	3 941	€179 562.50	27	€131 080.63	€516 588 743.13
ESSENTIALS NOT PREVIOUSLY REGULATED BY NIS1	1 519	€2 153 250.00	48	€1 119 690.00	€1 700 809 110.00
ESSENTIALS PREVIOUSLY REGULATED BY NIS1	300	€2 153 250.00	95	€107 662.50	€32 298 750.00
				TOTAL IMPLEMENTATION COST	**€2 249 696 603.13**

- **Impact on the Administration**
  - o Creation of the National Cybersecurity Department. (Annex 2)

With the approval of the preliminary draft Law transposing Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) into Spanish law, the creation of a National Cybersecurity Department is envisaged, the economic impact of which is as follows:

B) From the point of view of revenues.

The measures adopted will lead to additional revenue for the State, corresponding to the authorisations of the security officers as private security personnel, which are calculated in the section on administrative burdens.

4.1.9 Analysis of administrative burdens.

In essential entities, the person responsible for information security, their representative natural person if they are a collegiate body and their replacement, regardless of the technical capacity and training requirements, must obtain the status of

accredited personnel within the framework of Organic Law 2/1986 of 13 March on Security Forces and Law 5/2014 of 4 April on Private Security and in the manner established by regulation. In the case of essential entities that are also considered critical under Law XXXXXXX, this obligation will be similarly extended to the rest of the cybersecurity personnel.

Given the above, a cost will be incurred corresponding to the authorisation of the Information Security Officer as private security personnel, so the applicable charges listed below are estimated.

The amount is calculated using the model applied by the Directorate-General of Police for the directors and heads of security.

- Private security companies: fees applicable to processes and procedures relating to private security.
  - Authorisation of cybersecurity operators and cybersecurity directors: €97.23.

- Processes and procedures
  - Certification of documents: €3.92
  - Supplement for each page of the document to be certified: €1.95
  - Issuance of certification €23.34
  - Supplement for each extension page requiring certification €1.95

4.2. Gender impact

It does not have any impact on gender, given that its contents do not contain measures of any kind that could affect the equality of opportunity of women and men.

4.3. Impact on childhood and adolescence

It does not have any impact on children and adolescents as it does not regulate anything relating to that area.

4.4. Impact on the family

It does not have any impact on the family, as it does not regulate anything relating to that area.

4.5. Impact on the environment and climate change

Regarding the impact on climate change, incorporated into the Law on the Government, by final provision 5 of Law 7/2021 of May 20 2021 on climate change and energy transition, it is estimated that the impact that the preliminary draft will have on climate change in terms of mitigation and adaptation to it, sustainable use and protection of water and marine resources, the circular economy, including waste prevention and recycling, the prevention and control of air, water or soil pollution and the protection and restoration of biodiversity and ecosystems will be zero, complying with the principle of causing no significant harm.

4.6. Impact on data protection

This analysis is carried out following the criteria of the Spanish Data Protection Agency (AEPD) shared at its Regulatory quality in data protection (*Jornada de Calidad Normativa en Protección de Datos*) day event held on 23 May 2023.

The Regulation has a positive impact on the protection of personal data by regulating the matter, ensuring the protection of this fundamental right, in relation to the processing of personal data resulting from its application. Different types of data processing are envisaged and defined in the Regulation.

Given the scope of this Regulation and the effects it has on other legal provisions, an in-depth study has been carried out of its impact on data protection. In this regard, the depth and formality of this analysis is commensurate with the level of risk to, and interference with, the rights and freedoms of the persons concerned caused by the Regulation; in particular, the fundamental right to privacy, enshrined in Article 18.4 of the Constitution. Similarly, it is important to note that during the formal processing of the provision, a mandatory report will be requested from various bodies including the AEPD itself.

In this context, the purpose section of the preliminary draft sets out the objectives of laying down specific rules on information system security (which leads to guarantees for personal data) and establishing rules and obligations relating to the exchange of

information on cybersecurity.

The definitions contained in the standard also contain descriptions of concepts that affect or may affect personal data, such as networks and information systems, network and information system security, cybersecurity, quasi-incident, incident, registration of first-level domain names and data centre service.

Article 4 includes the obligation to submit a series of data to the supervisory authorities, including identifiers, therefore each of these authorities will have to create or incorporate this information into the corresponding internal processes.

In accordance with the content of Article 9(6), it is envisaged that national CSIRTs will be able to establish cooperative relationships with national computer security incident response teams in third countries, enabling effective, efficient and secure exchange of information, using the relevant information exchange protocols including the TLP protocol and personal data, although these actions will be carried out in accordance with EU data protection legislation.

As a relevant provision in the factor being analysed, Article 12 provides that the National Cybersecurity Department shall cooperate and collaborate with the bodies responsible, inter alia, for the protection of personal data.

The National cyber incident reporting and monitoring platform referred to in Article 19 will have the specific requisites applicable to personal data protection and will guarantee both the information and data security dimensions and the principle of transparency. This generates the obligation that each of its managers and users, according to their respective competences, develop the corresponding data processing.

The content of Article 24 is also very significant, as it lays down the obligations of the supervisory authorities in the event of an incident involving the transfer of personal data.

In the same way, a legal provision is enabled in Article 25 for the transfer of identifiers in the cases of notifications, management, analysis or resolutions relating to incidents, which limits the transfer to data processing that is strictly adequate, relevant and limited to what is necessary in relation to the purpose, of those indicated, that is pursued in each case. Including a list of cases in which this operation can be carried out.

Articles 26 and 27 require the transfer of certain personal data for inclusion in the registers of providers of digital services and infrastructure and in the domain name registration database.

As a specific and unique treatment, the fifth additional provision provides that the

Directorate-General for Coordination and Studies, of the State Secretariat for Security, will be the body responsible for processing the database of security incidents that are of a criminal nature. Thus, the data communicated will only be processed for the purposes set out in the Regulation, when they can be considered allegedly criminal.

When thus processing security incident data, at least the data relating to the identity of the persons, data identifying terminals and connectivity devices and the personal identity and contact data of the controllers, managers and users of the processing file may be processed.

The recipients of this data will be the criminal courts, the Public Prosecutor's Office and security forces and bodies, as well as other entities legally provided for, these also being responsible for processing the data communicated to them in accordance with the provisions of this Law.

The preliminary draft provides that the main legal basis of the processing, in accordance with its objective and purpose, is compliance with the provisions of Articles 11 and 13 of 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, without prejudice to the application to its processing of legislation governing the exercise of judicial power or such legislation as may apply.

On the other hand, the legal basis applicable to transfers of personal data to third countries or international organisations will comply with the provisions of Articles 43 to 47 of Organic Law 7/2021 of 26 May 2021.

All of this guarantees the principle of data minimisation and prior information for the interested parties regarding the conditions, rights and obligations associated with the processing, as well as the possible recipients of the data under the terms provided for in the law.

According to the purpose of the processing, the obligation to retain the data collected is established; for such time as is necessary to fulfil the purpose for which it was collected, under Article 8 of Organic Law 7/2021 of May 26 and, where appropriate, for the time necessary to address any responsibilities deriving from its processing before the competent administrative or judicial bodies. Once that retention period has elapsed, the data shall be deleted or redacted in such a way that it cannot be correlated with or used to identify the data subjects.

Exercise of the rights of natural persons subject to the Data Protection Regulation is guaranteed and requests associated with these rights will be answered by

the data controller under the terms established in Organic Law 7/2021 of 26 May 2021.

Should criminal proceedings be initiated as a result of the processing of personal data, the duty to provide information under the terms provided for in the Code of Criminal Procedure must be complied with.

It has been necessary to include the content of these provisions in the preliminary draft to take into account the case-law of the Constitutional Court and the recommendations of the Spanish Data Protection Agency.

The Regulation includes a limitation on the rights of the persons concerned, although it complies with the provisions of Article 23 of the General Data Protection Regulation (GDPR), Article 15 of Directive 680/2016 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and Article 24 of Organic Law 7/2021 of 26 May 2021, by respecting the essence of fundamental rights and freedoms and being a necessary and proportionate measure in a democratic society to safeguard State security, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including protection against and the prevention of threats to public security.

The Regulation includes the minimum provisions contained in paragraph 2 of each of the aforementioned Articles 23 and 15 (of the GDPR and Directive respectively).

Similarly, the provisions of the Regulation are developed in accordance with the opinion of the Constitutional Court (STC 76/2019 of 22 May 2019, published in Official State Gazette No 151 of 25 June 2019 and with ECLI:ES:TC:2019:76) whereby any legal provisions entailing interference with the fundamental right to the protection of personal data, especially in the case of special category data, must: specify what essential public interest justifies restriction of the right and the need to process the personal data; thoroughly regulate any interference with the fundamental right by establishing clear rules on the scope and content of the data processing that it authorises; establish appropriate safeguards in respect of any collection of personal data that it authorises, without being able to defer legal regulation of the personal data processing concerned to a later time, or to refer to the General Data Protection Regulation, Organic Law 3/2018 of 5 December 2018, on the Protection of Personal

Data and Guarantee of Digital Rights or any of the special laws regulating the protection of this right, such as Organic Law 7/2021 of 26 May 2021.

For its part, the Spanish Data Protection Agency (Reports 0074/2020, 0077/2020 and 0041/2022) indicates that laws involving the creation of data processing, since that data is in a special category, cannot refer generically to submission to the Data Protection Regulation, but must include specific provisions concerning the purpose, the person responsible, the basis of legitimacy, the legal motivation for collecting the data in the special category, compliance with the principles of processing, the basic form of access to the data, the rights of the persons concerned and their guarantees of exercise thereof.

In summary, the Regulation includes the following provisions:

Generally speaking, the Regulation clearly identifies the bases of legitimacy and the end purposes of the different types of processing.

Similarly, for each specific operation or processing, assessments of appropriateness, necessity and proportionality have been taken into account. In accordance with recital 4 of the GDPR, it should be noted that the processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality The draft respects all fundamental rights; in particular the protection of personal data.

Having analysed, in general, the risk to the rights and freedoms of citizens, it should be noted that the obligations, duties and prohibitions contained therein that might affect data protection rights have been balanced by mitigation provisions to keep this risk at an appropriate level.

The Regulation is legally consistent with the regulatory framework for data protection, since its provisions are formulated according to the content of those that are applicable.

Specifically:

- The persons responsible for each processing action and other parties involved have been identified.
- The operations and purposes of the processing actions are described.
- The bases of legitimacy of the processing can be clearly identified.
- Where possible and necessary, the categories of data subjects are identified.
- They can be processed, but the purpose of the Regulation is not to collect data

on vulnerable persons, in particular children, or which affects a large number of people.

- The personal data processed is appropriate, relevant and limited to what is necessary.
- The recipients of each processing action have been checked and the regulatory conditions for these operations have been met.
- No international data transfers are made; if they take place, they must be adapted to the appropriate conditions.
- Given the level of the Regulation and its purpose, data exchanges do take place between competent authorities at EU level.
- There are no fully automated decisions that harm the individuals concerned, nor any profiling.
- The Regulation requires technical and organisational security measures to be adopted for each processing action, that appropriately reflect the level of risk.
- There are no proformas in them.

4.7. Impact with regard to equal opportunities, non-discrimination or access for persons with disabilities.

The draft Regulation has no impact on equal opportunities, non-discrimination and accessibility for persons with disabilities, as it does not provide for measures affecting these matters.

5. EX POST EVALUATION.

This draft legislation will not be subject to ex post evaluation because the circumstances justifying its ex post evaluation, as provided for in Article 28(2) of Law 50/1997 of 27 November 1997, the Government, and Article 3 of Royal Decree 286/2017 of 24 March regulating the Annual Regulatory Plan and the Annual Regulatory Evaluation Report of the General State Administration and creating the Regulatory Planning and Evaluation Board, have not been met.