CYBERFERO

# NIS2

## Network and Information Security


**We analyze your situation to evaluate compliance with the NIS2 DIRECTIVE.**

https://www.cyberfero.com

# NIS2 Directive, what is it?

The NIS2 Directive integrates with the various European regulations and guidelines on data protection and privacy: the objective is to strengthen cybersecurity measures especially in critical sectors and manage the complexities of the supply chain, establishing an essential regulatory framework.

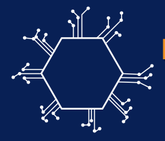
The new NIS2 Directive aims to improve the resilience and response capabilities to cyber incidents of the public and private sector and focuses, in particular, on fighting cyber crime and improving the management of cyber security at European and national level.


**Organizations have until October 17, 2024**
**to comply with the Regulations and not incur sanctions.**

# Who is it aimed at?

**The NIS2 Directive is aimed at companies, institutions and administrations belonging to the following sectors:**


Markets online


Infrastructure digital


Utilities


Machines and Equipment


Sector banking


Postal services and shipping


Financial market infrastructure


Products food


Assistance Healthcare


Online search engines


Vehicles a motor


Waste management


Computers and electronics


Transport


Chemical and medical products


Services of cloud computing

# Does your company not fall within the sectors listed above?

If your business operates in a field not explicitly listed in the list above, it is essential to also carefully consider the nature of your customers. Some of them may be subject to requirements that require collaboration with suppliers who fully adhere to the provisions of the NIS2 Directive.

# What are the sanctions if I don't comply?

**Member States may impose financial penalties on entities that do not comply with the Directive.**

## Essential Subjects

MAXIMUM SANCTIONS STARTING FROM

***€10 MILLIONS**

or

**2%** of turnover annual global

*The sanction ceiling can be arbitrarily raised at the time of transposition by the Government.

## Important Subjects

MAXIMUM SANCTIONS STARTING FROM

***€7 MILLIONS**

or

**1,4%** of turnover annual global

*The sanction ceiling can be arbitrarily raised at the time of transposition by the Government.

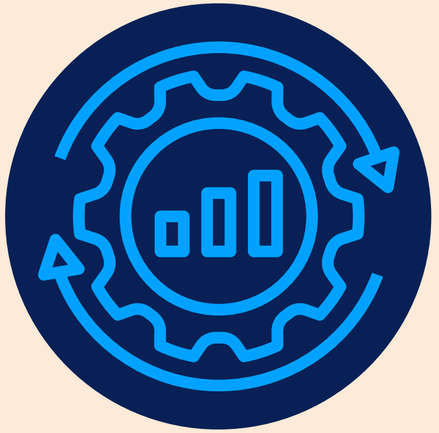
# What do we do for your company?

## Test

We carry out targeted tests to verify compliance with the NIS2 Directive, ensuring that your organization meets the required standards. We use advanced methodologies to evaluate your cybersecurity against emerging threats.

## Analysis

We review your security infrastructure to determine its compliance with the requirements of the NIS2 Directive. Through in-depth analysis, we identify vulnerabilities and risks, providing a clear picture of your current situation.



## Direct

We identify and report to you deficiencies in your security infrastructure in relation to the requirements of the NIS2 Directive. We offer precise guidance on what to improve to ensure full regulatory compliance and strengthen your defense against cyber threats.

# The main obligations for them companies:

## The obligations required by the NIS2 Directive concern the following areas:

The management bodies must approve the risk management measures adopted by the Organization, follow adequate training and guarantee similar training to their employees.

## Risk Management:

The subjects are required to adopt technical, operational and organizational measures to manage the risks posed to the security of the IT and network systems that the subjects use in their activities or in the provision of their services.

## Operational continuity:

Entities must ensure the continuity of their services and minimize the impact of any disruptions through measures such as backup management, disaster recovery and crisis management.

## Supply chain security:

Individuals are called upon to protect their supply chain by assessing the specific vulnerabilities of their suppliers and the adequacy of their cybersecurity practices.

## Incident reporting:

Entities are obliged to report incidents that have a significant impact on the provision of their services to their respective CSIRTs or competent national authorities (early warning within 24 hours and full/supplementary notification within 72 hours of becoming aware of the significant incident).

CYBERFERO

## For over 10 years a leader in the Cybersecurity and Security sector

Cyberfero is a Managed Security Service Provider (MSSP) specializing in providing comprehensive security solutions for businesses of all sizes. As a trusted partner, we offer a broad range of security services designed to protect your organization from cyber threats, data breaches and other security risks.

Website

## Contacts


+39 0522 1685330

https://www.cyberfero.com

info@cyberfero.com

Via Statuto 3, 42123 - Reggio nell'Emilia (RE)