VIEIRA DE ALMEIDA

INFORMATION, COMMUNICATION & TECHNOLOGY

REGULATION OF THE LEGAL FRAMEWORK FOR CYBERSPACE SECURITY

VdA EXPERTISE

August 2021

The regulation of the Cyberspace Security Legal Framework was published, with impact on operators of critical infrastructures and essential services, digital service providers and the Public Administration

The long-awaited Decree-Law no. 65/2021 (only available in Portuguese) came into force on the 9th of August 2021, regulating the Cyberspace Security Legal Framework (Law no. 46/2018, only available in Portuguese) and defining cybersecurity certification obligations, in implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council.

This Decree-Law addresses several questions that were unsolved by Law no. 46/2018, establishing, for the covered entities, **demanding obligations** regarding:

- **security requirements of networks and information systems**; and
- **requirements for reporting incidents** affecting the security of network and information systems.

Critical infrastructure operators (public or private entities operating a critical infrastructure), **operators of essential services** (in the energy, transport, banking and finance, health, water and digital infrastructure sectors), **digital service providers** (e-commerce, online search engines and cloud computing) and **Public Administration** entities must meet the established requirements. In particular, the security requirements applicable to digital service providers are defined by an implementing regulation of the European Commission.

Non-compliance with the established obligations is punishable as follows:

- **Very serious** infringements → fines ranging, for legal persons, from **€25.000** to **€50.000** (in the event of failure to comply with obligations relating to security requirements)
- **Serious** infringements → fines ranging, for legal persons, from **€9.000** to **€3.000** (in the event of failure to comply with notification obligations)

The **Decree-Law** also allows the implementation of a **national cybersecurity certification framework** by the **CNCS** (National Cybersecurity Centre), which will act as the National Cybersecurity Certification Authority. The CNCS will establish the necessary provisions for the development and implementation of specific cybersecurity certification schemes for information and communication technology products, services and processes.

The requirements set out in Decree-Law 65/2021 constitute a minimum to be ensured by the entities covered, without prejudice to the rules that, depending on the nature of the entities and the sectors in which they operate, may be established by other authorities, nor provisions resulting from other legislations (as is the case of the obligations applicable to digital service providers). The CNCS may also issue complementary technical instructions regarding security requirements and incident notification.

The **densification of cybersecurity obligations**, which is presented **in the next page of this Flash**, seeks to ensure a high level of security of the networks and information systems that support the use of increasingly disruptive technologies (such as Artificial Intelligence or the Internet of Things), so that it takes place in an environment of trust. It is undeniable that the fulfilment of cybersecurity obligations will not only enable legal compliance by organisations, but will also provide them with significant reputational and behavioural benefits.

It is therefore imperative that organisations start preparing their systems and teams as soon as possible for the implementation of this new regime, becoming more resilient to the internal and external threats affecting cyberspace and avoiding the application of severe fines.

Main obligations

Briefly, it is foreseen that the entities covered:

Permanent contact point **	Appoint a permanent contact point, in order to ensure the flow of information with the CNCS both at an operational and technical level.
Security officer **	Appoint a security officer to manage all the measures taken regarding security requirements and incident reporting.
Asset inventory *	Draw up and keep updated an inventory of all the **assets essential** for the provision of the services, with information defined in technical instructions issued by the CNCS. The inventory must be signed by the security officer and communicated to the CNCS.
Security plan **	Draw up and keep updated a security plan, duly documented and signed by the security officer.
Annual Report *	Prepare an annual report, with information about the activities developed in terms of security and the security incidents that have occurred, which must be sent to the CNCS in January of each year and signed by the security officer.
Security measures ***	Adopt technical and organisational measures to manage the risks posed to the security of the networks and information systems used by them, in line with the risk analysis conducted and taking into account latest technical developments, using internationally accepted technical standards and specifications.
Risk analysis ***	Carry out and document a risk analysis on all the assets that guarantee the continuity of the operation of the networks and information systems and/or guarantee the provision of services (depending on the entities in question). This analysis may be of **global or partial scope**, in accordance with the requirements and periodicity foreseen by law.
Incident notification**	Notify the CNCS of the occurrence of incidents with a relevant or substantial impact. For each incident that must be notified, the entity must submit: (i) an **initial notification**, (ii) a **notice of end of impact**, relevant or substantial, and (iii) a **final notification**, with specific deadlines provided by law. These notifications shall be articulated with the notifications of personal data breaches under the GDPR, as well as with other notifications to sectoral regulators.

* Obligation currently applicable
** Obligation applicable from November 2021
*** Obligation applicable from August 2022

Contacts

MAGDA COCCO
MPC@VDA.PT

INÊS ANTAS DE BARROS
IAB@VDA.PT

HELENA CORREIA MENDONÇA
HCM@VDA.PT

MARIA DE LURDES GONÇALVES
MLG@VDA.PT