SMARCO

SMARt COmmunities Skills Development in Europe

Cybersecurity

Short Term Course - Unit 3

Cefriel

POLITECNICO DI MILANO

Co-funded by the European Union

smarco

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Aim of the course

This course aims to strengthen the **resilience of smart communities** by promoting a culture of digital responsibility and awareness. Participants learn how everyday actions and informed behaviors contribute to collective cyber hygiene, making the community safer against evolving threats. Special attention is given to understanding and resisting social engineering, empowering individuals to recognize manipulation and protect both personal and shared digital environments.

Co-funded by the European Union

smarco

Unit 3

Cybersecurity compliance

Co-funded by
the European Union

smarco

AGENDA

- The necessity for a legal framework on Cybersecurity
- An overview
- Subject-relevant laws (NIS 2, GDPR)
- Product-relevant laws (CRA, AI Act)
- Cybersecurity in Smart Communities (CER)

Co-funded by the European Union

smarco

The necessity

Within the European framework, ENISA recorded 4,875 incidents in the period from 1 July 2024 to 30 June 2025, revealing:

- DDoS attacks dominant
- Ransomware as the most critical threat
- Hacktivism prevalent
- Sophisticated hybrid attacks

Source: ENISA threat landscape, October 2025

Co-funded by the European Union

smarco

A European complementary approach

The EU's Cybersecurity Strategy for the Digital Decade (dec 2020)

- Strengthening the EU's cyber resilience
- Promoting common security standards for digital products and services
- Creating a secure digital single market
- Protecting critical infrastructure and supply chains
- Promoting European digital sovereignty

Co-funded by the European Union

smarco

The EU Approach- Not without criticism

vs.

Co-funded by the European Union

smarco

The EU Approach Not without criticism

PROs

- Legal certainty
- Common level playing field
- It provides access to the single European market with hundreds of millions of potential consumers.
- Brussel's effect (Anu Bradford)
- Better protection of citizens and humans (Human rights)

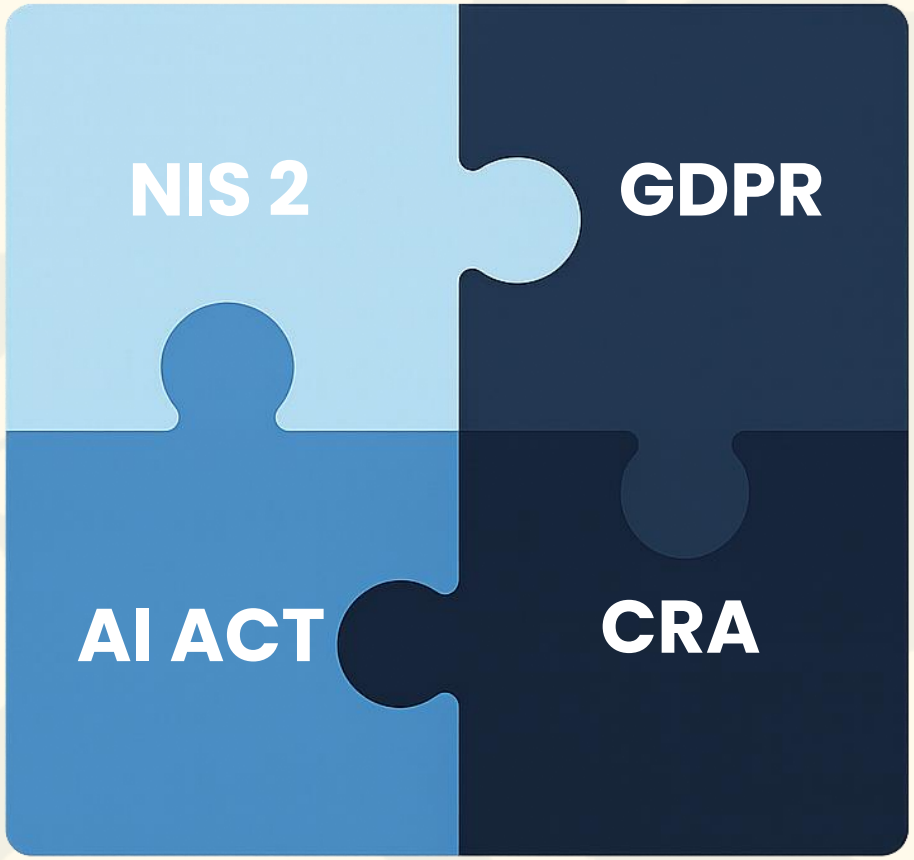
CONs

- Stifle innovation
- Fragmentation
- Competitive delay
- Importance of bureaucracy
- Costs for enterprises.

Co-funded by the European Union

smarco

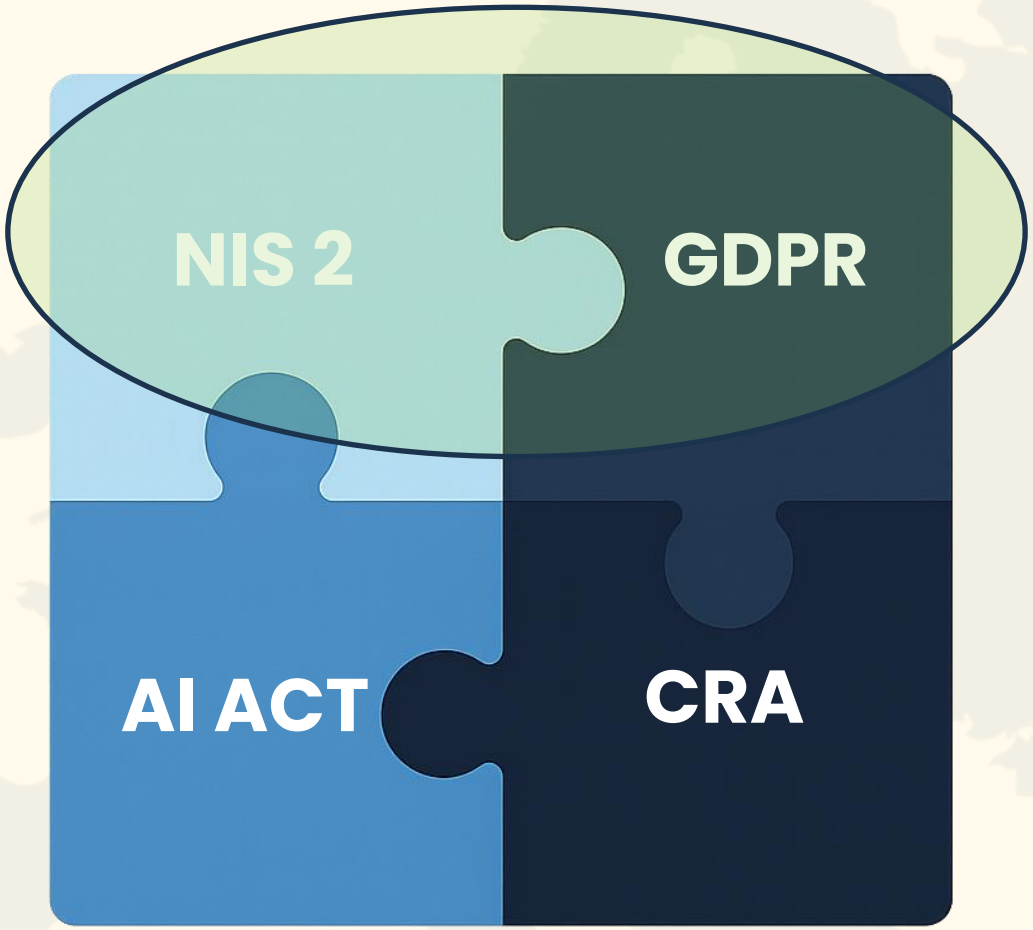
The EU Approach



Co-funded by
the European Union

smarco

The EU Approach

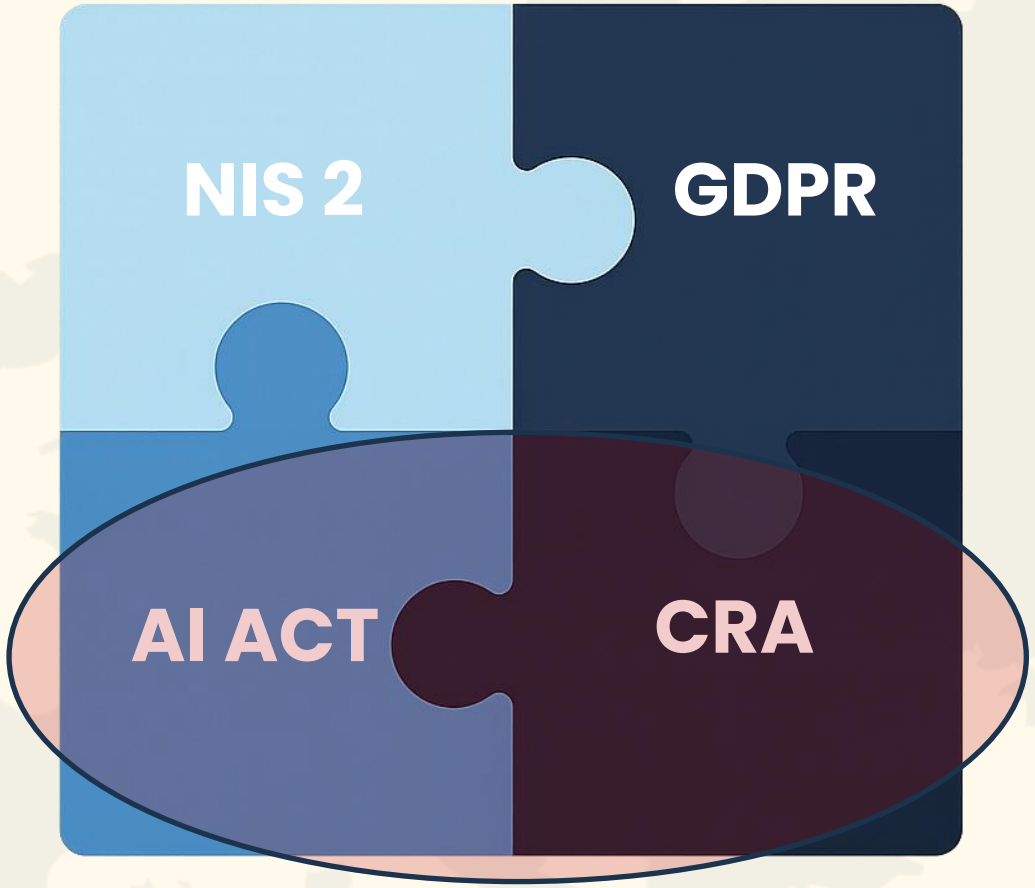


Focus on the subject (natural or legal person)

Co-funded by the European Union

smarco

The EU Approach



Focus on the product/system

Co-funded by the European Union

smarco

Network and Information Systems 2

Scope: Who is Affected? (Sectors).
Essential Entities (Examples):

- Energy: Electricity, oil, gas, district heating and cooling.
- Transport: Air, rail, water, and road transport.
- Health: Healthcare providers (hospitals, clinics, reference labs).
- Digital Infrastructure: Internet Exchange Points (IXPs), DNS service providers, TLD name registries.
- Water: Supply and distribution of water.
- Finance: Credit institutions, financial market infrastructures.
- Public Administration.

Important Entities (Examples):

- Digital Providers: Managed service providers, cloud computing services, data center services.
- Postal and Courier Services.
- Waste Management.
- Manufacturing: Medical devices, pharmaceutical products, and certain critical machinery.
- Food Production and Distribution.

Co-funded by the European Union

smarco

NIS 2: A risk-based approach

Co-funded by the European Union

smarco

NIS 2- Requirements overview

Organisational requirements

Risk assessment
Education and awareness (both for C-level and employees)
Policies and documented procedures
Incident communication and management
Business Continuity Plan
Vulnerability managment

Technical requirements

Antivirus
Firewall
Encryption (previous Unit)
Physical security
Tests
Updates
Back-ups
Strong passwords

Co-funded by the European Union

smarco

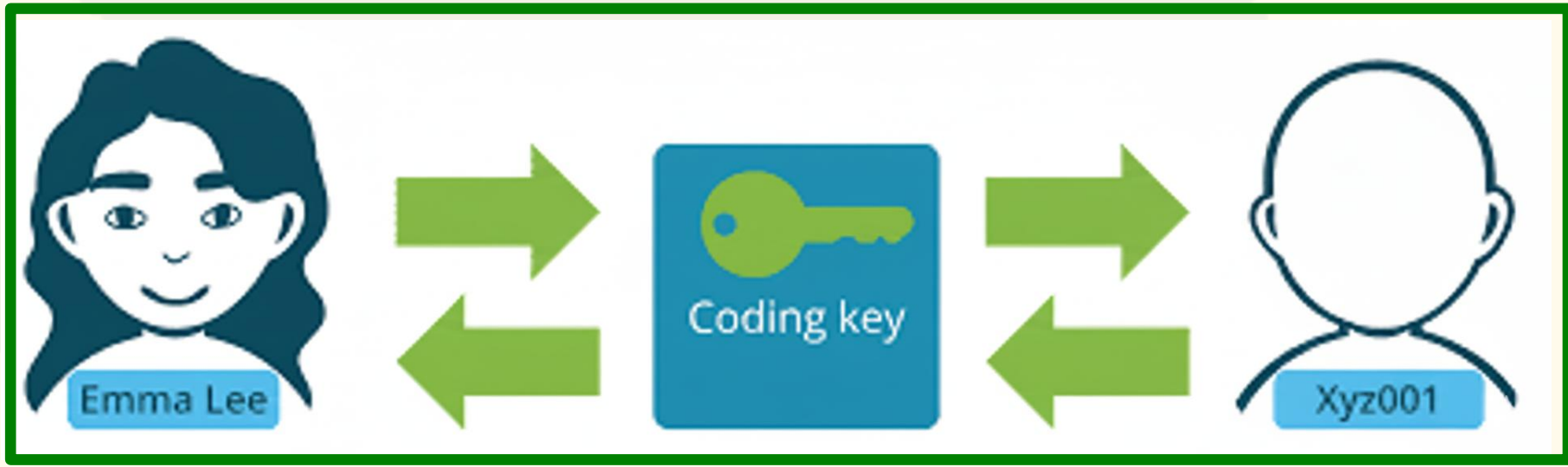
GDPR vs. NIS 2

GDPR applies to **personal data** (Regulation)

NIS concerns Network and Information Systems **data security** (Directive)

Article 32 GDPR: " (…) *the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*"

Example: pseudonymisation



Co-funded by the European Union

GDPR

The GDPR is oriented for the person (physical) protection, therefore introduces new rights such as the **right to be forgotten**, access right, right to portability, right to object, right of rectification.

Co-funded by the European Union

smarco

AI Act

Goal: To ensure AI systems placed on the EU market and used in the Union are safe, transparent, non-discriminatory, and respectful of fundamental rights.
Scope: Regulates the development, placement on the market, and use of AI systems and General Purpose AI (GPAI) models within the EU. It aims to make Europe a global hub for trustworthy AI.
Applicable To:
•Providers (Developers): Entities that develop or place an AI system or GPAI model on the market.
•Deployers (Users): Entities that use an AI system under their authority in a professional capacity (e.g., companies using an AI hiring tool).
•Importers/Distributors of AI systems.

Co-funded by the European Union

smarco

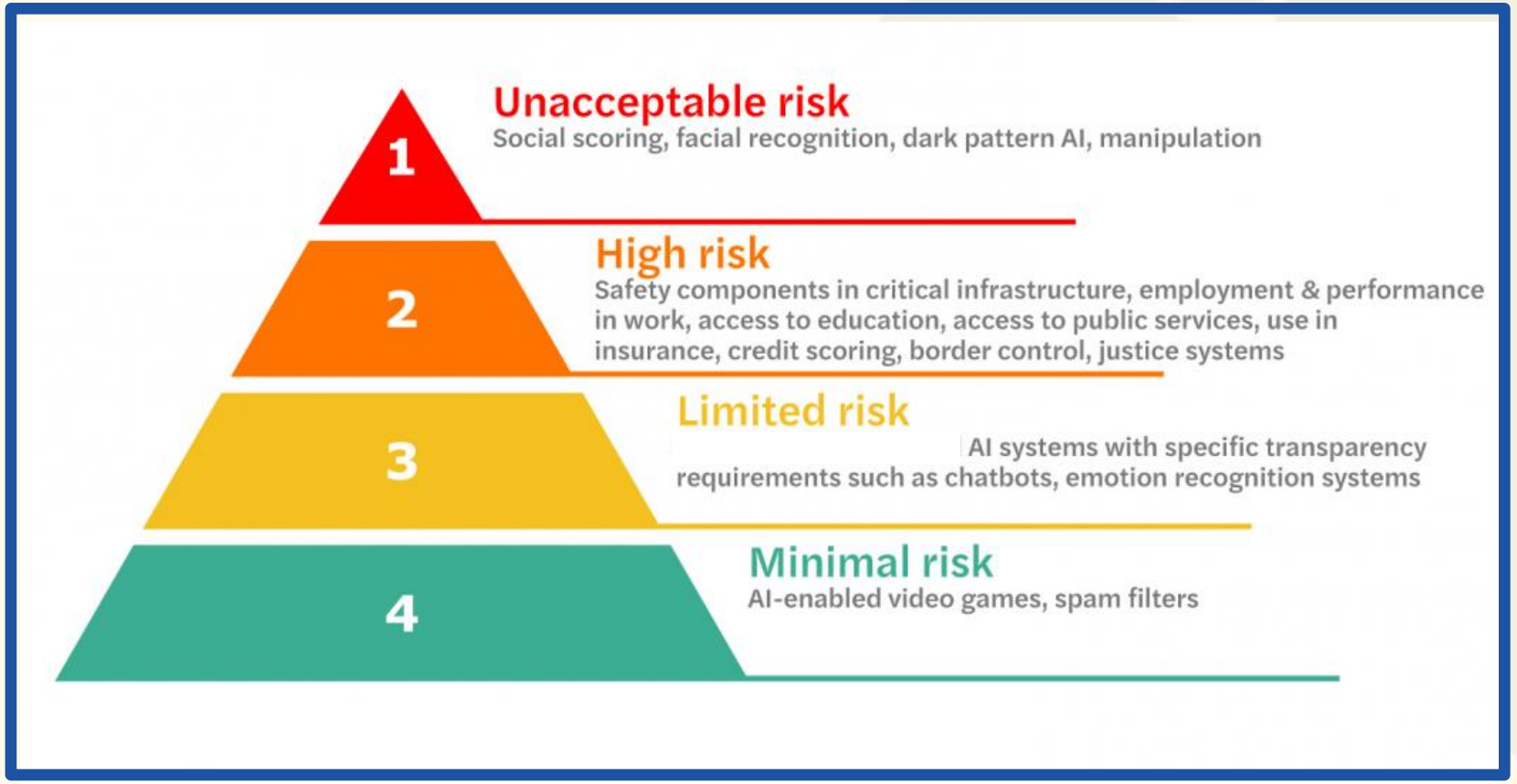
AI Act

Article 3(1) AI Act: **"AI system"** means a machine-based system that is designed to operate with varying levels of **autonomy** and that **may exhibit adaptiveness after deployment**, and that, for explicit or implicit **objectives**, **infers**, from the input it receives, how to generate **outputs** such as **predictions, content, recommendations, or decisions** that can influence physical or virtual environments.

Co-funded by the European Union

smarco

AI Act



Risk categories in the AI Act

Co-funded by the European Union

smarco

AI Act – Some key requirements

- **For High-Risk AI:** Rigorous requirements across the system lifecycle, including:
- Implementing a Risk Management System.
- Ensuring high-quality Data Governance (training, validation, testing data).
- Maintaining Technical Documentation and Record-keeping (automatic logging).
- Mandating **Human Oversight** and a high level of **Robustness, Accuracy, and Cybersecurity**.
- Mandatory registration in an **EU Database**.
- **For general Purpose AI Models:** Transparency and compliance with EU copyright law.

Co-funded by the European Union

smarco

Cyber Resilience Act – CRA

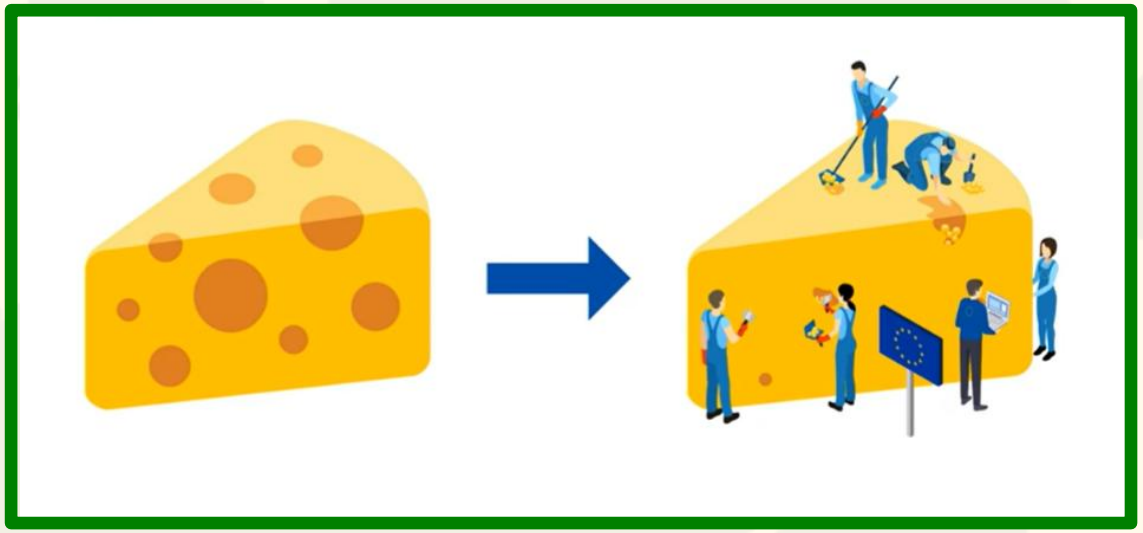
Goal: To set a **horizontal legal framework** establishing mandatory cybersecurity requirements for all products with digital elements (hardware and software) placed on the EU market.

Objectives:

Ensure manufacturers improve security throughout the entire product lifecycle.

Reduce vulnerabilities and the frequency/cost of cybersecurity incidents.

Enhance transparency of security properties for consumers and businesses.



Co-funded by the European Union

smarco

Cyber Resilience Act – CRA

Scope: Products with Digital Elements (PDEs)
Applies to any **product with digital elements** whose intended purpose or foreseeable use includes a direct or indirect logical or physical connection to a device or network (e.g., IoT devices, operating systems, routers, software components, etc.). They're classified in critical, important and default products.

Commercial Activity: The law applies when PDEs are **made available on the market in the course of a commercial activity**, whether for payment or free of charge. This includes many forms of commercial open-source software (OSS).

Co-funded by the European Union

Cyber Resilience Act – CRA

Key Manufacturer Obligations

I. Product Cybersecurity Requirements (Essential Requirements - Annex I)

Security by Design & Default: Integrate security from the initial design phase, minimizing the attack surface. Products must be delivered with secure default configurations.

Vulnerability Mitigation: Ensure protection from unauthorized access (e.g., strong authentication, access control) and protect the confidentiality and integrity of data (e.g., encryption).

Technical Documentation: Create and maintain a Software Bill of Materials (SBOM), a cybersecurity risk assessment, and technical documentation for at least 10 years after the product is placed on the market.

II. Vulnerability Handling Processes

Lifecycle Support: Manufacturers must define and implement policies for vulnerability handling and provide security updates without delay and free of charge for the product's expected support period (minimum of 5 years).

III. Mandatory Reporting (Effective Sept 2026):

Notify national CSIRTs/ENISA of any **actively exploited vulnerability** and any significant cybersecurity incident affecting the product **within 24 hours** of becoming aware.

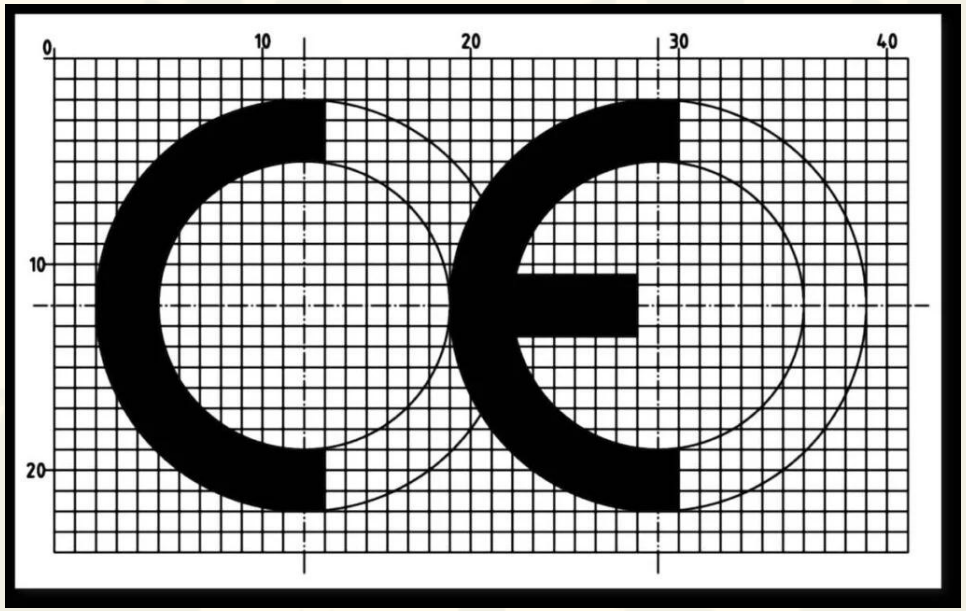
Public Disclosure: Publicly disclose information about fixed vulnerabilities, once the update is available.

Co-funded by the European Union

smarco

Cyber Resilience Act – CRA

III. Conformity Assessment & CE Marking
Manufacturers must perform a **conformity assessment** (self-assessment or third-party audit, depending on the product's criticality) to demonstrate compliance.
The product must bear the **CE Mark** to indicate compliance with CRA requirements before being placed on the EU market.



Co-funded by the European Union

Cybersecurity in Smart Communities

A **"renewable energy community"** is a local, member-driven organization (like a cooperative) that lets people, small businesses, or local authorities near its renewable energy projects join freely and have a real say in how it's run. Its main goal isn't making money, but creating environmental, economic, or social benefits for its members and the surrounding area. Think of it as neighbors teaming up to produce clean energy for their own community's good.

Concept in Directive (EU) 2018/2001

Co-funded by the European Union

smarco

Cybersecurity in Smart Communities

The technological fulcrum for a Renewable Energy Community (‘REC) is the **Smart grid**, that is an intelligent grid where data flows in parallel to electricity. Within the **Smart Meter** is the endpoint, it a connected meter that collects very granular data (personal data) on consumption and production.

Privacy and cybersecurity issues?

Co-funded by the European Union

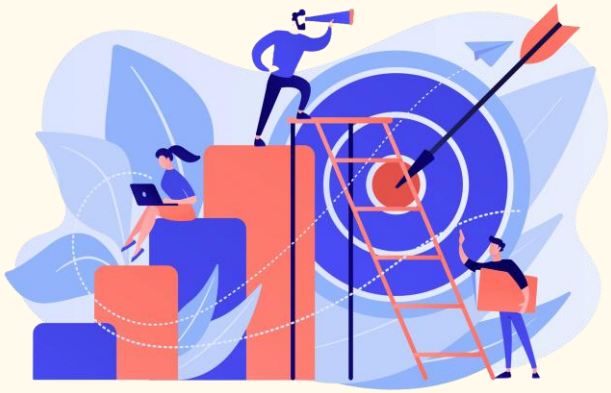
smarco

Unit Completed – What's Next?

To consolidate your learning and reflect on the key concepts covered, please take a moment to complete this quiz.

Your feedback and results will help you track your progress and support continuous improvement of the training experience.

Click the link to begin the quiz!



Co-funded by the European Union

smarco

SMARCO

SMARt COmmunities Skills Development in Europe

www.smarco.eu

info@smarco.eu

We are social! Follow us on:

@smarcoproject

@smarcoproject

@smarcoproject

Co-funded by the European Union

smarco

Cefriel
POLITECNICO DI MILANO

Project 101186291 — SMARCO