NEWSALERT

DATA PROTECTION AND CYBERSECURITY

Directive (EU) 2022/2555 (NIS2) and Italian implementing regulation

Introduction

On October 16, Directive (EU) 2022/2555 ("**NIS2**") will become applicable within the Italian jurisdiction by means of the implementing Legislative Decree No. 138/2024 (the "**Decree**"), which was published in the Italian Official Gazette on October 1.

The new regulation aims to introduce additional obligations on cybersecurity matters and to broaden the scope of application by repealing Legislative Decree No. 65/2018, which implemented Directive (EU) 2016/1148 ("**NIS1**").

I The sectors involved

As concerns the sectors involved, the following were already included:

- energy (electricity, oil, gas);
- transport (air, rail, water, road);
- banking and financial market infrastructures;
- health;
- drinking water;
- digital infrastructure (Internet Exchange Point providers, DNS service providers, TDL name registries); and
- digital providers (providers of online marketplaces, providers of online search engines, providers of domain name registration services).

In addition to the sectors listed above, the following new sectors have been introduced:

- energy (district heating, district cooling, hydrogen production);
- waste water;
- ICT Service Management (managed service provider, managed security service provider);

- public administration (public administration entities of central governments and public administration entities at regional level);
- space;
- postal and courier services;
- waste management;
- manufacture, production and distribution of chemicals;
- production, processing and distribution of food;
- manufacturing (of medical devices and in vitro diagnostics medical devices, computer, electronic and optical products, electrical equipment, machinery and equipment n.e.c., motor vehicles, trailers and semi-trailers, other transport equipment);
- digital infrastructure (cloud computing service providers, data center service providers, content delivery network providers, trust service providers, providers of public electronic communications networks, providers of publicly available electronic communications services);
- digital providers (providers of social networking services platforms); and
- research organisations.

II Implications within the NIS2

The NIS2 will introduce additional obligations, as listed below:

- MANAGEMENT LIABILITY. NIS2 introduces some important changes, such as management liability for non-compliance, which is becoming more common in cybersecurity regulations. Therefore, compliance planning should consider not only the technical aspects, but also the potential legal implications. Another novelty is the requirement for operators to take appropriate and proportionate measures, not only technical and organizational, but also operational.
- TRAINING. The legislation also imposes specific training obligations on both managers and employees. These activities should be carried out by competent, qualified and experienced individuals who can address the main challenges arising from the application of cybersecurity regulations in complex business scenarios.
- SUPPLY CHAIN CONTRACTING. A critical issue is that of suppliers, both in terms of contract analysis and negotiation, and in terms of ongoing audits and assessments. In fact, the regulations require actions to secure the supply chain. This may include drafting *ad hoc* contractual clauses, implementing supplier evaluation measures, reviewing contracts and planning periodic audits.
- NOTIFICATION. The legislation also includes notification obligations to the competent authority, **namely** the Italian Computer Security Incident Response Team (CSIRT). Entities subject to NIS2 and to the Decree must report incidents that have a significant impact on the provision of their service within **(i)** 24 hours, through a preliminary notification, which must be updated within **(ii)** 72 hours from the event. They must also submit at least one **(iii)** final report within one month, unless the Authority requests more information. Therefore, it will be necessary to update reporting procedures to comply with the new rules.
- FURTHER OBLIGATIONS. Finally, entities falling within the scope of the Decree may be required to only use certain European certified products, which will make it

necessary to evaluate suppliers and analyze possible alternatives offering the requires guarantees.

III Timeline

Date	Activities
November 16, 2024	Identification of the first group of entities to which the provisions apply
From the date of publication of the platform of the Italian Cybersecurity Agency ("**ACN**")	Registration on the ACN platform
By January 17, 2025	Registration on ACN's platform by: domain name system service providers, top-level domain registries, domain name service providers, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, online marketplace providers, online search engines and social networking service platforms.
By April 2025	Definition of obligations for essential and important entities
April 15 to May 31, 2025	Disclosure of additional information required by ACN, including contact details of the natural person in charge of the essential entity or its legal representative who will be liable in case of non-compliance with the Decree
By April 17, 2025	Communication to the Commission of the number of essential and important entities
Approximately January 2026 (9 months from notification of qualification as an essential or important subject)	Implementation of reporting requirements
Approximately April 2025 (18 months after publication of the decree)	The definition of categories of relevance, as well as methods and criteria for listing, characterizing and cathegorizing activities and services of cross-sectoral and, where appropriate, sectoral relevance
May 1 to June 30, 2026	Preparation of a list of its activities and services, including all elements necessary for their characterization and the corresponding assignment to a category of relevance
Approximately October 2026 (18 months after notification of qualification as an essential or important entity)	Implementation of management obligations and implementation of technical, organizational and operational measures

IV Conclusions

As the sector faces more and more regulations and obligations that go beyond technical assessment, cybersecurity issues are becoming more critical, and their legal aspects are another facet of the same challenge.

Therefore, even if the regulations at stake are not yet in force, it is crucial to think ahead and plan a strategic approach, including the legal aspects.

In addition, considering the complexity and broadness of the new regulations, interdisciplinary teams should be set up, combining technical and legal skills for compliance. In this context, involvement of external experts should also be evaluated.

Finally, as to multinational groups with entities in more than one jurisdiction, it is advisable to plan the adaptation in an integrated manner as far as possible, bearing in mind that, as this is a Directive, the modalities of adaptation may very from one Member State to another.

Contact

Pierluigi Perri
Of Counsel – Chiomenti
Data Protection and Cybersecurity
T. +39 02721571
pierluigi.perri@chiomenti.net

Marilena Hyeraci
Of Counsel – Chiomenti
Data Protection and Cybersecurity
T. +39 02721571
marilena.hyeraci@chiomenti.net

Lucrezia Falciai
Associate – Chiomenti
Data Protection and Cybersecurity
T. +39 02 721571
lucrezia.falciai@chiomenti.net

Virginia Putortì
Associate – Chiomenti
Data Protection and Cybersecurity
T. +39 02 721571
virginia.putorti@chiomenti.net

Tommaso Bratina
Junior Associate – Chiomenti
Data Protection and Cybersecurity
T. +39 02 721571
tommaso.bratina@chiomenti.net