CUATRECASAS

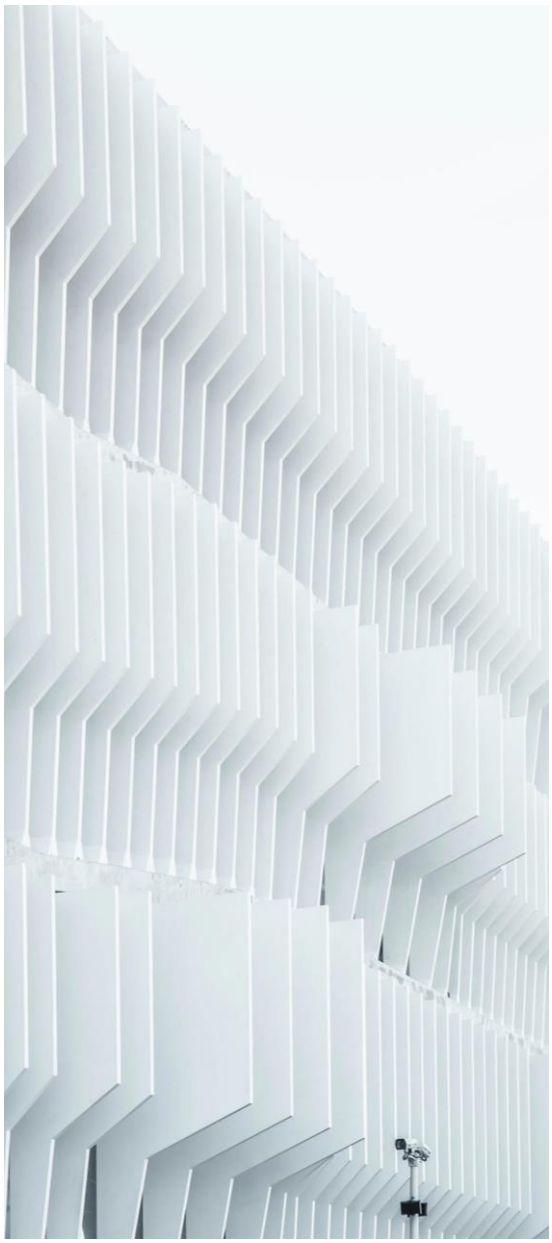
CUATRECASAS

EU Directives NIS and NIS 2 – Implementation in Portugal

Implementing Directive (UE) 2016/1148 (NIS Directive) and Directive (UE) 2022/2555 (NIS2 Directive) in Portugal: an overview of the current situation

Portugal - Legal Flash

November 3, 2023



Key aspects

- The NIS Directive brought about a shift in the institutional and regulatory approach to cybersecurity, yet it encountered challenges leading to fragmentation among Member States.
- The NIS 2 Directive was issued on December 14, 2022, aiming to enhance cybersecurity across the EU and requiring Member States to transpose it into their national laws by October 17, 2024.
- Directive NIS 2 introduces a range of changes from its predecessor, notably expanding the scope of application, implementing improvements on risk management and organizational awareness, establishing new incident notification criteria and introducing new entities such as EU-CyCLONe to bolster cooperation among Member States.
- Portugal is urged to adhere to the standardized approach outlined at EU level by implementing the NIS 2 Directive without deviation, as a centralized and uniform evaluation method ensures equal standards and fair competition among market operators.

Introduction

Adopted in 2016, the NIS[1] Directive aimed to strengthen cybersecurity resilience across the European Union through regulatory measures. It focused on strengthening cybersecurity capabilities at a national level, enhancing collaboration between Member States and incorporating cybersecurity into the DNA of organizations, in particular operators of essential services and digital service providers.

In Portugal, the NIS Directive was transposed in 2018, establishing the legal framework for cyberspace security[2] and appointing the National Cybersecurity Center (CNCS) as the body responsible for overseeing the implementation of the Directive. Later, Decree-Law 65/2021, published in 2021, regulated the existing legal regime and defined the requirements for entities.

The NIS Directive triggered a change in the institutional and regulatory approach to cyber security, but it faced certain challenges where the law could not provide a fitting answer, resulting in a fragmented approach at Member State level. In the last few years, the fast expansion of the digital landscape, caused by a wide array of circumstances such as the rapid sequence of innovations, the global pandemic and cyber warfare, also led to an increased number of cyberattacks targeting organizations and Member States.

As a result, on December 14, 2022, NIS2[3] Directive was published to speed up and establish a higher level of cybersecurity and resilience within organizations of the European Union. EU Member States will now have to transpose NIS2 Directive into their national legislation by October 17, 2024.

The measures established in the NIS2 Directive include (i) broadening its scope of application; (ii) creating new cooperation strategies; (iii) reporting obligations; (iv) defensive cybersecurity approaches; (v) cyber hygiene policies; and (vi) efforts to raise global awareness of cybersecurity.

This legal flash is an overview of the cybersecurity legal and regulatory developments in Portugal and the NIS2 Directive implementation process.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[2] Act 46/2018, of August 13

[3] 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 (NIS2 Directive)

Background of the NIS Directive in Portugal

The NIS Directive (2016)

The NIS Directive marked a major step forward in the EU's efforts to bolster cybersecurity across its Member States. Because of the increase in information security incidents and their impact on the operation of networks and information systems, the EU found it necessary to address the threat-landscape mostly affecting companies with greater exposure to cyber threats.
This Directive was the first horizontal piece of EU legislation to address the new cybersecurity challenges and a turning point in terms of the Union's cybersecurity resilience and cooperation, since, until then, there was no single cybersecurity strategy, and it was up to each entity to define whether and how to implement its own strategy.
The NIS Directive aimed to improve national cybersecurity capabilities, strengthen cooperation at EU level and foster a culture of risk management and incident reporting among the key economic players, namely:

- **Operators of essential services**: entities that operate in sectors considered critical to society and the economy such as (i) energy (electricity, oil and gas); (ii) transport (road, air, rail, maritime and inland waterway transport); (iii) health; d) banking services; (iv) financial market infrastructure; (v) drinking water supply and distribution; and (vi) digital infrastructure (which includes traffic exchange points, DNS service providers and top-level domain name registries); and
- **Digital service providers**: including online services that are essential for critical processes for society, i.e., cloud computing services, online search services and e-commerce platforms.

Entities under the scope of this Directive are now obliged to comply with certain requirements: (i) to implement **adequate security measures** according to their level of risk exposure and (ii) **report information security incidents** to the competent national authorities.
At national level, the Directive also requires each Member State to improve incident response performance by (i) defining a national cybersecurity strategy; (ii) appointing competent authorities in the field; (iii) establishing incident response mechanisms; (iv) carrying out regular tests; and (v) improving response capabilities. At EU level, it also introduces the obligation to set up cooperation structures and information exchange regarding emerging threats, vulnerabilities and best practices in information, network and systems security.

Transposing NIS Directive to Portugal - Act 46/2018, of August 13

It was up to each Member State to define the specifics of each measure, so Portugal transposed NIS through Act 46/2018, of August 13, establishing the legal framework for cyberspace security.
This legal framework provides the national network and information security strategy, and it covers operators of essential services and digital service providers, public administration and operators of critical infrastructures. The Portuguese national strategy thus goes beyond the minimum required by the European Directive.
The national structure for cybersecurity is comprised of:

- **The Cybersecurity High Council**: This body is responsible for ensuring political-strategic coordination for cybersecurity. It verifies the implementation and comments on the defined national strategy, issues reports and opinions on the national strategy and other cybersecurity matters, and responds to requests from the Prime Minister, the Government, or any representative.
- **The National Cybersecurity Center (CNCS)**: This is the national supervisory entity for cybersecurity, operating under the National Security Office. It is responsible for ensuring a secure and reliable cyberspace, both nationally and internationally. It serves as the single point of contact for international cooperation and has a comprehensive regulatory role. The CNCS has the power to issue cybersecurity instructions, define alert levels, and provide prior opinions on cybersecurity matters. Additionally, it closely collaborates with other national entities on issues of cyber espionage, cybercrime and data protection.
- **The CERT.PT**: This is the body responsible for operational coordination in responding to cybersecurity incidents in Portugal. Its competencies include monitoring incidents at the national level, activating rapid alert mechanisms, and participating directly in the analysis and mitigation of incidents. Furthermore, CERT.PT (i) dynamically assesses cyber risks and ensures cooperation with public and private entities; (ii) promotes the adoption of common security practices; (iii) represents Portugal in national and international cybersecurity cooperation forums; and (iv) participates in training events to improve its capabilities.

Chapter III of Act 46/2018 also implements the Directive's incident notification requirements in Portugal. These are

For Public Administration, operators of critical infrastructures and operators of essential services:

- Number of affected users
- Duration of the incident
- Geographical distribution, with regard to the area affected by the incident

For digital service providers:

- Number of users affected by the incident, particularly those who depend on the service to provide their own services
- Duration of the incident
- Geographical distribution, with regard to the area affected by the incident
- Level of severity of service disruption
- Extent of the impact on economic and societal activities.

The NIS Directive also introduced, in recitals (35), (59) and (72), a reference to voluntary sharing of information about incidents in specialty groups to increase resilience in the fight against cyber threats. Following the guidelines of the Directive, the Portuguese legal framework highlights the importance of this recommendation through article 20, thus enshrining a recommendation for voluntary incident notification that aims to make known some types of the most frequent incidents and known vulnerabilities and to offer an overview of the threat-landscape to the supervisory entity.
As for the specification of security measures, this legal framework for cybersecurity refers to a complementary law that will define, in addition to the expected security measures, the timelines for reporting incidents.

In terms of offenses, Act 46/2018 sets out the following penalties:

- Very serious offenses: €5,000 to €25,000 for an individual and €10,000 to € 50,000 for a legal person
- Serious offenses: €1,000 to €3,000 for an individual and €3,000 to €9,000 for a legal person
- Negligence: half the minimum and maximum fines set for serious and very serious offenses.

Decree-Law 65/2021, of July 30

Act 46/2018, of August 13, approving the legal framework for cybersecurity, transposed Directive (EU) 2016/1148 of the European Parliament and the Council, dated July 6, 2016, into the national legal system. This Directive relates to measures aimed at ensuring a common high level of network and information systems security across the Union (NIS Directive), and it refers to complementary legislation for defining the security requirements of networks and information systems, as well as the rules for incident notification. Public administration, operators of critical infrastructures and of essential services and digital service providers must comply with these requirements.
Decree-Law 65/2021, dated July 30, regulates the legal framework for cybersecurity and defines obligations concerning cybersecurity certification. These requirements constitute the minimum that entities under the scope of Act 46/2018, of August 13, must fulfill, without prejudice to the rules that, depending on their nature, specific aspects of their activity or the context in which they perform them, may be established by other authorities.
Thus, this Decree-Law primarily focuses on (i) the obligation to create two figures for corporate cooperation (the security officer and the permanent contact point); (ii) the obligation of periodic risk

analysis and documentation; (iii) strengthening collaboration between entities, and between them and the supervisory entity; (iv) creating an adequate security plan appropriate to the size and risk exposure of the entity; (v) developing an asset inventory; (vi) specifying the timelines for incident reporting and (vii) introducing a taxonomy of incidents that harmonizes and simplifies the process of classifying them.

The Decree-Law highlights the following topics:

- **Risk analysis**
  a) Global risk analysis:
     i. At least once a year; and
     ii. After the CNCS notifies an emerging risk, threat or vulnerability that implies that an incident with significant impact is likey to occur within the timeframe set by the CNCS.
  b) Partial scope risk analysis:
     i. During planning and preparation to introduce a change to the involved asset or assets;
     ii. After an incident with significant impact or another extraordinary situation occurs, in relation to the assets involved; and
     iii. After the CNCS notifies an emerging risk, threat or vulnerability that implies that an incident with significant impact is likey to occur within the timeframe set by the CNCS.
  c) Documentation, preparation, execution, and presentation of the results of risk analyses
  d) To be included in the risk analysis for each asset:
     i. Identification of threats, internal or external, intentional or unintentional (system failure, natural phenomenon, human error, malicious attack, or failure in the supply of goods or services by a third party); and
     ii. Classification of the impact and likelihood of the threats identified in the previous point.
  e) Criteria for risk analysis:
     i. History of extraordinary situations that have occurred;
     ii. History of incidents and, in particular, of incidents with significant impact;
     iii. Number of users affected by the incident;
     iv. Duration of the incident;
     v. Geographical distribution, in terms of the area affected by the incidents; and
     vi. Intersectoral dependencies for the provision of services, including those set out in the annex to the legal framework for cybersecurity and the electronic communications sector.
  f) Adoption of appropriate technical and organizational measures to manage risks to network and information systems security resulting from sector-specific regulations approved by the CNCS or the National Cybersecurity Reference Framework.

- **Deadlines for incident notification:**
    a) Initial notification must be issued as soon as the entity finds that there is or may be a significant incident or substantial impact and within two hours after verifying it;
    b) End of significant or substantial impact must be submitted to the CNCS as soon as possible, within two hours after the incident of significant or substantial impact and include an update in comparison to the initial notification;
    c) Final notification must be sent within 30 business days from the moment the incident is solved and include all the information obtained about the incident.
- **Incident taxonomy:**
    a) For the purposes of this Decree-Law, the following root cause categories are considered:
        i. System failure
        ii. Natural phenomenon
        iii. Human error
        iv. Malicious attack
        v. Failure in the supply of goods or services by a third party
    b) Incidents may have the following effects:
        i. Malware infection
        ii. Unavailability
        iii. Information gathering
        iv. Intrusion
        v. Intrusion attempt
        vi. Information security breach
        vii. Fraud
        viii. Abusive content
        ix. Other

In addition, this Decree-Law introduces a set of notification obligations to report incidents to the National Cybersecurity Center (*Centro Nacional de Cibersegurança*) regarding:

- the permanent contact point;
- the security officer;
- critical assets for the continuity of operations; and
- the annual report.

In summary, this Decree-Law details how the technical requirements defined in Act 46/2018 of August 13 should be fulfilled.

Regulation 183/2022 of February 21, 2022

Regulation 183/2022 of February 21, 2022, sets out the technical instructions for communication and information concerning the permanent contact point, the security officer, the asset inventory, the annual reports and incident notification between entities and the National Cybersecurity Center.

- **Sending and processing information:** Article 1 of the regulation provides that the information to be sent to CNCS under articles 4 (permanent contact point), 5 (security officer), 6 (asset inventory) and 8 (annual report) of Decree-Law 65/2021 must be communicated electronically to the email address sri@cncs.gov.pt or via an API (application programming interface) provided by CNCS for that purpose. If entities wish to send information protected by cryptographic methods, they can secure the information using the PGP public key associated with the above email address published on the CNCS website. CNCS must store and manage such information in a secure information system.

- **Security officer:** The name of the individual appointed security officer must be communicated to CNCS in accordance with paragraphs 2, 3 and 4 of article 5 of Decree-Law 65/2021.

- **Asset inventory**: Below is the information that must be included in the equipment and application inventory:
    a) Physical devices and systems:
        i. Inventory number
        ii. Name and model of the equipment
        iii. Serial number
        iv. Location
        v. Classification of how critical they are to the entity
    b) Network-connected devices must have the following additional information:
        i. IP address
        ii. Hardware address
    c) Individuals responsible for the devices and systems:
        i. Name
        ii. Contact information
        iii. Department
    d) Applications:
        i. Software name
        ii. Version
        iii. Manufacturer
        iv. Name of the person in charge
        v. Contact information
        vi. Department

vii. Classification of how critical the app is to the entity
viii. Type of support contract in place with the application or software platform provider (when applicable)

e) Assets publicly accessible via the internet:
   i. Supported service
   ii. Equipment or software name
   iii. Model and version
   iv. IP address (if applicable)
   v. Fully Qualified Domain Names (FQDNs) (if applicable)
   vi. Manufacturer

- **Annual report**: It must be sent to the CNCS according to sections 2 and 3 of article 8 of Decree-Law 65/2021, with the information listed in section 1 of that article: (i) main network and information systems security activities; (ii) quarterly incident statistics; (iv) aggregated analysis of significant incidents; (v) recommendations for activities, measures or practices to improve network and information systems security; and (vi) issues identified and measures implemented as a result of incidents.
- **Incident notification**: Under articles 11 to 16 of Decree-Law 65/2021 (in force since the last quarter of 2021) incidents must be notified through the CNCS website (https://www.cncs.gov.pt) by completing the reporting template under "Incident Notification" or via the API provided by the CNCS for this purpose. As an exception, when, as a result of an incident or a justified predominantly technical reason, the entitly cannot ensure notification on the CNCS website or where it is unavailable, an incident can be notified by
  - Email to cert@cert.pt
  - Calling (+351) 210 497 399
  - Calling (+351) 910 599 284 available 24/7

If entities wish to use cryptographic methods to protect the information, they can use the PGP public key, associated with the above email address listed on the CNCS website.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive)

Introduction

The NIS 2 Directive, published on December 27, 2022 in the "Official Journal of the European Union," aims to enhance the cybersecurity posture of EU Member States. It builds upon the original NIS Directive of 2016, extending its scope and introducing new measures to address the evolving cyberthreat landscape.

Expanded scope

Under article 3,[4] NIS 2 identifies essential entities (article 3.1) and important entities (not listed as essential), while its annexes I and II list critical sectors, to which other sectors and entities have been added. Member States must produce a list of essential entities and important entities by 2025 to identify the those highly exposed to a significant cyber threat.
The following table highlights the additional entities covered by the NIS 2 Directive:

Essential entities	Important entities
› Energy (electricity, district heating and cooling, oil, gas and hydrogen) › Transport (air, rail, water, road) › Banking › Financial market infrastructures › Health (healthcare providers, EU reference laboratories, entities manufacturing basic pharmaceutical products and pharmaceutical preparations, entities carrying out research and development activities of medicinal products and entities manufacturing medical devices considered to be critical during a public health emergency) › Drinking water › Waste water › Digital infrastructure (Internet Exchange Point providers, DNS service providers, excluding operators of root name servers, TLD name	› Postal and courier services › Waste management › Manufacture, production and distribution of chemicals › Production, processing and distribution of food › Manufacturing (manufacture of medical devices and *in-vitro* diagnostic medical devices, manufacture of computer, electronic and optical products, manufacture of electrical equipment, manufacture of machinery and equipment n.e.c., manufacture of motor vehicles, trailers and semi-trailers and manufacture of other transport equipment) › Digital providers (of online marketplaces, of online search engines and of social networking services platforms) › Research organizations

[4] The NIS Directive (2016) only differentiated between operators of essential services and digital service providers.

registries, cloud computing service providers, data center service providers, content delivery network providers, trust service providers, providers of public electronic communications networks and providers of publicly available electronic communications services) › ICT service management (business-to-business) › Public administration › Space	

In addition to the new definitions inserted in article 6 of the new Directive, where more than 20 new obligations for entities were added compared to the NIS Directive, the new Directive:

- strengthens some of the measures already provided in Decree-Law 65/2021, particularly with regard to risk assessment and incident handling, and
- includes a minimum set of precise cybersecurity aspects that organizations must address.

Similarly to what was provided in the NIS Directive (2016), the new Directive maintains some of the functions and obligations imposed on Member States and European institutions.

Improvements in cybersecurity risk management

Both essential and important entities must adopt appropriate technical, operational and organizational measures to address the risks affecting network and information systems security. Also, the mechanisms for direct communication and notification of mandatory information to the competent authorities are improved. This Directive highlights the following main risk management issues:

- Policies on risk analysis and information system security
- Incident handling
- Business continuity, such as backup management and disaster recovery, and crisis management
- Supply chain security, including security-related aspects of the relationship between entities and direct suppliers or service providers
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyberhygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and encryption

- Human resources security, access control policies and asset management
- Multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity

Reporting obligations

As opposed to the notification thresholds provided in the law transposing the NIS Directive in Portugal (an incident with relevant or substantial impact), entities covered by the NIS 2 Directive must immediately inform the supervisory authorities of any actual or potential cybersecurity incident.

European Union cooperation on cybersecurity issues

This Directive reinforces the importance of the Cooperation Group and the network of national teams responsible for responding to security incidents, which proved to be insufficient or inadequate during the course of the NIS Directive (2016).

With these requirements in mind, Computer Security Incident Response Teams (CSIRTs)[5] are set up to monitor cyber threats and vulnerabilities at national level. In addition, the European Union Agency for Cybersecurity (ENISA) will provide guidelines and templates regarding the obligations of information sharing arrangements. Moreover, the NIS 2 Directive reinforces the importance for Member States to ensure that information sharing can still be performed on a voluntary basis as with its predecessor.

Finally, it creates a framework for EU response to cybersecurity crises through existing cooperation networks, namely the Network of Cybercrisis Coordination Organizations (EU-CyCLONe), made up of representatives from the cyber crisis management authorities of the Member States, the European Commission (especially when a cybersecurity incident has a significant impact on the services and activities covered by the Directive), and ENISA (European Union Agency for Cybersecurity).

The main functions of EU-CyCLONe include:

- preparing Member States for the management of large-scale cybersecurity crises and incidents;
- creating a common understanding of large-scale cybersecurity crises and incidents;
- assessing the consequences and impact of crises and incidents and proposing mitigation measures;
- coordinating crisis management and supporting decision-making at the political level; and
- upon request from the concerned Member State, discussing national plans for responding to cybersecurity crises and incidents.

[5] In Portugal, represented by CERT.PT

Raising awareness about cybersecurity

The Directive encourages the practice of cyber hygiene, which involves basic steps like regular software updates, employee training and multi-factor authentication, among others. These practices are about creating a culture of security awareness where all stakeholders understand their role in safeguarding the organization's digital assets.
Reinforcing these aspects aligns the NIS 2 Directive with the broader EU strategy to create a digital single market, where a high level of cybersecurity is essential for consumer trust and the seamless operation of crossborder services. By mandating higher standards and promoting awareness, the Directive aims to create a more resilient digital ecosystem, thereby contributing to economic stability and public safety.

Non-compliance with the NIS 2 rules

To ensure enforcement, the Directive allows for fines for non-compliance with the established rules.[6] Although the transposition of NIS in Portugal already provided fines, NIS 2 has increased them:

<table>
<tr><th>Act 46/2018</th><th>NIS 2 Directive</th></tr>
<tr><td>Very serious offenses: €5,000 to €25,000 for individuals, and €10,000 to €50,000 for legal persons.</td><td rowspan="3">Essential entities: A maximum of €10,000,000 or a maximum of at least 2% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

Important entities: A maximum of €7,000,000 or a maximum of at least 1.4% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.</td></tr>
<tr><td>Serious offenses: €1,000 to €3,000 for individuals, and €3,000 to €9,000 for legal persons.</td></tr>
<tr><td>Negligence: Half the minimum and maximum fines for serious and very serious offenses limits.</td></tr>
</table>

Implementation deadlines

The NIS 2 Directive came into effect in the European Union on January 16, 2023. However, as stipulated in its article 41, the deadline for transposing NIS 2 into the national legislation of the Member States is October 17, 2024, and its provisions will be applicable from October 18, 2024.

[6] The NIS2 Directive provides that "in order to ensure the enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of fines."

As of now, there has not been a public consultation to discuss the implementation of the NIS 2 Directive, which may raise concerns about the level of preparedness, leaving companies and other entities without clear guidelines on how to prepare for the upcoming changes in cybersecurity legislation.
However, it is known that Portugal is one of the European Union countries that has delayed transposing Directives, including missing the implementation deadline for the NIS Directive, but it is advisable for the entities concerned to start preparing and adapting to the new Directive based on the European legislation, while maintaining compliance with the NIS Directive (2016). This is because it is expected that some obligations will remain unchanged.

Transposing Directive NIS 2 in Portugal

Directives, as secondary legislation, lead to harmonizing legal systems across the European Union. They are particularly useful when the aim is to **harmonize laws within a certain area**. They can be addressed to all Member States or to any one, and they are binding with respect to the aim to be achieved and the time to be realized, while leaving some choices as to form and method to the Member States.[7] Unlike regulations and decisions, national transposition of Directives is considered necessary in the Treaty of the European Union to guarantee the effectiveness of EU Law, in accordance with the principle of sincere cooperation established in article 4(3).
Based on the experience of EU Member States and the European Court of Justice in implementing EU Directives, some rules can be drawn up:

- Each State decides the kind of legal act that should be enacted based on its constitutional regime. The status of domestic enactment, however, should be the status of the act that previously regulated a given matter under domestic law.
- The body responsible for passing an implementing act is defined by domestic law. It may be the regional or local government, if the matter falls within their jurisdiction. In any case, central government agencies are responsible for proper implementation of a Directive. States are not allowed to invoke their domestic law (including constitutional provisions) to justify non-fulfillment of the obligations stemming from EU Law.[8]
- Directive nomenclature does not have to be translated word for word into domestic legislation, since such translation creates a danger of introducing institutions unknown to domestic legislation. **Domestic legislation should reflect the spirit or idea rather than the wording of a Directive,**[9] which means that national measures must achieve the objectives set by the Directive.
- However, in case of some Directives, especially those that use highly technical language and are very detailed, **the only solution may be a literal transposition of the text of a Directive into domestic legislation**, but a Directive cannot be treated as an annex to an act of domestic legislation.

---

[7] Article 288 of the Treaty on the Functioning of the European Union (TFEU) "A Directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."
[8] Case 163/78 Commission v. Italy, (1979) ECR 771
[9] Case 131/88 Commission v. Germany, (1991) ECR I825

- If necessary, in specific situations domestic legislation should expressly cite the Directive it is implementing (usually the specific provisions of the Directive) to avoid misinterpretation.
- Domestic laws transposing a Directive have to be enacted within the deadline stated in the Directive. Delays due to domestic factors are not justified.[10]
- If the existing domestic legislation guarantees proper implementation of a Directive or provisions of a Directive, there is no need to issue new act; however, the European Commission should be notified.[11]
- Domestic legislation should include both the substantive provisions of a Directive and the procedures necessary for its implementation, including competent bodies and penalties for non-fulfillment.
- Measures for implementing a Directive into domestic legislation must be notified to the Commission.

The above are practical guidelines to follow when passing the legal act transposing NIS 2 Directive in Portugal.

The general principle that stands out when transposing a Directive into domestic legislation is that the objectives set by the Directive must be reflected in the domestic law. When that law goes beyond the minimum objectives of the Directive ("gold plating"), it must not (i) impede the functioning of the EU internal market or (ii) infringe the principle of non-discrimination under article 18 of the TFEU.
The ultimate goal of the NIS 2 Directive is to introduce a common high level of cybersecurity in the EU that will prevent fragmentation at different levels across the internal market[12] and remove divergences in cybersecurity requirements and in implementing cybersecurity measures in different Member States. This general objective will be implemented in the longer term by a coordinated EU risk assessment.[13]
Portugal must not deviate from the harmonized EU approach and must transpose the NIS 2 Directive and its risk evaluation mechanism "as is," since only centralized and uniform methodology will cumulatively guarantee the equal standard of evaluation and ensure the level playing field among market operators.
Transposing the NIS 2 Directive in Portugal must also follow the general principles of EU Law:

- The **principles of free movement of goods and freedom to provide services** established in articles 28, 34 and 56 of the TFEU, which prohibit any quantitative restriction and sets out that all measures must have equivalent effect on goods traded or services provided within the internal market. Restrictions on free movement may only be justified if they serve a legitimate aim and are proportionate. While the protection of national security can, in principle, constitute a legitimate aim, the public security exception available under the TFEU is construed narrowly. It is available only where there is "a genuine

[10] Case 43/80 Commission v. Italy, (1980) ECR 3543
[11] Case 69/90 Commission v. Italy, (1991) ECR I-6011
[12] See Recital 4, NIS 2 Directive
[13] See Recital 4, NIS 2 Directive

and sufficiently serious threat affecting one of the fundamental interests of society."[14] Therefore, Portugal must not create any barrier to the free movement of a variety of goods and technology without clearly identifying a "cyber threat," as defined by the NIS 2 Directive.

- The **principle of proportionality** (article 5(4) of the TEU), which requires that a measure must not go further than what is necessary to achieve its objective, i.e., a measure has to serve the pursued objective in order to be proportionate. Portugal must, therefore, follow the technical security enhancing measures established in the NIS 2 Directive and abstain from establishing any non-technical (political) criteria, considering its disproportionate nature.
- The **principle of legal certainty,** according to which Member States must word their regulations "unequivocally," so that the entities concerned will have a clear and precise understanding of their rights and obligations and national courts can ensure that those rights and obligations are observed. Any non-technical (political) criteria are subject to broad interpretation and, therefore, are difficult to implement by entities and to interpret by regulators and national courts.
- The **principle of non-discrimination** (article 2 TEU, 18 TFEU), to the extent that any criteria for assessment that is not based on objective criteria makes the risk assessment mechanism inherently discriminatory and in contradiction with this EU principle.

According to Directive 2015/153522 (the TRIS Directive), when a Member State intends to pass a law that contains technical regulations relating to products, prohibiting the manufacture, import, marketing or use of a product or prohibiting the provision or use of a service or establishment as a service provider, it must notify the European Commission. The purpose of this notification is to ensure that the texts comply with EU legislation and the principles of the internal market.

The Commission publishes the notification through the Technical Regulation Information System (TRIS). From the moment it is notified, the "standstill period" of three months starts running. During these three months, the notifying Member State cannot adopt the technical rule, and the Commission and the other Member States can examine the intention of the technical regulation and react appropriately. If it appears that the intention to adopt the technical regulation may hinder the free movement of goods and services or secondary EU legislation, the standstill period may be extended by a further three months, during which the Member State will have to propose amendments to accommodate the legal concerns raised.

[14] Case C-546/07, Commission v Germany (2000) EU:C:2010:25

Conclusion

The NIS 2 Directive represents a significant development from its 2016 predecessor. It addresses gaps and ambiguities in the original Directive, offering a comprehensive and nuanced framework for cybersecurity in the EU. By expanding its scope, refining definitions, and introducing new measures for risk management and operational capabilities, NIS 2 aims to create a more resilient and secure digital environment across the EU. The Directive also has the potential to harmonize cybersecurity practices across the EU, facilitating crossborder cooperation and making the digital single market safer for consumers and businesses.

In summary, NIS 2 is not just a legislative update; it is a shift of paradigm that places cybersecurity at the center of digital strategies, impacting not only how businesses operate, but also how Member States collaborate to address emerging cyber threats.

In line with the fundamental principles of EU Law, Member States must fully respect the openness of the EU internal market and its principles. Although the NIS 2 Directive presents minimum harmonization (as endorsed by article 5 of the NIS 2 Directive), Member States, aiming to adopt or maintain provisions ensuring a higher level of cybersecurity, have to respect the obligations laid down in EU Law.

Portugal must, therefore, guarantee that no barriers are created in the EU internal market and that no disproportionate and unclear criteria are established when transposing the NIS 2 Directive.

For additional information on the contents of this document, please contact *Cuatrecasas*.