Building Trust in Digital Systems: Navigating the EU Regulatory Landscape

Nadia Liapi

Group Director

Governance, Risk & Compliance Services

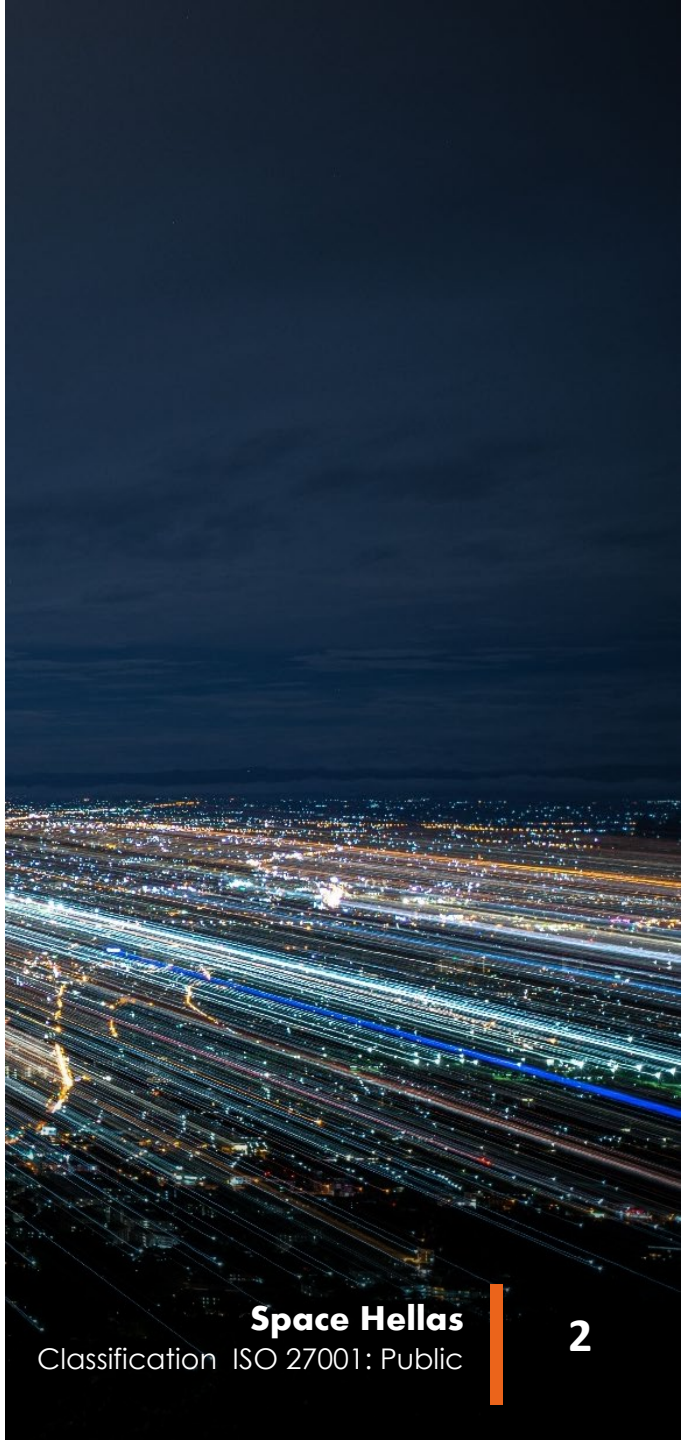
Space Hellas Group of Companies

SPACE

Classification ISO 27001: Public

www.space.gr

Agenda



GDPR

SPACE

Classification ISO 27001: Public

www.space.gr

General Data Protection Regulation (GDPR)

GDPR increases privacy for individuals and gives regulatory authorities the jurisdiction to act against companies that break new laws. This means:

Tough Penalties:
Fines up to
4% of annual global revenue
or **€20 million**
whichever is **greater**

The Regulation also applies to non-EU companies that process personal data of individuals in the EU

International data transfer will continue to be governed in accordance with the rules of the **European GDPR**

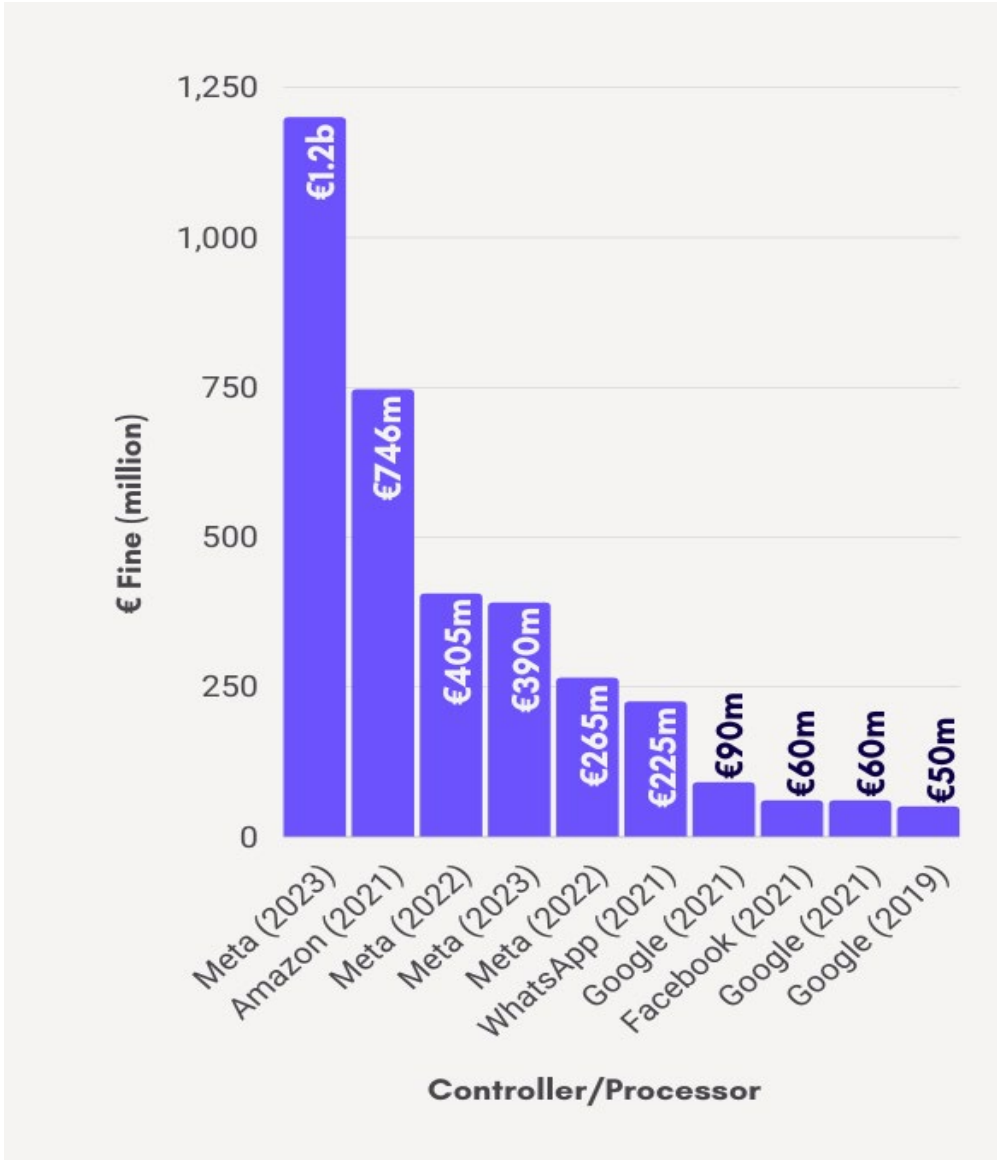
SPACE

Classification ISO 27001: Public

How GDPR Transformed the Landscape of Personal Data Protection

- **Companies are prioritizing data protection** and adapting to evolving privacy standards.
- **Data transfers** outside the EU are a key focus for ensuring the protection of EU citizens' data.
- **Guidance from the EDPB and national DPAs** is essential for organizations to achieve GDPR compliance.
- The GDPR has influenced the **proliferation of new privacy laws worldwide**.

The 10 biggest GDPR fines



What's next?

- Although the past 5 years have seen considerable progress in respect of compliance with the GDPR, we still have **a long way to go**. Organizations of all sizes need to do more to progressively improve their compliance in an ever-changing global privacy landscape.
- This is especially evident with the **rapid proliferation of AI** and large language models (like ChatGPT) and their ability to harvest vast amounts of personal data for training
- Organizations need to ensure that their utilization of these **new and emerging technologies** remains compliant

NIS2

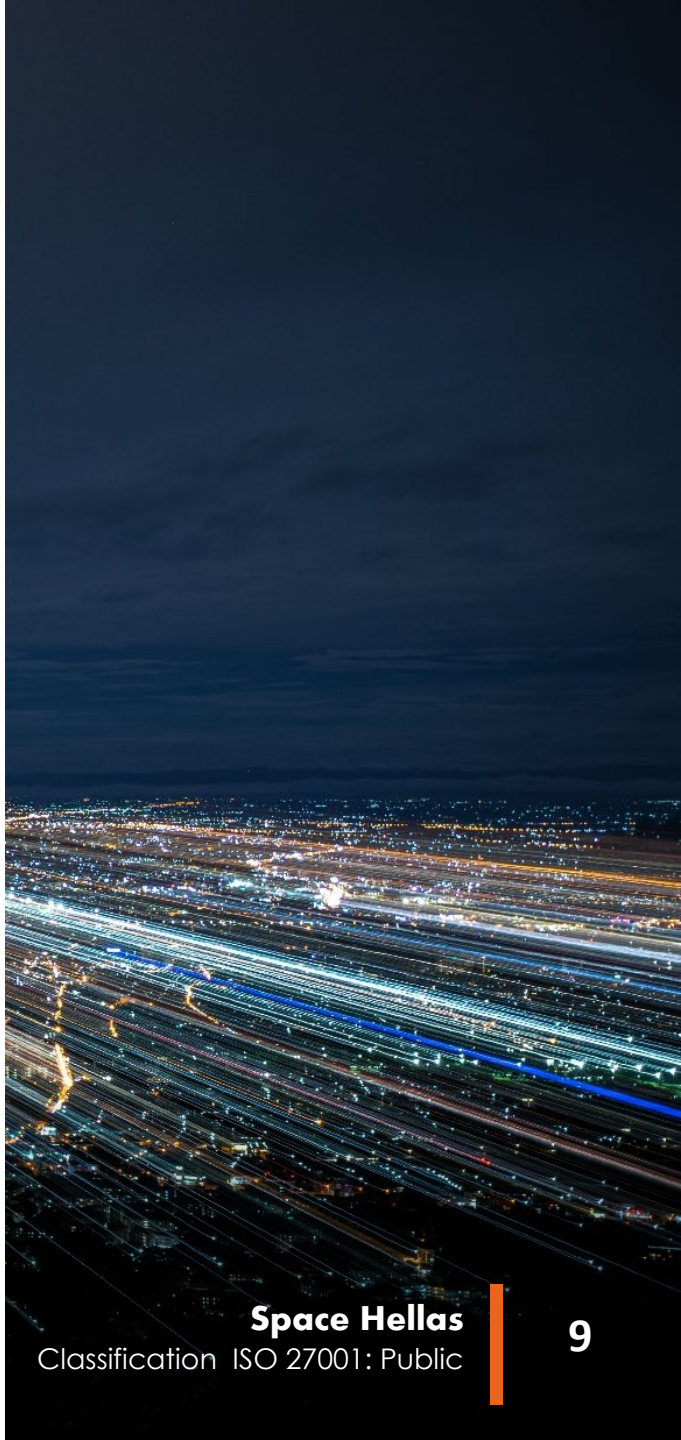
SPACE

Classification ISO 27001: Public

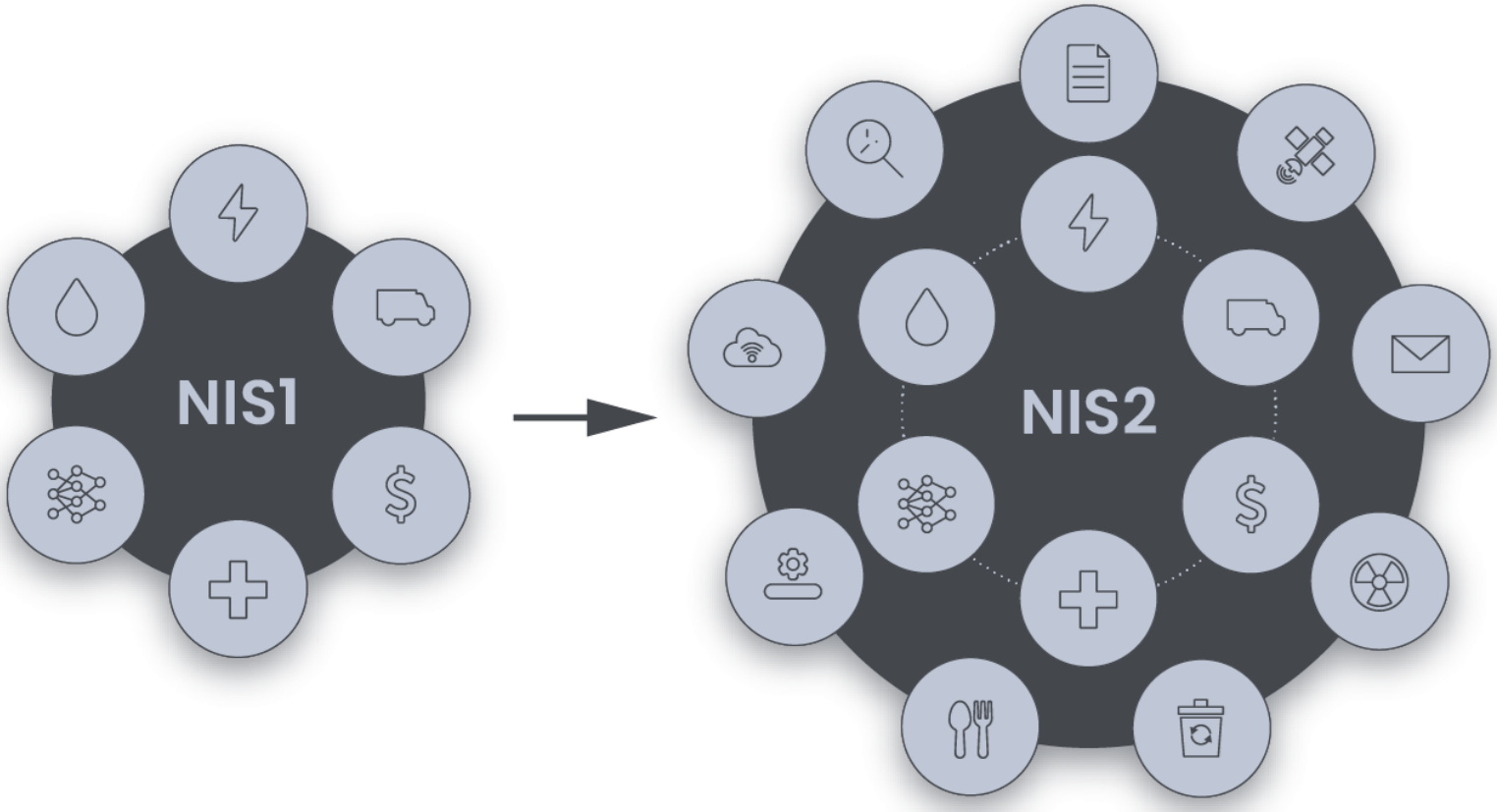
www.space.gr

Necessity of the directive

- The reliability and security of systems are crucial for **economic and social activities**, as well as for the functioning of the internal market
- The frequency, extent and impact of **security incidents** have skyrocketed and pose a serious risk to public confidence and the EU economy.
- **Differences in** the level of preparedness in **Member States** lead to unequal protection of consumers and businesses



Organizations covered by NIS 2



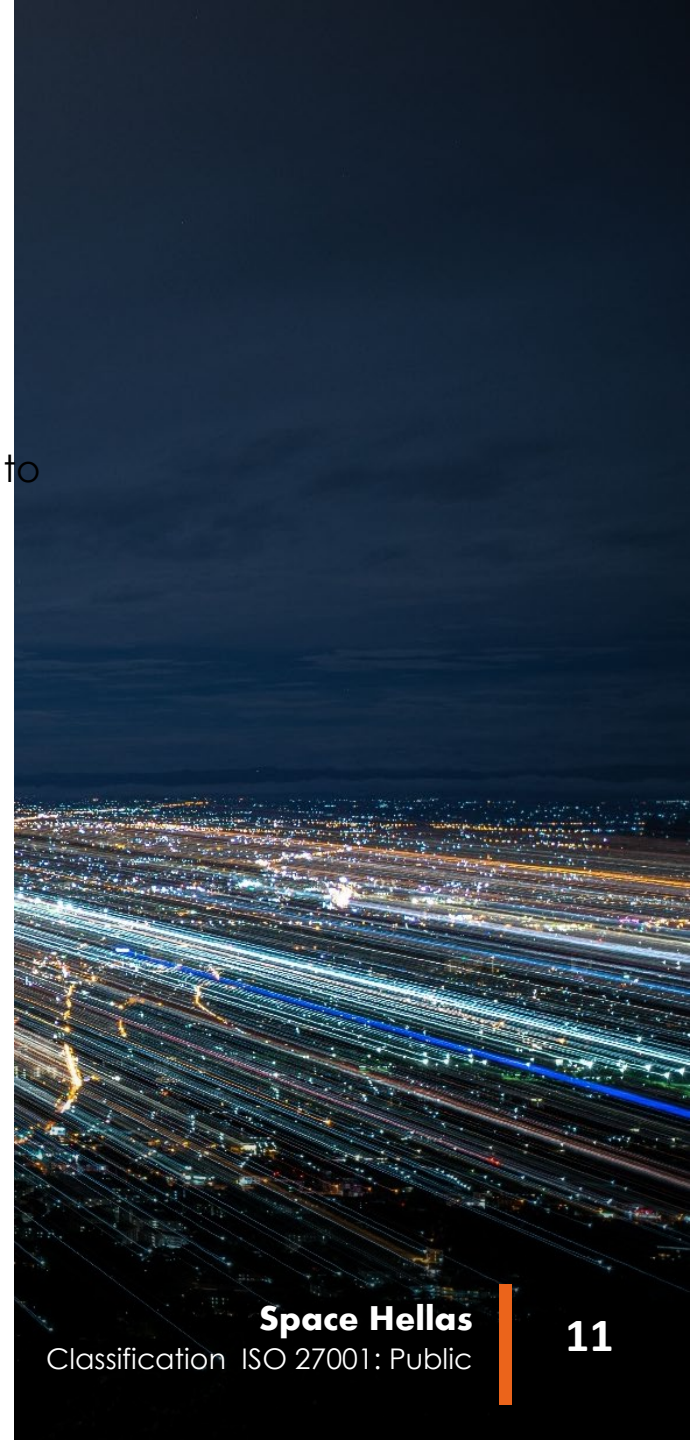
Basic and Important Entities

High Criticality:

- energy
- transfers
- Bank System
- financial market infrastructure
- health
- drinking water
- effluent
- digital infrastructures
- ICT service management (business to business)
- public administration entities
- space

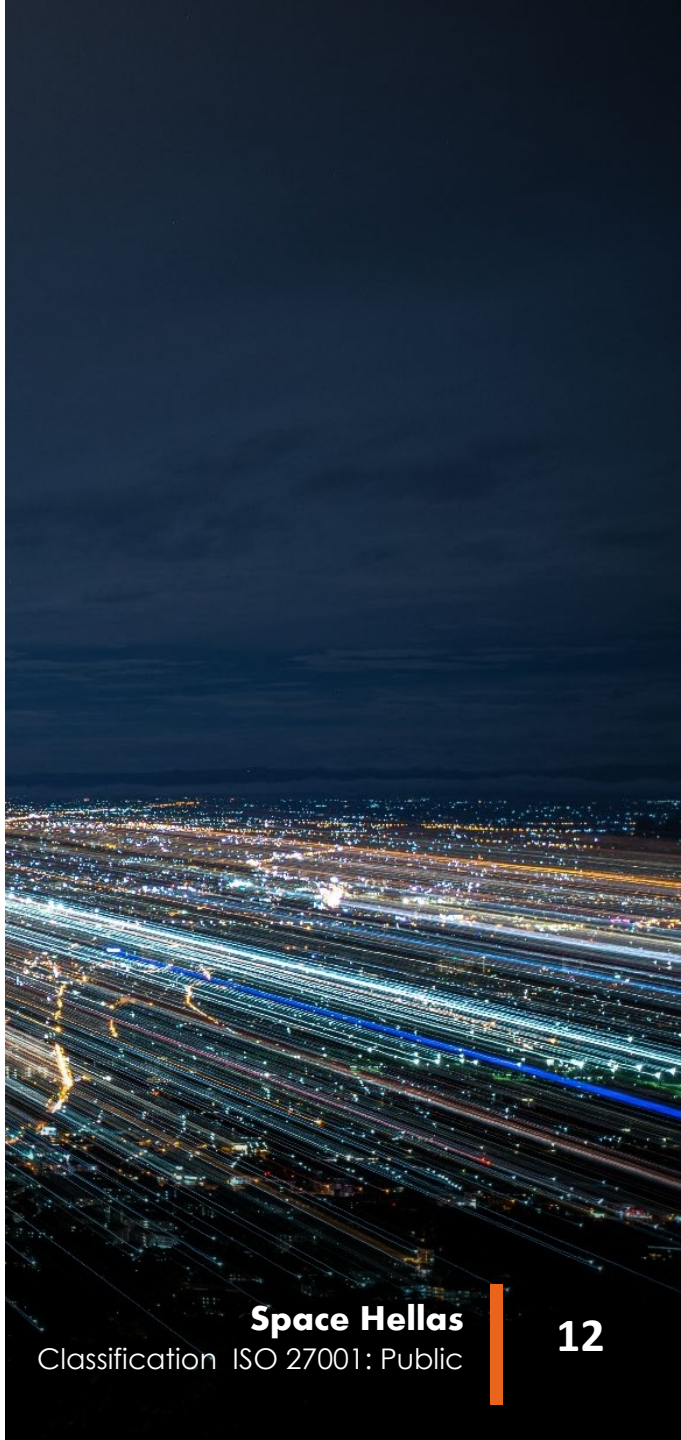
Other critical infrastructure:

- courier services
- waste management
- manufacture, production and distribution
- chemical products
- production, processing and distribution of food
- construction sector
- digital providers
- research



Fundamental Principles

- Remedial actions to **cover vulnerabilities** appearing in the European database.
- **Risk assessment** considering the cyber threat landscape by performing risk analysis.
- Assessing the general level of cyber security **awareness** and conducting **trainings** within the organization.
- **Timely notification** of important incidents to the CSIRTs and cooperation with the competent supervisory authorities.
- Taking **appropriate technical and organizational measures**.
- **Policies and procedures for evaluating** the effectiveness of cybersecurity risk management measures.



Criticality of adaptation

Obligation to **comply by 10/2024**

Businesses worldwide **lose** nearly 1% of GDP to cybercrime

The organization will be **audited by customers** and manufacturers who will assess the level of safety implemented under the directive

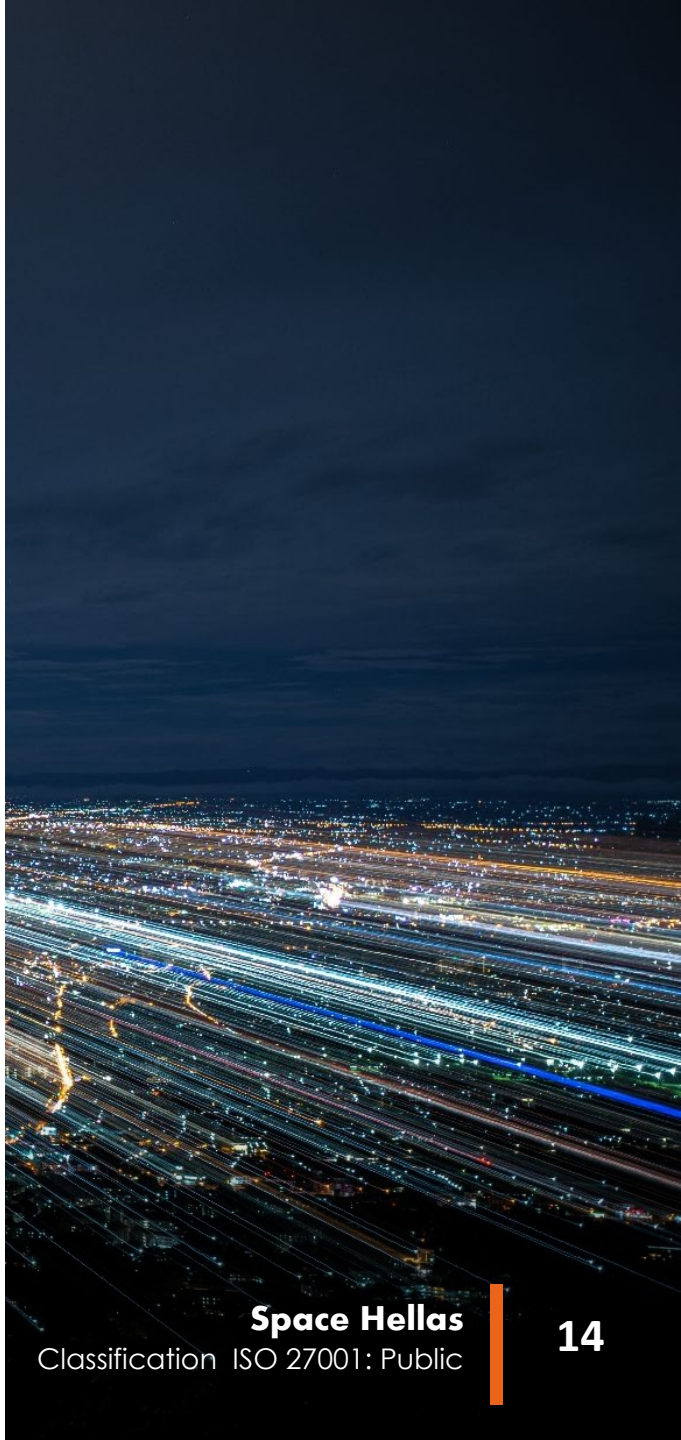
Prevention, identification and response to **risks**

Protection of **networks**, information systems from **natural disasters**, unauthorized access, etc

Protection against system failures, human errors and malicious actions and contribution to **data recovery**

Penalties for non-compliance

- Key Entities: Administrative fines up to a maximum of EUR 10,000,000 or 2% of the previous financial year's total global annual turnover for the Key Entities, whichever is greater
- Significant entities: Administrative fines of a maximum of EUR 7,000,000 or 1.4% of the previous financial year's total global annual turnover for the significant entities, whichever is greater
- **Temporary ban on the exercise of managerial duties** by any natural person exercising managerial duties at the level of managing director or legal representative (we will see how it will be provided in the new law)



DORA

SPACE

Classification ISO 27001: Public

www.space.gr

What is DORA?

- A binding EU regulation on **digital operational resilience for the financial sector**
- DORA seeks to address potential systemic and concentration risks posed by the sector's **reliance on ICT third-party providers (TPPs)**.
- DORA attempts to accomplish this by compelling regulated entities to **follow bloc-wide rules for the protection, detection, containment, recovery, and repair of capabilities against ICT-related incidents**.

5 Pillars and their Implications

Sectors covered by DORA

- Credit institutions
- Payment institutions
- e-money institutions
- Investment firms
- Crypto-asset service providers
- Central securities depositories
- Managers of alternative investment funds
- UCITS management companies
- Administrators of critical benchmarks
- Crowdfunding service providers
- ICT third-party service providers

If you think

COMPLIANCE is EXPENSIVE

try non-compliance

Empowering

Your Digital Transformation Journey

Thank you

Classification ISO 27001: Public

www.space.gr