

European Cybersecurity Regulations who's who

@carlofanciola

exprivia

resent
exprivia group

Cybersecurity & Europe

Since several years EU is trying to develop a common set of rules and regulations to help combat raging increase in cyberattacks and reduce digital fragility and and increase protection of member states from Cybercrime Threat Actors. Several regulations has been promulgated. let's take a look at them and how Opensource software can impact and been impacted.



EU Cybersecurity Regulations

GDPR and ePrivacy Directive: While broader than just cybersecurity, they work in tandem to protect data privacy and integrity.

Cyber Resilience Act (CRA): Ensures products with digital elements (like hardware and software) are secure by design and throughout their lifecycle. Manufacturers must provide automatic security updates and report incidents to agencies like ENISA. Products will need a CE marking to show compliance.

NIS2 Directive: Expands the scope of the original NIS directive to cover a broader range of essential and important sectors. It requires organizations to implement risk management measures and report incidents.

DORA (Digital Operational Resilience Act): Aims to strengthen the IT security of financial entities like banks and insurance companies. It includes requirements for risk management and incident reporting and also affects ICT service providers.

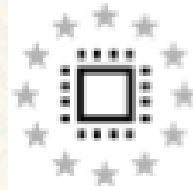
Product Liability Directive: (Applies from 2026) Will consider a product defective if it fails to meet the cybersecurity requirements outlined in other safety legislation.

Organizational Regulations:

Cybersecurity Act: Established the European Union Agency for Cybersecurity (ENISA) with a permanent mandate and created a voluntary European certification framework for ICT products, services, and processes.

Cyber Solidarity Act: Creates an EU-wide system to bolster resilience against cyber threats. It includes a cybersecurity alert system, a crisis management mechanism for critical entities, and strengthens cooperation between member states.

And One more thing...



EU Artificial Intelligence Act

The European AI Act, which entered into force on August 1, 2024, is a major part of the EU's regulatory framework for AI, including crucial cybersecurity provisions. It uses a risk-based approach that classifies AI systems into unacceptable, high, and other risk categories. The Act prohibits certain harmful AI practices outright (e.g., AI-based manipulation, biometric categorization, social scoring).

Risk Based Approach

AI systems are classified based on their risk level, with rules tailored to each category:

Prohibited AI: Certain practices, like AI that manipulates people or uses real-time remote biometric identification in public spaces (with limited exceptions for law enforcement), are banned.

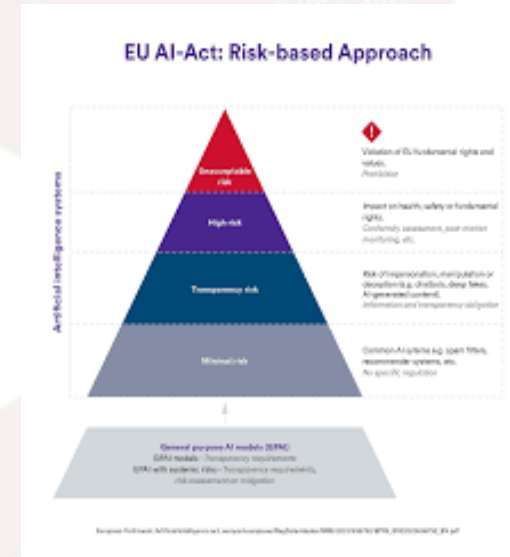
High-risk AI: Systems with a potentially detrimental impact on health, safety, or fundamental rights face strict requirements for market access, such as certification and risk management obligations.

Limited risk AI: Systems like chatbots are subject to transparency requirements, ensuring users are aware they are interacting with an AI.

Minimal risk AI: Systems with only minimal risk are not subject to additional obligations.

General Purpose AI models (GPAI): Specific rules apply to General Purpose AI (GPAI) models, with more stringent requirements for those with systemic risks. A Code of Practice is being developed for these models.

Global impact: As the first comprehensive legal framework of its kind, the Act has a significant global impact, affecting any company that develops or uses AI systems in the EU, including those based in the United States.



NIS2 in particular: his objectives



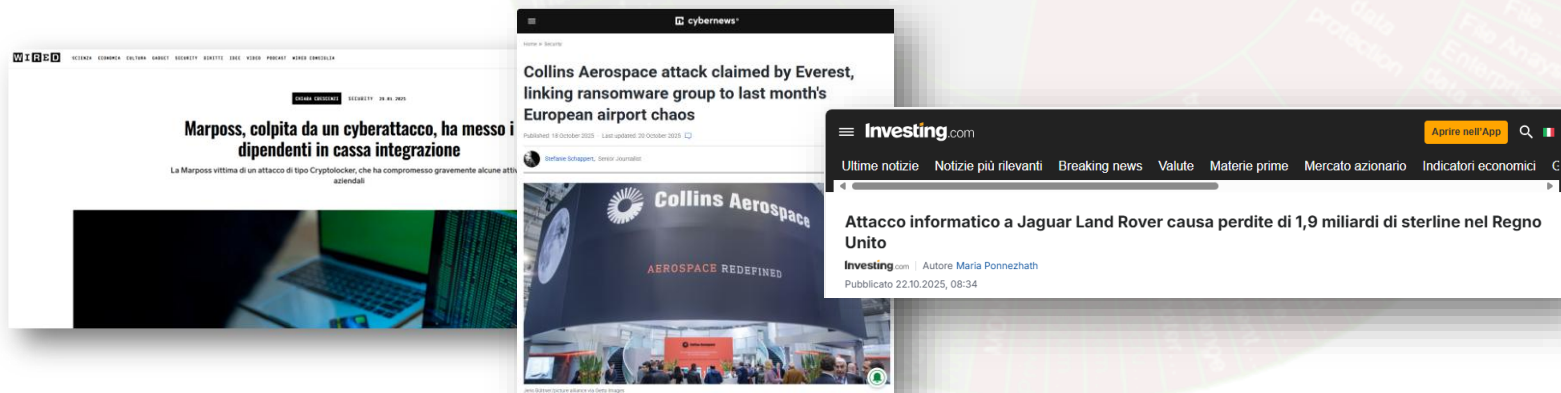
Increased security of all critical infrastructures in EU Member States;



Protection of information and network systems;



Protecting the physical environment from security incidents by strengthening its cybersecurity measures.



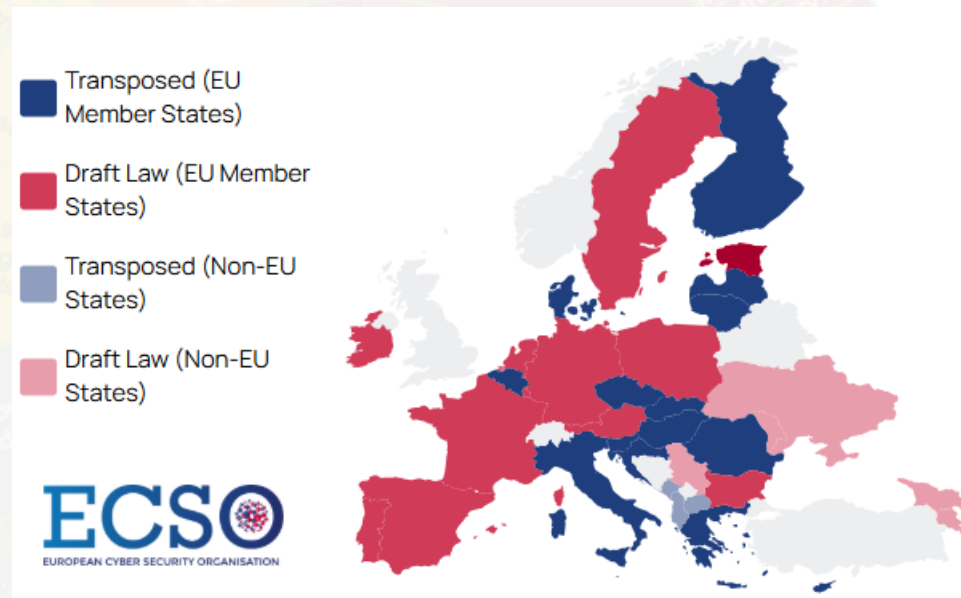
NIS2: adoption path

The NIS 2 Directive (EU Directive 2022/2555 of the European Parliament), which entered into force in January 2023, was created with the aim of strengthening the work begun with the previous NIS (Network and Information Security) Directive, which since 2016 has created a common level of cybersecurity across the European Community.

Member States were **required to transpose** the directive by issuing a national regulation by **October 18, 2024**, focusing on:

- Greater coordination of the strategy among Member States
- New types of organizations included within its scope
- List of security measures

At present (October 2025), the directive has been transposed by fifteen European countries: Belgium, Croatia, Slovakia, Italy, Lithuania, Latvia, Greece, Finland, Romania, Hungary, Denmark, Luxembourg, Czechia, Cyprus + Albania, and Montenegro



[NIS2 Directive Transposition Tracker - ECISO](#)

NIS2 and Opensource

In Italy, at the moment, there are more than **23.000** organization of many sizes accounted in the NIS2 perimeter and already enrolled. **25 to 30 thousand** are supposed to be enrolled in **Germany** and more than **20 thousand in France**.

Those are big numbers.

As an example, ACN, the Italian Cybersecurity Authority has listed more than 60 main requirements (called Misure di Base) that shall be evaluated and, if needed, been implemented by organization in perimeter; may also be possible that more to be added in the future.

These requirements in some cases may need tools to be **implemented** and more tools to be **monitored, governed** and **assessed** during time

For most of the small and medium sized organizations that are most of the organizations in NIS2 perimeter the cost associated to fully commercial approach to cybersecurity products may lead to imbalanced and partial protection.

This led to a huge opportunity for Opensource , even more because those solution probably do not increase dependence to not European countries.

NIS2 will continue the Crane Hall !

If you are interested in the NIS2 as a citizen, a developer or as an interpreneur you can join us in the Cranehall for the “NIS2 It’s here to stay ” BOF.

17:00

SIDE EVENT | CRANE HALL BOF

BOF

NIS2 is here to stay

Deepdive in the norm with an opensouce perspective

Where: [Crane Hall](#)

Duration: 40 mins

Carlo Falciola

Exprivia S.p.A.



Graziano
Specchierla

Exprivia SpA



BOF (Birds of a Feather) meetings are informal gatherings where communities can come together to discuss any topic of interest.

