

11 October 2024

# Directive NIS2 and national transposing legislation

On October 2 the **Legislative Decree No. 138/2024** that transposes in Italy the Directive (EU) 2022/2555 (so called **NIS2 Directive**), which aims to establish **measures to guarantee a common high level of cybersecurity** within the European Union, has been published.

The relevant rules – which **will be applied** as from the next **18 October** – will repeal Legislative Decree No. 65/2018 transposing the previous NIS1 Directive.

One of the major features of NIS2 Directive is the broad range of entities to which it will be applied, further extended by the Legislative Decree.

This includes public and private entities that jointly have the following 3 requirements:

**Territorial requirement:** the entity provides its services and carries out its activity within EU.

**Dimensional requirement:** the entity, according to Article 2 of the Recommendation 2003/361/CE, qualifies as a medium or large enterprise, *i.e.* it has more than 50 employees and has a yearly turnover or an annual balance sheet total more than € 10 million.

**Except for the PA listed in Annex III and other entities under Article 3 to which the Decree applies regardless of their dimension**

**Sectorial requirement:** the entity provides its services or carries out its activity in one or more sectors alternatively qualified as:

**Critical sectors:** (i) postal and courier services; (ii) waste management; (iii) manufacturing, production and distribution of chemicals; (iv) food production, processing and distribution; (v) manufacturing; (vi) digital service providers; (vii) research.

**Highly critical sectors:** (i) energy, (ii) transports, (iii) banking, (iv) financial market infrastructure, (v) health, (vi) drinking water, (vii) wastewater, (viii) digital infrastructure, (ix) ICT service management, (x) space.

The entities that fall within NIS2's scope of application shall comply with obligations related to cybersecurity risk management and incident reporting. In particular:

- *Governance obligations*

The **administrative and governing bodies** shall (i) approve the implementation methods of the adopted cybersecurity risk management, (ii) oversee their implantation, and (iii) follow a cybersecurity training and offer a similar training to their employees.

Moreover, they are personally accountable for any **breach** of the regulations.

- *Risk Management*

Obligation to adopt **proportionate technical and organizational measures** to **manage** cyber risks, which shall include, for example, risk analysis and security policies, incident management, business continuity, cryptography procedures, hygiene practices and cybersecurity training.

- *Supply chain security*

Obligation to ensure the **supply chain security** by overseeing the security aspects of relationship with its own suppliers.

- *Reporting obligation*

Obligation to **report** security incidents which have a **significant impact on supply** of relevant services to the competent authorities and to collaborate in threats management.



Severe **administrative penalties** are provided in case of non-compliance with the obligations set out in the Decree, differentiated according to the type of violation and the qualification of the entity.

In the event of breach of the most significance obligations, penalties are qualified as follows:

- with reference to essential subjects, penalties amount up to a maximum of **€10,000,000 or 2% of the total annual worldwide turnover** for the previous year, if higher;
- with reference to important entities, penalties amount up to a maximum of **€7,000,000 or 1.4% of the total annual worldwide turnover** for the previous year, if higher.

Moreover, in the event of non-compliance, is provided:

- a **personal liability of the directors and management bodies** and the possibility to apply to them the ancillary administrative penalty of temporary **inability to perform executive functions**, and
- the **suspension of certifications** or authorizations related to (in whole or in part) the services provided by the penalized entity.

The provisions of the Legislative Decree will be applied starting from the next **18 October**. However, compliance obligations applicable to entities which fall into the scope of application have been extended by the Legislative Decree.

In particular, the Decree provides a preliminary phase of identification of companies and public administrations subject to the regulations as follows:

- **By the end of year 2024**, companies and public administrations shall carry out *assessment activities* to evaluate whether they fall within the scope of NIS2;
- From **1 January 2025 until 28 February 2025**, entities that deem to fall within the scope of NIS2 shall **register themselves on a dedicated digital platform** (being adopted by ACN), by furnishing several information. This with exception of any companies (listed in Article 42), the registration of which is necessary within the 17<sup>th</sup> of January 2025;
- **By 31 March 2025**, CAN shall prepare the **list of entities** (distinguished between **essential** and **important**) to which the regulations apply which will be notified of their inclusion in the specific list through the platform **by 15 April**;
- **By 31 May 2025**, entities that have received ANC's communication shall **provide further information** indicated in the regulations.

Once the preliminary phase is completed, the selected entities shall:

- starting from **January 2026**, comply with incidents' **reporting obligations**; and
- by **October 2026**, comply with the **obligations** (i) of the **administrative and management bodies**; (ii) of risk management and implementation of **security measures**; and (iii) relating to the **domain name registration databases**.

# Contacts

**Vittoria Omarchi**

*Senior Associate*

**E.** [vomarchi@pglex.it](mailto:vomarchi@pglex.it)

**T.** (+39) 02 303051

Milano