To whom it may concern

Of counsel
Dott. Sandro Guarnieri

Dott. Marco Guarnieri
Dott. Corrado Baldini
Dott. Paolo Fantuzzi

Dott.ssa Clementina Mercati
Dott.ssa Sara Redeghieri
Dott.ssa Beatrice Cocconcelli
Dott. Daniele Pecora
Dott.ssa Veronica Praudi
Dott.ssa Federica Lusenti
Dott. Andrea Friggeri
Dott.ssa Martina Carobbi
Dott. Matteo Giovannini

Avv. Francesca Palladi

Reggio Emilia, Nov. 19, 2024

MEMORANDUM N. 42/2024

Insight

Subject: NIS Directive 2 and Cybersecurity: compliance for companies

Legislative Decree No. 138 of September 4, 2024 transposed EU Directive 2022/2555 (known as the NIS 2 Directive) into Italian law with the aim of implementing the **level of cybersecurity** in EU member countries.

What is meant by cybersecurity?

Information security (or **cybersecurity**) is the set of practices, technologies, and processes designed to protect computer systems, networks, devices, and data from attack, damage, or unauthorized access. This discipline deals with the protection of digital information and technological infrastructure against threats such as malware, hacker attacks, ransomware, phishing, and other forms of cybercrime.
The main goals of cybersecurity are:

1. **Confidentiality**: ensuring that only authorized persons have access to certain information.
2. **Integrity**: ensuring that data is not altered in an unauthorized or unintentional way.
3. **Availability**: ensuring that systems and information are accessible to legitimate users when needed.

Within cybersecurity, practices of **resilience**, that is, the ability of a system to prevent, detect and recover from cyber attacks, and risk **mitigation**, with the implementation of preventive measures to reduce the impact of attacks, are also developed.

The main changes introduced by NIS Directive 2:

- **Expanded scope:** the directive extends security requirements to more sectors and services considered critical to the socioeconomic functioning

SGB & Partners
Sede legale
Via Meuccio Ruini, 10
42124 Reggio Emilia
CF e Piva 01180810358

Tel. +39 0522 941069
Fax +39 0522 941885
Mail info@sgbstudio.it
Web www.sgbstudio.it

of the EU. In addition to the sectors already covered by the previous NIS directive, new areas such as ICT service management, financial market infrastructure, research, postal services, chemicals, food, digital suppliers, waste management, and manufacturing are included.
The full list of high criticality sectors and subjects can be found by logging on to the Official Gazette website, www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG, by viewing the annexes to the text of the Decree.

- **Risk Management and Incident Reporting Obligations:** stakeholders will be required to take security measures appropriate to the actual risks associated with their business and/or implement existing ones, create a plan to manage incidents (Data Breach Recovery Plan), monitor cybersecurity levels with an ongoing approach, and notify the CSIRT (www.csirt.gov.it) of any incidents that may occur. These measures should be proportionate to the specific risks, size of the entity, and potential severity of the incidents.
- **Entity classification:** The directive distinguishes between "essential entities" and "important entities," based on the criticality of the services offered and the potential impact of any disruptions. Essential entities are subject to more stringent safety requirements than important entities.
- **Audits and inspections:** the NIS Competent National Authority may subject entities within the scope of Legislative Decree 138/2024 to audits, inspections, or may make requests for access to data and documents.
- **Penalties for non-compliance:** The NIS 2 Directive provides administrative fines for essential and important entities that fail to comply with cybersecurity obligations. Penalties vary depending on the severity of the violation and the type of entity involved.
  For essential entities:
  Penalties of up to 10,000,000 euros or 2 percent of the previous year's total annual worldwide turnover, whichever is higher.
  For major entities:
  Penalties of up to 7,000,000 euros or 1.4 percent of the previous year's total annual worldwide turnover, whichever is higher.
  It is important to note that public administrations may be subject to fines ranging from 25,000 to 125,000 euros.

The firm remains available for clarification.

SGB & Partners – Commercialisti

SGB & Partners
Sede legale
Via Meuccio Ruini, 10
42124 Reggio Emilia
CF e Piva 01180810358

Tel. +39 0522 941069
Fax +39 0522 941885
Mail info@sgbstudio.it
Web www.sgbstudio.it