Transposition of the NIS 2 Directive: Cybersecurity Legal Framework

Practical Guide

Transformative Legal Experts

PLMJ

Contents

On 4 December, Decree-Law 125/2025 was published, establishing the new legal framework for cybersecurity (the "Cybersecurity Legal Framework" or "CLF"), following its approval by the Council of Ministers and subsequent promulgation by the President of the Republic.

The decree transposes Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union ("NIS 2 Directive"), thereby strengthening the national capacity to prevent and respond to cyber threats.

The long-awaited Cybersecurity Legal Framework clarifies the obligations of each covered entity. It also defines the processes for implementing and improving information security management systems, which can now be implemented in compliance with the obligations arising from the transposition.

This practical guide provides information on the most important changes to the new Cybersecurity Legal Framework.

1. What is the NIS 2 Directive?

Directive (EU) 2016/1148 of 6 July 2016 (the NIS Directive) was the EU's first comprehensive law to address new cybersecurity challenges and it represented a significant milestone in the development of the EU's cybersecurity resilience and cooperation. Prior to its introduction, there was no unified approach to improving cybersecurity, leaving it to individual companies to determine their own implementation strategies.

The NIS Directive was implemented in Portugal through the transposition of Law 46/2018 of 13 August (the "Legal Framework for Cyberspace Security"). Law 46/2018 was supplemented by Decree-Law 65/2021 and Regulation 183/2022, which provide technical instructions on communication and information relating to permanent contact points, security officers, asset inventory, annual reports, and incident reporting.

▲ RETURN HOME

However, the evolving threat landscape and the need to strengthen companies' preventive activities and cooperation between Member States on cybersecurity required an updated version of the original NIS Directive, adapted to the current scenario, hence the NIS2 Directive.

In face of a significant increase in digital threats, the NIS 2 Directive (Directive (EU) 2022/2555) establishes a European legal framework for cybersecurity. It aims to increase the resilience of critical and essential infrastructure against cyber threats. In Portugal, the transposition of this directive:

- Reflects the increasing sophistication of cyber threats, which are becoming more frequent and complex.
- Strengthens national security by protecting strategic and critical sectors.
- Harmonises measures at the European level, ensuring uniformity and collaboration between Member States.

The NIS 2 Directive expands the list of entities covered and introduces stricter requirements to prevent and mitigate cybersecurity incidents.

2. What are the CLF's objectives, and what changes will it bring?

The previous cybersecurity legislation applied to operators of essential services, critical infrastructure operators, digital service providers, and civil servants. The legislation's main objectives were to (i) adopt appropriate security measures to manage risks to networks and information systems, (ii) define clear criteria and deadlines for reporting significant cyber security incidents to national authorities, and (iii) promote information exchange and cooperation between EU member states and between the public and private sectors. While the new Cybersecurity Legal Framework shares certain similarities with its predecessor, it introduces new features and greater rigour for the entities involved.

The following changes stand out in the Cybersecurity Legal Framework:

- The extension of its personal scope of application to both new sectors and sectors existing under the old legislation[1].
- The role of the National Cybersecurity Centre ("CNCS") in regulation and supervision.
- The distinction between obligations and supervision based on entity size, business, and level of risk exposure.

The clarification of a set of minimum information security measures to be adopted by covered entities, although they may opt for stricter measures.

The proposed legal framework is guided by the principle of proportionality, balancing the costs of implementing and maintaining information systems with the associated risk level of the sector, entity, or business type. All entities must implement the same information security and cybersecurity risk management measures, ensure senior management accountability, and report cybersecurity incidents. However, the most visible difference in the application of the principle of proportionality is in the supervision by the CNCS. Essential entities will be subject to both ex ante and ex post supervision (before and after a significant incident). Important entities, on the other hand, will only be subject to ex post supervision. Essential entities will undergo regular, specific, and ad hoc audits, whereas important entities will only undergo specific audits. Additionally, fines resulting

1 See Article 3.

from administrative offences established in the Decree-Law vary depending on whether they are applied to essential or important entities. Important entities generally have a smaller size and turnover than essential entities, and are generally exposed to a lower level of risk. Therefore, the proportionality of the fines reflects the legislature's intention to prevent the current Cybersecurity Legal Framework from economically strangling small and medium-sized businesses.

Furthermore, it encourages information sharing and cooperation between public and private entities to promote a coordinated response to cybersecurity incidents, aiming to strengthen the resilience of Portugal's business sector.

3. What entities are covered?

The CLF divides these entities into four main categories:

ESSENTIAL ENTITIES

These correspond to entities that are not SMEs[2] and are referred to in Annex I of the Decree-Law (critical sectors), or to entities referred to in Article 6(1):

- Qualified trust service providers, top-level domain name registrars, and domain name system service providers.

- Medium-sized enterprises that offer public electronic communications networks or publicly available electronic communications services.

- Public administration entities whose responsibilities include providing services in the development, maintenance and management of information and communication technology infrastructure. This also includes entities that have a particularly high degree of digital integration in the provision of their services, as well as the public entity responsible for educational assessment.

- Entities identified as critical under Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022.

- Any entity listed in Annexes I or II of the Decree-Law that is classified as essential based on its degree of exposure to risks, size, and the likelihood and severity of incidents occurring, including their social and economic impact:

a) The entity is the sole provider of a service essential for maintaining critical social or economic activities (such as those identified in Annexes I and II).

b) Disruption to the service it provides could significantly affect public safety, security, or health.

c) Disruption to the service it provides could generate significant systemic risks, including disruptions with a cross-border impact.

d) The entity is critical due to its specific importance at a national or regional level for the relevant sector or type of service, or for other interdependent sectors.

Examples of critical sectors include energy, transport (road, rail, air, and sea), health, water (drinking and wastewater), digital infrastructures, financial market infrastructures, credit institutions, ICT management, and space (see Annex I).

2 Article 2 of Annex III provides that the SME category consists of companies that employ fewer than 250 people, with an annual turnover of no more than €50 million and an annual balance sheet total of no more than €43 million.

IMPORTANT ENTITIES

This residual category comprises entities referred to in Annex I that are not considered essential.

Other critical sectors (See Annex II) include postal services, chemical production and distribution, waste management, food production and distribution, manufacturing (including the production of medical, computer and electrical equipment, as well as automotive and other transport equipment), digital service providers, and research institutions.

Other critical sectors include postal services, chemical production and distribution, waste management, food production and distribution, manufacturing, digital service providers, and research institutions.

KEY PUBLIC ENTITIES

These are divided into Group A[3] and Group B[4] and include public administration bodies that impact the provision of essential services.

Relevant public entities are subject to supervisory measures proportionate to their group, with specific obligations to be defined by CNCS regulation.[5]

ENTITIES REGARDLESS OF NATURE OR SIZE

The law excludes small and microenterprises from its scope, except in the following cases:

- The entity concerned is one of the following:

a) A provider of public electronic communications networks or a provider of publicly available electronic communications services.

b) A trust service provider.

c) A top-level domain name registry, a domain name registration service provider, a domain name system service provider.

- The entity is the sole provider of a service essential for maintaining critical social or economic activities.
- Disruption to the service it provides could significantly affect public safety, security, or health.
- Disrupting the service it provides could lead to significant systemic risks, particularly in sectors where such disruption could have a cross-border impact.
- The entity is critical due to its specific importance at a national or regional level for the relevant sector or type of service, or for other interdependent sectors[6].
- The entity is identified as a critical entity in accordance with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022[7].
- Higher education institutions[8].

3 See Article 7(2), Group A entities include direct and indirect state administration services with 250 or more employees, for example.
4 See Group B entities are defined in Article 7(3) and include direct or indirect state administration services with between 75 and 249 employees.
5 Article 33.
6 Article 3(2).
7 Article 3(5).
8 Article 3(6).

4. What is the difference between the classification and registration requirements?

Although complementary, classification and registration have distinct functions and must both be submitted by entities to which the CLF applies. This will be done through an electronic platform created by the CNCS for this purpose.

Qualification[9] involves entities covered communicating their existence and classification under the legislation. This procedure must be completed **within 30 days of commencing activity. For entities already operating on the date the CLF comes into force, this must be completed within 60 days of the platform becoming available.** Qualification allows the CNCS to confirm whether an entity is covered by the CLF and which category it falls into, thereby defining its obligations. These classifications are reviewed at least every two years or whenever relevant changes occur.

The CNCS must substantiate the classification process, and entities subject to classification are entitled to a prior hearing. Once an entity has completed the classification process, the CNCS has a maximum of 30 days to notify the entity.

The CNCS may also reclassify the entity if it finds that the situation does not correspond to the original declaration. In such cases, the decision must be justified and the entity must be given the right to a prior hearing.

Where an entity falls into more than one classification category, the most demanding rules apply to manage the risks to the security of networks and information systems[10].

Failure to meet classification deadlines, the omission of mandatory information, or the provision of inaccurate information may result in warnings, binding instructions (including orders to adopt preventive or corrective measures, and to correct infringements), audits, and fines. Furthermore, lack of classification does not exempt an entity from the obligations applicable under the CLF framework, i.e. the fact that there has been no classification process does not remove the obligations applicable depending on the framework of the entity in question under the CLF.

Once classification is complete, the obligation to register and update data in a timely manner begins permanently. This serves as the basis for reporting incidents and supervisory action[11].

Entities must provide information that allows them to be fully identified, including their name, tax identification number, address, and up-to-date contact details. They must also provide information on the designated responsible persons (including the Cybersecurity Officer), the permanent contact point and the sectors and EU Member State(s) in which they operate. Registration serves as a basis for reporting incidents, facilitates supervision by the CNCS, and enables a faster response when necessary. While qualification is an initial and one-off step, registration represents a permanent obligation to update information and be transparent with the CNCS.

Failure to meet classification deadlines, the omission of mandatory information, or the provision of inaccurate information may result in warnings, binding instructions, audits, and fines.

9 Article 8.
10 Article 9.
11 Article 35.

In addition, specific service providers – including those offering cloud computing services, data centres, managed services, online marketplaces, and social networking platforms – must register additional information. In these cases, entities must provide the address of their main establishment in the EU. If they are not established in the EU, they must provide the details of their designated representative instead. They must also provide contact details and a list of the EU Member States in which they operate, as well as their IP address ranges.

Any changes to this registered information must be reported within 30 working days, except for the aforementioned service providers, who have a three-month update period.

5. Which cybersecurity measures are required?

These measures vary according to the entity's category and are mainly directed at essential and important entities[12], including:

- Identification and mitigation of relevant cybersecurity risks.
- Supply chain security, through the assessment and management of risks associated with the entity's direct suppliers and service providers.
- Information security policies and procedures, particularly those related to cybersecurity training, backup management, access management, asset management, incident handling, and business continuity in the event of an incident.
- The appointment of responsible persons, including an internal cybersecurity officer and a permanent single point of contact who collaborates directly with the CNCS[13].
- Contingency and recovery plans to ensure operational continuity.
- Cybersecurity certification, as defined by the CNCS (see Article 34).

The cybersecurity measures applied to relevant public entities will be approved by CNCS regulation, as provided for in Article 33.

The CNCS will define the minimum and specific cybersecurity measures and compliance levels to be adopted by essential and important entities through specific regulations to be approved by the CNCS. These entities must also assess and manage 'residual risk' and adopt appropriate and proportionate measures to respond to these risks.

12 Article 27
13 Articles 31 and 32.

▲ RETURN HOME

6. What are the obligations of senior management?

In contrast with the Legal Framework for Cyberspace Security, the legislation that transposed the now repealed Directive, the CLF increases the responsibilities, functions, and obligations of operational, executive, and administrative management bodies[14], as well as the Cybersecurity Officer[15]. By making this change, overlaps or gaps in accountability among the various stakeholders are avoided, and legal certainty is provided regarding the role of these key figures within the entities covered This clarification is particularly relevant given that the CLF innovates in relation to its predecessor by providing for the liability of operational, executive and administrative management bodies for intentional or grossly negligent actions or omissions that infringe the provisions of this new legal framework.

The operational, executive, and administrative management bodies of essential and important entities play a crucial role in implementing and overseeing cybersecurity policies. They are responsible for specific duties set out in the current legal framework. Their main obligations include approving and supervising cybersecurity risk management measures, and ensuring regular cybersecurity training and awareness activities.

The functions and responsibilities of these bodies may not be delegated, except to another member of the same body.

The Cybersecurity Officer – who may be a member of one of these bodies or report directly to them – has the following functions:

- Proposing the implementation of certain cybersecurity risk management measures.
- Providing information and support to other top management bodies to help them maintain and comply with the proposed and implemented cybersecurity risk management measures.
- Contributing to the promotion of a cybersecurity culture, together with other bodies, namely through cybersecurity training and awareness-raising activities.
- Ensuring the management of residual cybersecurity risks.
- Ensuring compliance with the obligation to submit the annual report to the CNCS.
- Coordinating the actions of the permanent contact point in all matters within its remit.

For essential and important entities belonging to the same business group, a representative can be appointed in each company to liaise on cybersecurity matters under the supervision of a group-wide Cybersecurity Officer.

7. How does incident reporting work?

Entities must assess incidents based on specific parameters[16], including:

- The number of users affected by the service disruption.
- The duration of the incident.

14 Article 25(1).
15 Article 31(2).
16 Article 40.

- The severity of the disruption to service operations.

Incident reporting is divided into three main phases[17]:

INITIAL NOTIFICATION AND UPDATING

This must be sent to the CNCS within 24 hours of a significant incident being detected and must include preliminary information on its impact and the measures taken.

If justified and if the incident is still significant, the entity must send an update to the CNCS within 72 hours of verifying the incident.

NOTIFICATION OF THE END OF THE SIGNIFICANT IMPACT:

This must be done within 24 hours of confirmation of the end of the significant impact and must include a description of the situation, details of the measures taken to resolve the incident, and an update of the information provided in the initial notification.

FINAL AND INTERIM REPORT

These must be sent to the CNCS within a maximum of 30 working days of notifying the end of the significant impact. They must detail the causes, impacts, corrective actions, and preventive measures taken.

In addition, the CNCS may request information from the public in cases of significant incidents, to increase transparency and protect users.

The CLF also stipulates that entities must comply with the thresholds and technical criteria defined by the CNCS, although these have not yet been published. The current National Cybersecurity Framework requires organisations to define impact levels for risk management, considering factors such as the classification of information assets, security breaches, financial impact, disruption to plans, and reputational damage.

Incidents must be reported via an electronic platform created by the CNCS. Updates to the platform are being considered to enable coordinated communication between the CNCS, sector-specific cybersecurity authorities and other designated bodies, such as the Public Prosecutor's Office and the National Data Protection Commission. However, the implementation of this coordinated platform is pending the formalisation of an inter-agency protocol.

8. What is the role of the CNCS, and how does it coordinate with other entities?

As the national cybersecurity authority, the CNCS has a range of responsibilities, including:

- Coordinating responses to national and international incidents.
- Supervising compliance with cybersecurity obligations.
- Acting as the single point of contact for the EU in the context of the NIS 2 Directive.
- Drafting technical regulations, including the National Cybersecurity Reference Framework.

17 See Section II, Articles 40 et seq.

Its expanded role will include overseeing the implementation of the National Cybersecurity Strategy, coordinating responses to large-scale incidents, and ensuring compliance with the National Cybersecurity Reference Framework.

9. How do the Response Teams work?

The CLF designates 'CERT.PT', which is integrated into the CNCS, as the national cybersecurity incident response team. It has technical and operational autonomy[18], and this autonomy enables it to act swiftly and effectively in critical situations, without having to rely on other entities for technical decisions[19].

CERT.PT's responsibilities include:

- Ensuring immediate intervention in the event of cybersecurity incidents, coordinating actions to contain and mitigate their impact.
- Continuously monitoring the national landscape of cyber threats, vulnerabilities and incidents and providing technical support to important public entities, including real-time monitoring when requested.
- Activating early warning mechanisms and disseminating critical information about threats and incidents to affected entities, competent authorities, and other interested parties, ensuring speed and clarity, including in real time.
- Directly supporting affected entities and proposing concrete instructions and measures to the CNCS to contain, mitigate and resolve incidents, setting appropriate implementation deadlines.
- In scenarios involving serious and proven risk, recommending to the relevant authority the immediate adoption of executive measures if the affected entity does not act voluntarily.
- Collecting and preserving forensic data, performing dynamic risk and incident analyses, and developing situational awareness in order to strengthen national cybersecurity.
- Upon request, performing detailed analyses of entities' networks and systems to identify significant impact vulnerabilities.
- Implementing mechanisms that enable secure data exchange between critical, important, and relevant public entities, as well as other stakeholders.

18 Articles 19(3) and 22.
19 Article 22.

▲ RETURN HOME

In addition to CERT.PT, there are sector-specific teams for regulated sectors such as banking, finance, insurance, and communications. These teams ensure a rapid and specialised response in each area. They also provide a specialised response tailored to the specific characteristics of each area, working in coordination with CERT.PT. When an incident affecting a regulated sector occurs, the team for that sector takes direct action, while CERT.PT coordinates and provides support to ensure that the response aligns with the national strategy.

The relationship between the teams is one of cooperation and information sharing. The CNCS coordinates the national response and ensures interoperability with similar European teams.

CERT.PT coordinates and provides support to ensure that the response aligns with the national strategy.

In the event of a large-scale crisis, such as an attack compromising critical infrastructure or essential services with cross-border implications, a crisis office is activated. This office is composed of representatives from the main security and defence bodies, ensuring a coordinated and effective response. This office coordinates and optimises technical and strategic efforts to ensure an effective response, restoring normality and protecting national interests.

In practice, CERT.PT responds to incidents ranging from isolated ransomware attacks on public bodies to complex DDoS attacks against financial market infrastructures, which require international coordination. CERT.PT's role extends beyond reaction to include prevention, monitoring, and providing technical advice as necessary to effectively respond to cybersecurity incidents.

10. How will consistency be ensured across the different sectors?

The framework strengthens the role of the National Cybersecurity Centre (CNCS) as the national authority responsible for supervising and monitoring the covered entities. It also defines how the CNCS will coordinate with sector-specific and special supervisory authorities for specific economic sectors, all of which will act in coordination with the CNCS.

Additionally, the institutional framework for cybersecurity is composed of the Higher Council for Cybersecurity ("CSSC"). The CSSC acts as an advisory body to the Prime Minister on matters of cybersecurity. Its responsibilities include ensuring the strategic coordination of cybersecurity and responding to requests from the Prime Minister, as well as proposing security assessments by the Cyberspace Security Assessment Commission.

The CLF establishes the following as national, sector-specific cybersecurity authorities:

- The National Security Office (GNS)
- The National Communications Authority (ANACOM)

With regard to the digital operational resilience of the financial sector, the special national cybersecurity authorities are:

- The Insurance and Pension Funds Supervisory Authority (ASF)
- The Securities Market Commission (CMVM)
- Banco de Portugal (BdP)

The following also form part of the institutional framework for cybersecurity:

The Secretariat-General of the Internal Security System, which is responsible for managing large-scale cybersecurity crises and incidents

- The Judicial Police
- The Security Information Service
- The Strategic Defence Information Service
- The Cyber Defence Operations Command

At the operational level, CERT.PT, the national cybersecurity incident response team integrated into the CNCS, also stands out.

The CNCS and the relevant supervisory authorities will be responsible for monitoring compliance with the CLF. They must also ensure that entities covered by the legislation comply with it, guaranteeing that they meet regulatory requirements and risk management standards. The role of these authorities extends beyond supervision. They are also responsible for applying corrective and punitive measures, such as inspections, audits, and binding orders. These measures are always intended to ensure that entities comply with the standards defined by the relevant legislation.

Coordination with the CNPD (the National Data Protection Commission) is particularly important in the event of significant incidents involving personal data. It is also essential when the CNCS or national sector-specific and special cybersecurity authorities reasonably suspect, during a supervisory action or the imposition of an enforcement measure, that certain infringements – such as those relating to cybersecurity measures, risk management or incident reporting – may result in a personal data breach[20].

In the event of significant incidents involving the breach of personal data, the CNCS or the national sector-specific and special authorities are required to notify the CNPD of the breach[21].

Additionally, the CLF facilitates cooperation and interoperability between the various authorities involved in its implementation. This is reflected in the cross-cutting nature of information flows between supervisory authorities, as well as the CNCS's access to relevant national databases and registers.

11. What are the main instruments of the CLF?

The instruments set out in the Cybersecurity Legal Framework are intended to establish an integrated architecture that strengthens national cybersecurity and ensures the effective prevention, detection, and response to incidents. The main instruments include:

- The National Cyberspace Security Strategy (Article 12): this is the guiding instrument for national cybersecurity policy. It defines national priorities and strategic objectives to guide the actions of the state, as well as public and private entities, in protecting cyberspace. The strategy should be reviewed periodically to adapt to changes in the national threat landscape and technological developments.
- The National Plan for Response to Large-Scale Cybersecurity Crises and Incidents (Article 13): this defines procedures for the coordinated management of incidents that exceed national response capacity and impact at least two European Union Member States. It includes communication, coordination, and mitigation procedures, ensuring coordination with European authorities and the activation of international cooperation mechanisms. The plan must be approved within six months of the CLF coming into force[22].

20 Articles 23(1) and 79.
21 Article 40(5).
22

- The National Cybersecurity Reference Framework (Article 14): this brings together various standards, best practices and technical guidelines that entities covered by the CLF must follow. It serves as a reference for implementing and maintaining effective information security measures in line with international standards and the requirements of the NIS2 Directive. The aim is to harmonise practices, reduce vulnerabilities, and promote a consistent approach to risk management.

- Alongside these instruments, the CLF is linked to the National Cyber Defence Strategy (Article 11(d)) and the Strategic Concept of National Defence (Article 11(e)), which provide general guidelines for protecting cyberspace in the context of national defence. These documents complement the civil approach to cybersecurity with a defence perspective, ensuring that military and civil capabilities are aligned to respond to hybrid threats and attacks that could compromise the State's sovereignty or security.

The CLF instruments are not only essential tools for maintaining compliance with the CLF by covered entities, but also from a national security perspective, providing an integrated and coordinated approach, particularly in the event of significant incidents.

12. What enforcement and supervision measures are established?

As mentioned in point 2 above, the CNCS's actions will differ depending on the respective classification, particularly with regard to amendments to the CLF and the principle of proportionality.

- **Essential entities[23]:** proactive enforcement, such as on-site inspections and remote supervision, as well as regular or targeted security audits and ad hoc audits.

- **Important entities and key public entities[24]:** ex post supervision prompted by complaints or suspected non-compliance with the law, based on evidence or proof of such non-compliance, with the same supervision measures as for essential entities and ad hoc audits.

If the national supervisory authority finds that an entity is not complying with the obligations arising from the CLF, it may take measures, including:

- Warnings about detected infringements or instructions to correct them.

23 Article 54.
24 Article 55.

- Binding instructions to take certain preventive or corrective measures in response to an incident.
- Orders or instructions for the correction of infringements.
- Orders to communicate the potential impact of an incident to the natural or legal persons to whom they provide services.
- Appointment, for a limited period, of a supervisor responsible for monitoring compliance with cybersecurity risk management obligations.
- Imposition of fines.

The CNCS may also instruct the entity to implement measures to neutralise cyberattacks, such as blocking or redirecting in the event of misuse of domain names or IP protocol addresses[25].

The CNCS may also instruct the entity to implement measures to neutralise cyberattacks.

13. What administrative offences and fines are there for non-compliance with the Cybersecurity Legal Framework?

Penalty provisions[26] are graded according to the seriousness of the infringement and the classification of entities that fail to comply with cybersecurity rules. Fines can be divided into:

VERY SERIOUS OFFENCES

This is the case, for example, for non-compliance with cybersecurity measures or the duty to report incidents.

- Fines for essential entities: Up to €10 million or 2% of annual global turnover, whichever is higher. Up to €200,000 if committed by a natural person.
- Fines for important entities: Up to €7 million or 1.4% of annual global turnover, whichever is higher. Up to €200,000 if committed by a natural person,
- Fines for public entities: Up to €4 million for public entities in Group A and up to €350,000 for public entities in Group B. If committed by a natural person, up to €16,000.

25 Article 57.
26 Chapter VII.

SERIOUS OFFENCES

This applies, for example, to failure to comply with the obligations set out in Article 8, or the obligation to register on the CNCS platform.

- Fines for essential entities: Up to €5 million or 1% of annual global turnover, whichever is higher. Up to €125,000 if committed by a natural person.
- Fines for important entities: Up to €3.5 million or a maximum amount not less than 0.7% of annual global turnover, whichever is higher. Up to €125,000 if committed by a natural person.
- Fines for public entities: Up to €2.5 million for public entities in Group A and up to €225,000 for public entities in Group B. Up to €10,000 if committed by a natural person.

MINOR OFFENCES

For example, this applies to the misuse of invalid, expired, or revoked cybersecurity certification marks. Fines for minor administrative offences are applied uniformly, regardless of the entity's classification. They can range up to €45,000 for legal persons and up to €3,750 for natural persons.

The CLF also provides for the punishment of obligations that constitute very serious and serious administrative offences on the grounds of negligence. Additionally, penalties apply to the use of invalid, expired, or revoked cybersecurity certification marks and to the use of expressions or graphics suggesting certification of products, services, or processes that are not certified. In these cases, the minimum and maximum limits of the fines are halved.

Proceeds from fines will be distributed, with 60% going to the state and 40% to the CNCS or national cybersecurity authority, depending on which entity initiated and conducted the proceedings[27].

The criteria for applying fines include:

- The seriousness of the infringement
- The degree of fault of the perpetrator
- The economic situation of the perpetrator
- The economic benefit derived by the perpetrator from the administrative offence

14. When will the new legislation come into force, and what will the transition period be?

The CLF will come into force 120 days after publication.

For 12 months from its entry into force, entities may request an exemption from fines if they can demonstrate that they are adapting to the new legal framework[28].

The CNCS is currently working on making available the regulations detailing the envisaged obligations, forms, and electronic platform for classification, registration, and incident reporting. These regulations will take effect 24 months after they are made available, along with the measures and obligations on which they depend[29].

27 Article 73.
28 Article 65.
29 Article 10(2) of the Decree-Law.

15. What can we expect from the new Cybersecurity Legal Framework?

The CLF is expected to reinforce a more cross-cutting cybersecurity culture across various business sectors, in terms of both preventive measures and responding to information security incidents.

The impact of this legislation is also expected to extend beyond the entities covered to their supply chains, as they will be obliged to ensure that their service providers do not pose an increased cybersecurity risk. Faced with rigorous supply chain risk analysis processes and more demanding contractual obligations, service providers will also be forced to adopt adequate security measures to remain competitive.

Additionally, the CLF will have a differentiated impact depending on the sector and size of the companies covered. For entities already covered by the previous Legal Framework for Cyberspace Security that demonstrated adequate maturity and resilience to the risks in their sector, the rigour of the CLF is not expected to affect the organisational culture that has already been implemented and promoted. However, in the case of entities that are now covered by this legislation, particularly small and medium-sized companies, the CLF will require planned and structured investment for its implementation.

In any case, companies should begin by outlining a phased strategy for the verification and, if necessary, implementation of the Cybersecurity Legal Framework. This will involve:

- Identifying the risks to which they may be subject and defining or reviewing risk management procedures.
- Identifying and classifying assets, particularly those critical to service provision. If they have already been identified, it will be necessary to review their classification based on an assessment of cybersecurity risks.
- Developing or reviewing internal policies and procedures related to information security to ensure full compliance with the CLF.
- Reviewing supply chain analysis procedures, identifying service providers that may pose an increased risk to the company, and developing a plan for prior analysis and contract review.
- Ensuring that management, executives, and administrators are aware of their roles in promoting a culture of cybersecurity.
- Developing or reviewing the cybersecurity awareness and training plan for the entire organisation and, where applicable, for third parties.

Once the CLF is approved, we can expect a robust regulatory framework that will give organisations which anticipate and invest in their digital resilience a competitive advantage. It will also ensure a more secure and resilient economy that inspires confidence in technology. Preparing for this new legislation is now more than ever a strategic opportunity to lead with security in the digital universe.

▲ RETURN HOME

About PLMJ

→ Who we are

About the Technology, Media and Telecommunications

→ What we do

> "PLMJ is the most organised firm and the most committed at doing things on schedule and to the time that is asked. They are the most up to date and one of most professional law offices that work with us."
>
> CLIENT REFERENCE FROM CHAMBERS AND PARTNERS

KEY CONTACTS

Pedro Lomba

Partner

(+351) 213 197 412
pedro.lomba@plmj.pt

Pedro was a member of the working group appointed by the Portuguese government to prepare a draft bill transposing the NIS 2 Directive on cybersecurity.

Marta Salgado Areias

Senior associate

(+351) 210 103 741
marta.salgadoareias@plmj.pt

Marta has advised on cybersecurity, focusing on governance and risk management. Has extensive experience in negotiating technology contracts, conducting audits and supporting implementation projects that require regulatory guidance.

Inês Cabugueira

Associate

(+351) 213 197 462
ines.cabugueira@plmj.pt

Inês advises clients on the intersection between cybersecurity and data protection and holds an ITIL4 Foundation certification in IT service management.

Mafalda de Brito Fernandes

Associada

(+351) 213 197 300*
mafalda.britofernandes@plmj.pt

Mafalda is an experienced cybersecurity and risk management consultant who holds ISO/IEC 27001, ISO/IEC 27701 and ITIL4 Foundation certifications.

▲ RETURN HOME

December 2025