ECCO

European Cybersecurity COmmunity

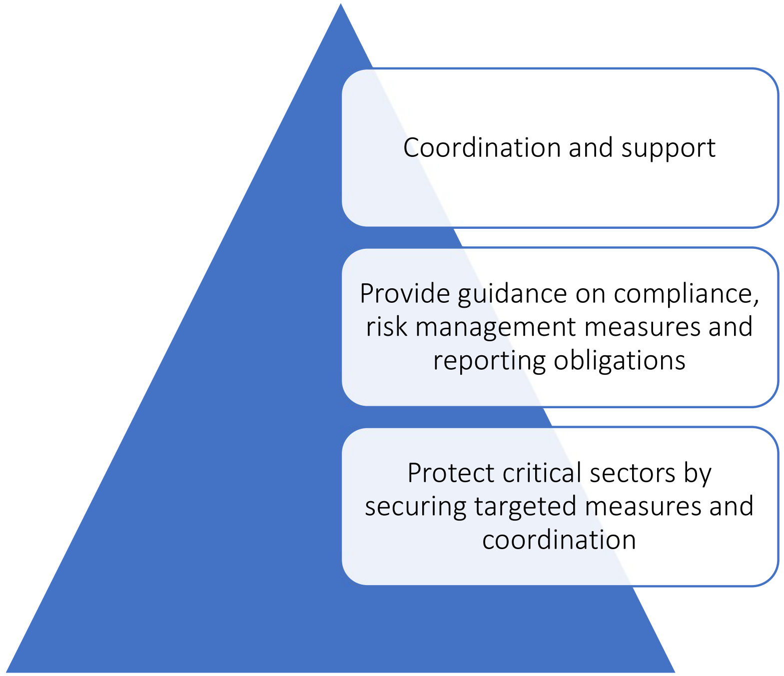
Understanding the new NIS2 Directive: cybersecurity requirements and their practical application for the EU Space Sector

ECCO Community-driven Knowledge Sharing Events

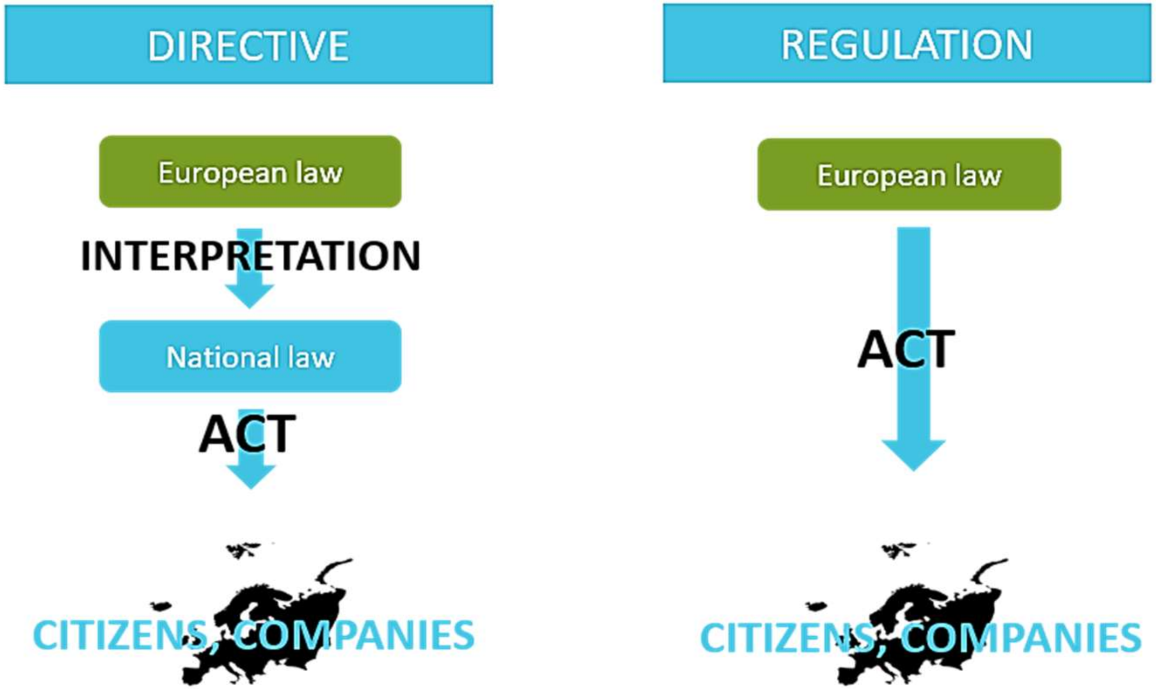
Disclaimer

- *These sessions are ECCO community-driven and expert-led, reflecting the collective knowledge and contributions of the members of the ECCO Community Groups. They are designed as knowledge-sharing events to build/animate the cybersecurity Community Groups on key topics and share valuable insights among stakeholders.*
- *The information and opinions in this document are provided "as is" for general purposes only.*
- *Experts are encouraged to ensure their presentations are accurate and up-to-date.*
- *The views expressed in this webinar are purely those of the experts and may not, in any circumstances, be interpreted as stating an official position of the European Commission (EC), the European Cybersecurity Competence Centre (ECCC), the ECCO project, or any other EU institution, body or agency. The European Commission does not guarantee the accuracy of the information included in this webinar, nor does it accept any responsibility for any use thereof.*
- *References to specific commercial products, processes, or services do not imply endorsement or recommendation, and this webinar should not be used for advertising purposes.*

NCCs' crucial role in building a strong cybersecurity community under NIS2



Understanding Directives vs. Regulations before delving into NIS2



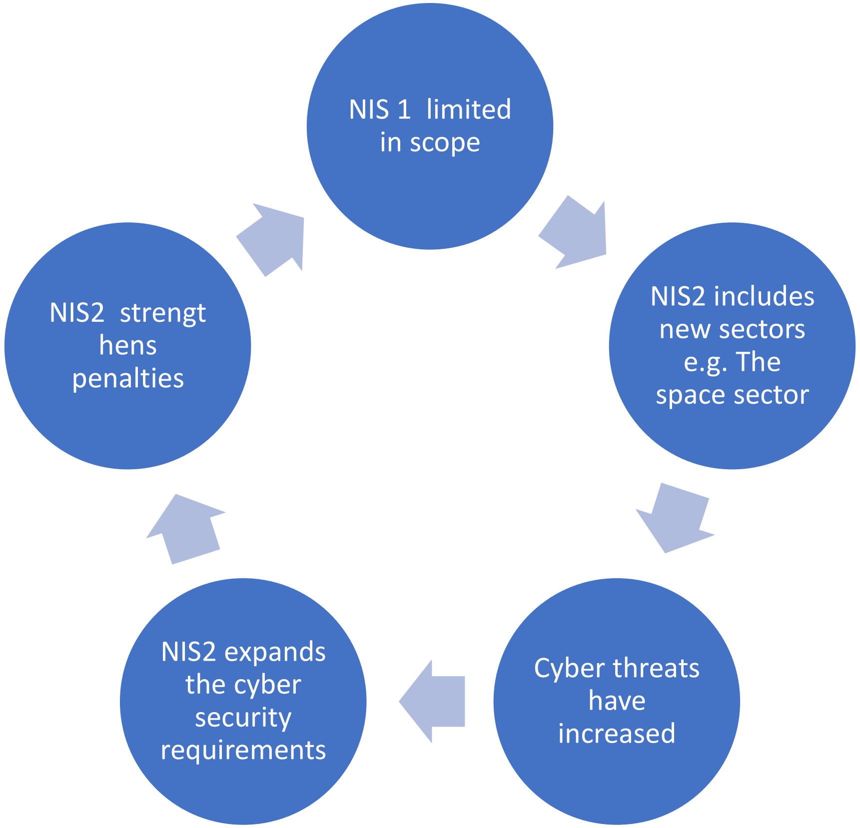
Consequences if a Member State fails to implement the NIS2 Directive before the deadline?

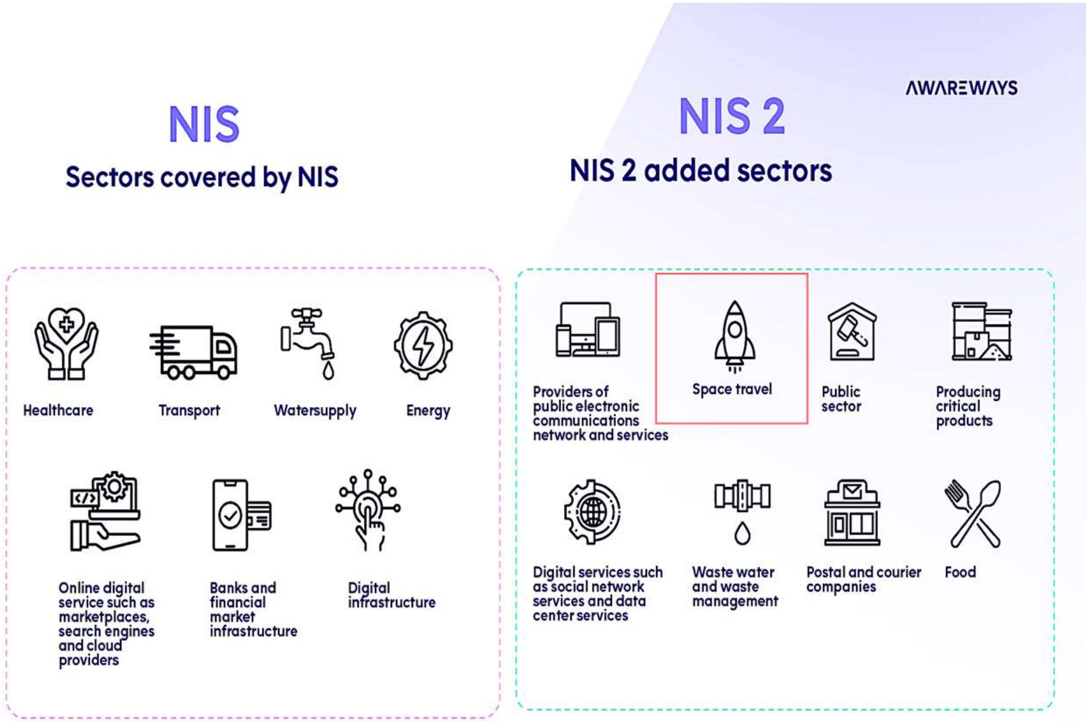
Private parties can require the Member State to provide a regulatory environment compliant with NIS2

Compliance requirements in case the Directive is not transposed into national legislation

- No requirement to comply with NIS2 (Member States' obligation)
- Voluntarily align with cybersecurity measures within NIS2

Why NIS2 ?


NIS 1 limited in scope
NIS2 includes new sectors e.g. The space sector
Cyber threats have increased
NIS2 expands the cyber security requirements
NIS2 strengt hens penalties


AWAREWAYS
NIS
Sectors covered by NIS
Healthcare
Transport
Watersupply
Energy
Online digital service such as marketplaces, search engines and cloud providers
Banks and financial market infrastructure
Digital infrastructure
NIS 2
NIS 2 added sectors
Providers of public electronic communications network and services
Space travel
Public sector
Producing critical products
Digital services such as social network services and data center services
Waste water and waste management
Postal and courier companies
Food


NIS2
Directive

Specific considerations for the space sector

- **Specific considerations for the space sector**
  - **Cybersecurity risks**
    - The space sector is a prime target for sophisticated cyber attacks
    - Identifying and addressing cyber risks is essential
  - **Reporting requirements**
    - Any significant incident must be reported
    - Timely identification and response to cybersecurity incidents
  - **Registration**
    - Register with the competent authority
    - Where appropriate, register with the sectoral authority
  - **Impact on the space market**
    - Smaller space organizations must find it challenging to comply
    - Impact on the ability to compete in the space market
  - **Compliance costs**
    - Internal assessment vs NIS2 requirements
    - Investing in enhanced cybersecurity measures may be needed

ECCO

European Cybersecurity COmmunity

Does your organization fall within the scope of the NIS2 Directive?

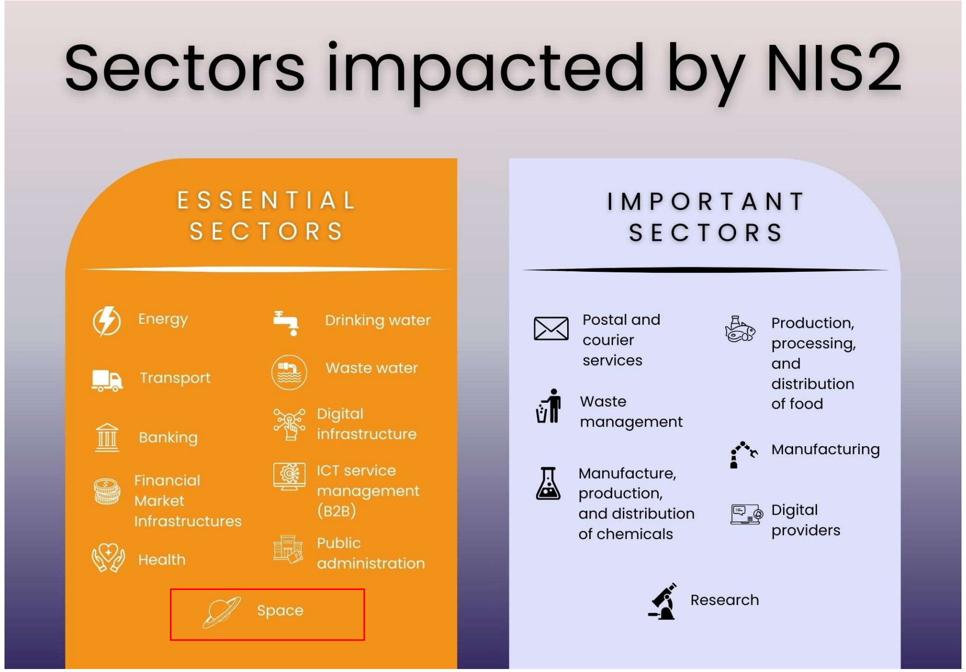
Are you impacted by the NIS2 Directive?

There are three general criteria (location, size, industry) that define which organizations must comply with the NIS 2 Directive:

1) Location: services provided or activities carried out in any country in the European Union (no matter if based in the EU or not), and

2) Size (art. 2) — mid-sized or large organizations, and

3) Industry — operate in any of the 18 sectors (energy; transport; banking; financial market infrastructures; health; drinking water; waste water; digital infrastructure; ICT service management (business-to-business); public administration; space; postal and courier services; waste management; manufacture, production and distribution of chemicals ; production, processing and distribution of food; manufacturing; digital providers; research)



Fundamental elements for space sector's entities

Entities established in the EU, operating in the space sector, will likely be in scope with the NIS2 Directive because:

- They fall within the space sector – operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties that support the provision of space-based services
- They manufacture spacecraft/aircraft or related machinery or
- They manufacture electrical, electronic or communication equipment or various types of machinery or engines/turbines or related components or equipment or
- They provide digital infrastructure

Article 2

Scope

1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.

02022L2555 — EN — 27.12.2022 — 000.004 — 3

▼B

Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.

2. Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:

(a) services are provided by:

(i) providers of public electronic communications networks or of publicly available electronic communications services;

(ii) trust service providers;

(iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

Essential vs. Important entities: different obligations

- The same substantive obligations apply to both essential and important entities
- Essential entities are subject to stricter enforcerment and oversight obligations
- Member States shall ensure that the members of the management bodies of essential and important entities follow training and shall encourage essential and important entities to offer similar training to their employees
- Essential and important entities must take appropriate and proportionate technical, operational and organisational measures

Essential entities (reflect a higher level of criticality)	Important entities
Ex ante & ex post supervision = regular conformity assessments	Ex post supervision = on the basis of evidence that the entity isn't complying with the Directive
On site inspections (no more than annually) and off-site supervision	On site inspections and off-site ex post supervision
Regular and targeted security audits	Targeted security audits
Security scans	Security scans
Information requests i.e. obtain a copy of any document needed for the supervisiory mission e.g. the implementation of cybersecurity policies	Information requests i.e. obtain a copy of any document needed for the supervisiory mission e.g. the implementation of cybersecurity policies
Ad hoc audits for example after a significant incident	X

ECCO

European Cybersecurity COmmunity

Cybersecurity risk management requirements for entities operating in the space sector

Cybersecurity risk management measures for the space sector

- Proactive rather than reactive approach to risk management

- Entities are expected to implement industry-accepted and state-of-the-art cybersecurity measures

- The level of cybersecurity required depends on the level of risk that the company is willing to accept

Why cybersecurity risk management measures are crucial for your organization?

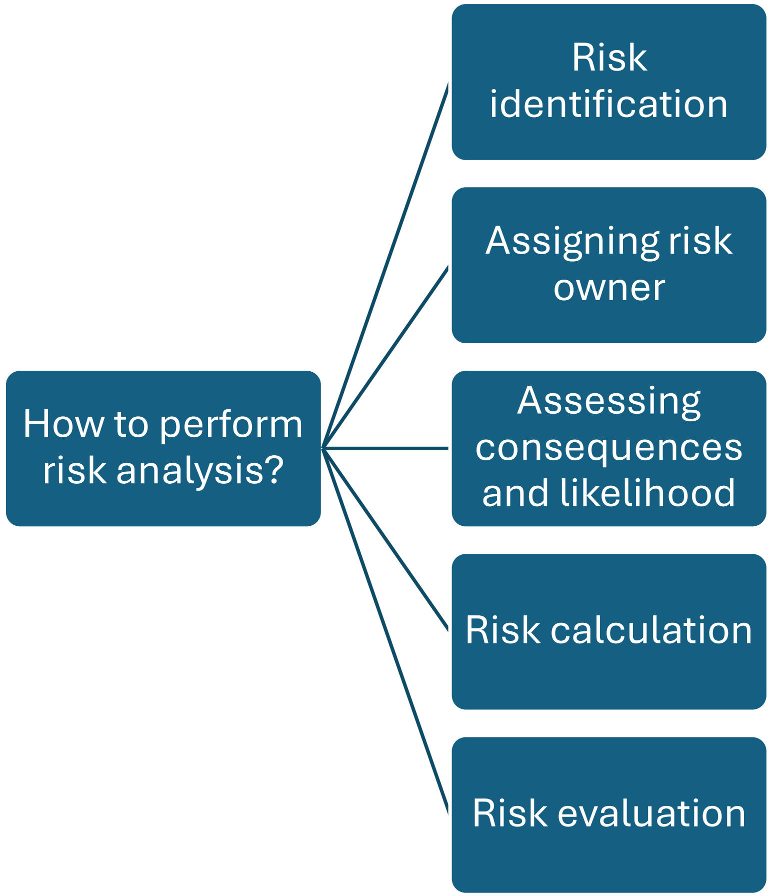
The CIA Triad

The CIA Triad	Definition	Example	Opposite of CIA Triad	How to achieve it?
Confidentiality	Information is not made available or disclosed to unauthorized entities	• Only people having authorisation can access the information	• Someone reads the content of a message not directed to them	• Encryption
Integrity	Property of accuracy and completeness	• Data is free from improper modification, errors or loss • It is recorded, used and maintained in a way that ensures its completeness	• The attacker not only will read the content of the message, but also modifies it	• Hashing
Availability	The timeline and reliable access to information and the ability to use it	• The authorized user has access to the data when and where it is needed, in the form and format required	• Information is destroyed	• Backups • Redundant system

- ISMS guarantees the information security of its information assets
- Information security ensures the CIA Triad
- Protecting sensitive information is more important than never

Risk analysis and information system security in the space sector

- The risk analysis should result in aligning each identified risk with goals, objectives, assets or processes
- The aim of risk analysis is to assess the impact and likelihood of identified risks and then evaluate them
- Risk assessment involves answering key questions e.g. Possible adverse events? Their causes? Their impacts? Likelihood?



Risk assessment process steps for entities operating in the space sector

- Identify the risks that harm the CIA Triad
- Choose the responsible and related partners
- Risk analysis (Quantitative OR Qualitative)
- Plan the responses and determine controls
- Implement risk responses and chosen controls
- Monitor risk improvements and residual risk

Risk identification

- Identify the assets
- Identify vulnerabilities
- Identify the current threat landscape
- Identify the risk owner

Risk analysis

- Impact of the risk
- Likelihood of the risk
- Risk level

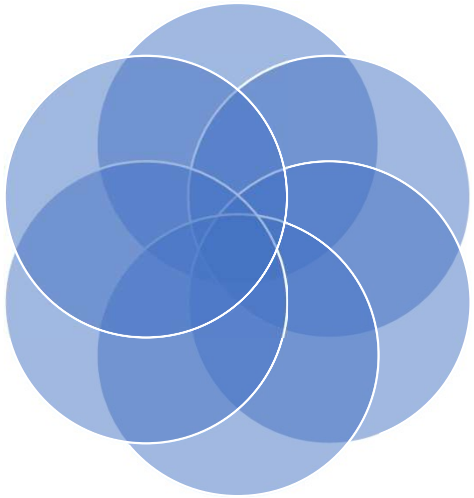
Risk evaluation

- Is the risk acceptable or does it require a treatment ?

Supply chain security under the NIS2 Directive

The NIS2 Directive introduces a number of requirements to conduct supply chain security assessments for particular products and services

To ensure compliance with its legal obligations, an entity may contractually require its suppliers or service providers to be certified with ISO27001



In order to guarantee a successful supply process, both entities and their experts should be involved in such risk assessments

Organisations are required to ensure the security of the supply chain to which they belong. Based on the risk in the supply chain, they must impose cyber security measures on their suppliers.

Implement robust security measures and work closely with suppliers to minimize potential cyber threats

It is essential to set up an efficient supplier risk management process, because not every supplier is equally critical and not every supplier requires the same cybersecurity requirements

Other cybersecurity risk management measures

- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Use cryptography and encryption
- Implement concepts for access control to systems and installations
- Use solutions for multi-factor authentication or continuous authentication, secure voice, video and text communication and if necessary, secure emergency communication systems within the facility

Key aspects:

Management bodies are required to **explicitly approve** the risk management measures

Management bodies can be held **liable**

Competent authorities can impose a **temporary prohibition of the exercise of managerial functions**

Member States can require infringing entities to publicly acknowledge the NIS2 breach and identify those responsible

ECCO

European Cybersecurity COmmunity

Key elements for the fulfillment of entities' obligations

Reporting obligations

New reporting requirements for space organisations

- Report any cyber incident that could impact the space infrastructure
- Challenges in terms of monitoring, detecting and responding to potential cyber threats
- Under the NIS2 Directive, entities are required to notify any incident that has a significant impact on the provision of the services

Three – staged reporting of significant incident :

1) Initial notification within 24 hours

2) Follow up notification within 72 hours

3**) Intermediate status report at the request of the National Competent Authority**

4) Final report within one month

A significant incident :

1) Has caused or is capable of causing severe operational disruptions of the services or financial loss for the entity concerned or

2) Has affected or is capable of affecting other natural or legal person by causing considerable material or non-material damage

Reference framework for NIS2 Directive compliance

- ISO 27001 is a comprehensive cybersecurity framework based on a set of processes and controls

- ISO27001 outlines the requirements for an ISMS

Key considerations for both large and small organisations :

- Ensure adequate coverage of top NIS2 requirements i.e. cyber risk management, incident response planning, access controls

- Maximise integration with existing security programs, policies and technologies

- Implementing ISO27001 requires time, financial resources and qualified personnel in order to demonstrate a commitment to information security

- Objectives must be consistent with the information security policy, measurable so that the progress can be tracked, achievable-realistic, relevant to the organization's goals and have a clear deadline

Consequences in case of non compliance with NIS2 Directive

- Supplier failure
- Financial losses
- Reduced business growth
- Personal liability of directors/management
- Fines
- Damage to reputation

Sanctions

- For essential entities:
  - **10 million euros**
  - Or **2%** of the company's worldwide annual turnover for the previous financial year
- For important entities:
  - Maximum fine of **7 million euros**
  - Or **1.4%** of their turnover