ADIGITAL'S CONTRIBUTION TO THE TRIS PROCEDURE ON THE PRELIMINARY DRAFT LAW ON CYBERSECURITY COORDINATION AND GOVERNANCE

On February 21, the Spanish Government notified the European Commission of the Preliminary Draft Law on cybersecurity coordination and governance (hereafter referred to as draft law) in compliance with the TRIS (Technical Regulation Information System) procedure. The main objective of the draft law is to transpose the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) into Spanish law. The draft text had been previously submitted to a public information process by the Spanish Ministry of Interior, from January 16 to February 10.

The TRIS procedure, established by Directive 2015/1535, introduces the obligation for Member States to notify the Commission of technical regulations related to information society products and services prior to their adoption, to ensure that these are compatible with European Union law, and they do not create any barriers for the proper functioning of the internal market.

From the date of notification, a standstill period of three months is opened, during which the European Commission and the Member States can examine the text of the notified draft and make contributions if they consider so. Furthermore, during this period, the Member State that has notified the draft cannot adopt it. In the case of this draft law, the standstill period ends on May 26.

Adigital, the Spanish Association of Digital Economy, appreciates the opportunity to provide input to this TRIS procedure.

COMMENTS ON POTENTIAL BARRIERS FOR THE INTERNAL MARKET

In the following paragraphs, we highlight a series of aspects of the draft law that at Adigital we consider can hinder the proper functioning of the internal market, and go against the spirit of the NIS2 Directive.

On the identification and compliance with general cybersecurity risk-management measures and the predominance of the Spanish Security Scheme

Article 15.2 of the draft law establishes that: "*The security measures referred to in the preceding paragraph shall be based on those provided for in both the National Security Scheme and equivalent European and international technical standards*". Additionally, the same article states: "*In the case of entities subject to Royal Decree 311/2022 of 3 May 2022, the corresponding National Security Scheme Specific Compliance Profile for essential and important entities will certify compliance with the cybersecurity risk-management measures of this regulation. The same shall apply to those essential or important entities that are not subject to Royal Decree 311/2022 and which voluntarily obtain a satisfactory assessment vis-à-vis the National Security Scheme Specific Compliance Profile*".

The Spanish "National Security Scheme" *(Esquema Nacional de Seguridad*, ENS) is a local Spanish technical standard. The objective for its development and adoption in Spain is to ensure an adequate level of cybersecurity in the Spanish public sector entities and to certain of their direct suppliers, as well as for the Spanish critical entities.

The fact that the cybersecurity measures that the National Cybersecurity Centre will determine as per Article 15.1 will be based primarily and predominantly on the ENS **contravenes the principle set forth by the Article 21.1 of the NIS2 Directive** that reads "*taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation (…)*", which makes an emphasis on leveraging "*European and international*" standards as a basis for the cybersecurity measures.

The primary and predominant use of the ENS for such measures will lead to:

- additional internal market fragmentation;
- barriers to entry into business in the local state;
- additional costs of implementation.

Furthermore, the draft law seems to imply that the National Cybersecurity Centre will develop yet a new and additional set of cybersecurity measures, resulting of the mix of the ENS and other standards. **This will lead to an additional burden on entities, who will need to examine and demonstrate compliance to this new set of local measures, as well as to market fragmentation.**

Along the same line, as for the article 15.4 of the draft law, essential entities are required to become certified to demonstrate compliance to the cybersecurity measures. European and international standards are again placed in a secondary position while favouring the ENS as the

unique mechanism recognised to demonstrate compliance to the cybersecurity measures. On top, per the writing of article 15.4 of the draft law, essential entities will be required to become certified to the ENS standard concurrently and together with whatever other international standards the National Cybersecurity Centre determines of its convenience. The option of becoming certified to the ENS **or** other European or international standard is not allowed by the draft law.

Given the fact that the ENS is already established in Spain, it is only fair that, for public and private entities who have already invested in implementing the cybersecurity measures it puts forth and/or getting certified to this local standard, the draft law allows such certification to be a proof of compliance to the cybersecurity measures. However, **it is not fair, nor does it follow the spirit of the NIS2 Directive, for the ENS to be the primary choice both to develop the cybersecurity measures and to demonstrate compliance to them** (for the later matter the ENS is furthermore the only explicitly recognized mechanism in the Law).

It is hence proposed for the draft law to clearly specify in Article 15.2 that **the cybersecurity measures will be determined favouring and firstly based on European and international standards**, leaving the option of the ENS for entities who have already invested in it, or for whom it provides added business value due to the nature of their presence in the Spanish market. Moreover, **the draft law must recognize that certifications to existing international standards, such as ISO 27001, are a valid mechanism to demonstrate compliance** to the cybersecurity measures put forth by NIS2 Directive and referred to in Article 15.1 and 15.2 of the draft law.

On cybersecurity risk-management measures for cross-border entities

In compliance to Article 21.5 of the NIS2 Directive, the Commission adopted in October 2024 an Implementing Regulation laying down the technical and methodological requirements for certain entities — known as cross-border entities —, as, given the nature of their operations, they require a higher level of harmonization at Union level (NIS2 Directive recital 84). Such cross-border entities are the ones referred to in the article 26.1 of the Spanish draft law.

Nevertheless, article 15.6 of the draft law only refers to requiring such cross-border entities to adequately apply the Implementing Regulation, but does not clearly specify that for those entities, those are the actual technical and methodological requirements to be implemented.

For cross-border entities, the business value added of certifying cybersecurity measures on the ENS is none, given the fact that the ENS certification is not a recognized certification or standard in other EU countries, let alone outside the EU. **Obliging cross-border entities to certify according to the ENS hinders substantially the competitiveness within the EU and outside the EU of such cross-border entities**, adding an administrative burden on them for the demonstration of compliance against their local authority. Therefore, the draft law must make it clear that **cross-border entities must apply the technical and methodological requirements set forth by Implementing Regulations per Article 21.5 of NIS2 Directive rather than any others determined locally by Spanish authorities**.