Message 001

Communication from the Commission - TRIS/(2025) 0503

Directive (EU) 2015/1535

Notification: 2025/0104/ES

Notification of a draft text from a Member State

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx il-perijodi ta’ dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20250503.EN

1. MSG 001 IND 2025 0104 ES EN 21-02-2025 ES NOTIF

2. Spain

3A. Subdirección General de Asuntos Industriales, Energéticos, de Transportes y Comunicaciones y de Medioambiente
DG de Mercado Interior y Otras Políticas Comunitarias
Ministerios de Asuntos Exteriores, UE y Cooperación
d83-189@maec.es

3B. Ministerio del Interior

4. 2025/0104/ES - SERV - INFORMATION SOCIETY SERVICES

5. Preliminary Draft Law on Cybersecurity Coordination and Governance

6. Digital services considered essential for the security and functioning of society

7.

8. This legislation aims to establish measures to achieve a high common level of cybersecurity in Spain and contribute to the cybersecurity of the European Union by transposing into Spanish law 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.

The law will affect public and private entities in essential and important sectors, such as energy, transport, banking, health, water, digital infrastructure, and technological services.

The main measures included in the draft are:
- Establish the National Cybersecurity Centre, which will coordinate cybersecurity actions and ensure cross-sectoral and cross-border cooperation.
- Define uniform criteria for determining the entities that are included in the scope, classified as essential entities and important entities.
- Establish a catalogue of measures necessary for the management of cybersecurity risks.
- Strengthen the procedure for notifying incidents that disrupt, or are likely to disrupt, the provision of services by essential and important entities.
- Create the position Information Security Officer.
- Strengthen the rules on the exchange of cybersecurity information.
- Establish an institutional and coordination framework between the competent authorities.

9. The main objective of the Preliminary Draft Law on Cybersecurity Coordination and Governance is to strengthen the protection of networks and information systems in Spain, which are essential for the development of social and economic activities. The increasing number, magnitude and sophistication of cyber incidents pose a serious threat to the functioning of these infrastructures, which can disrupt economic activities, undermine user confidence and cause major damage to the national economy and security.

To address these challenges, the law proposes the establishment of the National Cybersecurity Centre, which will coordinate cybersecurity actions and ensure cross-sectoral and cross-border cooperation. In addition, the measures of Directive (EU) 2022/2555 (NIS-2), aimed at contributing to a high common level of cybersecurity across the Union, will be incorporated into the Spanish legal system.

The law will affect public and private entities in essential and important sectors, such as energy, transport, banking, health, water, digital infrastructure, and technological services, obliging them to implement state-of-the-art security measures and to notify any significant cybersecurity incidents.

10. References to basic texts:

11. No

12.

13. No

14. No

15. Yes

16.
TBT aspects: No

SPS aspects: No

****

European Commission
Contact point Directive (EU) 2015/1535
email: grow-dir2015-1535-central@ec.europa.eu