

COMPLIANCE

# NIS 2 COMPLIANCE **IN ITALY**

*BY MAY 31, 2025, ESSENTIAL AND IMPORTANT ENTITIES ARE REQUIRED TO SUBMIT TO THE ACN THE UPDATED INFORMATION SET REQUIRED BY THE REGULATION.*

AUTORI

avv. **MAURIZIO MARULLO**  
marullo@lawp.it

avv. **CLAUDIA MARONGIU**  
marongiu@lawp.it

The NIS 2 legislation (specifically Directive (EU) 2022/2555 and, in Italy, Legislative Decree 138/2024) is designed to improve the cybersecurity of essential and important organizations, both in the public and private sectors, across the European Union.

Specifically, NIS 2 regulation expands the scope of the previous NIS directive (Directive (EU) 2016/1148), covering a broader range of sectors and introducing more stringent requirements for risk management, incident reporting, and organizational accountability.

Under the new legal framework, Italian entities that have identified themselves as falling within the scope of NIS 2 legislation have already registered on the portal set up by the National Cybersecurity Agency (ACN) by the deadline of February 28, 2025.

Following this registration, the ACN has communicated via certified email to the entities registered on the portal their actual inclusion within the scope of the NIS 2 Directive. With the receipt of this communication, the second phase of implementation of the legislation begins.

This phase requires essential and important entities to communicate to ACN or update the specific information outlined in the following sections by the **deadline of May 31, 2025**.

The information must be provided by the essential and important entities through the ACN portal "**Portale dei Servizi**", available at <https://portale.acn.gov.it/login>. After accessing the portal using the contact point's SPID digital identity or login credentials, essential and important entities can access the dedicated section related to "NIS/Aggiornamento" (NIS/Updates).

## 1. Contact point and substitute contact point details

Essential and important entities must confirm or update the personal and contact details of the contact point designated during the registration phase (name, surname, place and date of birth, tax code, citizenship, country of residence and domicile, role, telephone number, email address and, if available, certified email address).

Furthermore, each essential and important entity must designate a **substitute contact point**, providing to ACN his personal and contact details (name, surname, role, email address, and phone number). Envisioned as a key support figure, the substitute contact point possesses the capacity to directly interact with ACN and perform a wide array of actions on the digital platform, mirroring the capabilities of the primary contact.

## 2. List of management and directive body members

Essential and important entities are required to provide an updated list of the members of their management and directive bodies. The list must include for each member the set of identifying information listed below: full name, surname, the Italian tax code (*codice fiscale*), and their certified email address (PEC).

This requirement is closely connected to the key role that the NIS 2 legislation assigns to directors and managers in ensuring an adequate cybersecurity posture. Specifically, pursuant to Article 38 of the Legislative Decree 138/2024, the individuals managing the company are liable for ensuring compliance and security of the entity.

Each **designated individual** must personally **access the ACN portal to formally acknowledge and accept their designation**, thereby demonstrating awareness of their personal responsibilities under the NIS 2 framework.

**3. List of services provided and geographical perimeter**

Essential and important entities must accurately identify and **list all services** provided that fall within the scope of the NIS 2 legislation. For each relevant service, it must be specified the **EU Member States** where these services are offered.

This information allows ACN to gain a comprehensive understanding of the cross-border dependencies and potential impact of these services within the European digital ecosystem.

**4. Public static IP address space used or available**

Essential and important entities are required to provide a detailed inventory of their **public and static IP addresses**. This encompasses all IP address ranges that the entity actively uses or has secured the right to use through contractual agreements with Internet Service Providers (ISPs), Regional Internet Registries (RIRs), or other duly authorized organizations.

The provision of this information is crucial for ACN to effectively map critical infrastructure and understand network interdependencies.

5. **Domain names used or available**

Essential and important entities must communicate to ACN **all domain names used or that they have the right to use** under contracts or agreements with domain name registrars or other authorized organizations.

This information is essential for ACN to receive a full and comprehensive mapping to ensure a complete overview of the entity's operational landscape.

6. **Notification of voluntary information sharing agreements on cybersecurity**

Recognizing the power of collective defence, Article 17 of Legislative Decree 138/2024, encourages and facilitates voluntary agreements for the sharing of cybersecurity information among entities.

Essential and important entities entering into such agreements must communicate to ACN, the list of all agreements executed. **Any changes** to the list of agreements, including new subscriptions, terminations, or modifications to the agreement text or participants, must be **notified** promptly, and in any case, **within fourteen days** of the change.

7. **Optional support roles: "segreteria" and "operatori"**

To streamline the processes of updating and managing information on the ACN platform, the designated contact point has the **option** (not an obligation) **to invite additional users** with the roles of **"Secretary"** (i.e. Segreteria) (one user limit) and **"Operator"** (i.e. Operatore) to assist with ACN platform management.

These supplementary roles are conceived to provide valuable assistance to both the primary contact point and the substitute contact point in navigating and operating within the ACN platform.

Neither the “Secretary” nor the “Operator” are authorized to perform actions that constitute the formal fulfilment of obligations under the NIS 2 legislation. Specifically, they cannot confirm or transmit official communications to ACN. The ultimate responsibility for the accuracy, completeness, and timely submission of all required information rests with the designated contact point and the overarching management and directive bodies of the entity.

\*\*\*

Meeting the **May 31, 2025** reporting deadline is **essential** for ensuring compliance with the NIS 2 legislative framework. Failure to comply with these requirements within the stipulated timeframe may result in penalties as outlined in the relevant legislation.

For any clarifications or assistance regarding these requirements, please do not hesitate to contact our firm.