Casarosa

Definition of cybersecurity law

Cyber attacks have grown rapidly in scale, scope and sophistication

Four different and overlapping threat-categories:

- Cyber war
- Cyber Espionage
- Cyber Terrorism and Cyber Vandalism
- Cybercrime

Cybersecurity

Cybersecurity is a term that covers a wide range of activities aimed at preventing and mitigating cyber-threats

It can be divided into:

- Network and information security
- Fight against cyber crime and cyber defense

Cybersecurity law

In order to define cybersecurity law we must answer five fundamental questions:

1. What are we securing?
2. Where and whom are we securing?
3. How are we securing?
4. When are we securing?
5. Why are we securing?

Let's answer them:

1. What are we securing?
    a. promote the **confidentiality**, **integrity**, and **availability** of information, systems, and networks
    b. Cybersecurity is not confined only to data security
    c. Cybersecurity focuses not only on the protection of data, but also on the systems and networks of the public and private sector
        i. **Confidentiality:** prevention of unauthorized disclosure of information
        ii. **Integrity:** guarantee that the message that is sent is the same as the message received and that the message is not altered in transit
        iii. **Availability:** guarantee that information will be available to the user in a timely and uninterrupted manner when it is needed regardless of the location of the user
2. Where and whom are we securing?
    a. Should law be focused only on bolstering the security of military and civilian government systems?
    b. Should the laws apply also to private-sector cybersecurity?
        i. Does Internet design provide for a different infrastructure for public and private sector? NO
    c. Any effective cybersecurity law regime will seek to secure both the public and private sector
3. How are we securing?
    a. Hard law or soft law?
        i. Coercive laws deter inadequate cybersecurity whereas cooperative laws that provide incentives for companies and government agencies to invest in cybersecurity
4. When are we securing?
    a. Should law focus on events that already have occurred, or should it attempt to build resilience to prevent future attacks?
    b. There is a need for a forward looking approach

5. Why are we securing?
    a. Three distinct types of harm that cybersecurity law should seek to avoid (or at least mitigate):
        i. (1) harm to individuals
        ii. (2) harm to business interests
        iii. (3) harm to national security

Flexibility and adaptability of measures

Importance of human factor

Update vis-à-vis changing risks

Cooperation and Information sharing

EU competence in cybersecurity

EU competence

Under the **principle of conferral**, the Union shall only act withing the limits of the competences conferred upon it by the Member States in the Treaties, and in order to attain the objectives set out therein.

Art 4 TFEU (Treaty on the Functioning of the European Union)

1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States
2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State

Which is the legal basis for EU cybersecurity legislation?

- Article 114 TFEU - Internal market
    - This article allows the EU to adopt measures for the harmonization of laws within Member States to ensure the proper functioning of the internal market. It provides a legal basis for regulatory alignment across countries to remove obstacles to trade and competition within the EU.
- Article 62 and 53(1) TFEU - right of establishment and freedom of service
    - Article 62 pertains to the provisions needed to ensure the freedom of establishment and the freedom to provide services within the EU. It refers to articles 51-54, which provide for limitations and specific rules concerning the freedom of establishment.
    - Article 53(1) enables the European Parliament and the Council to issue directives for the mutual recognition of diplomas, certificates, and other qualifications. It facilitates the freedom of establishment by making it easier for professionals to practice in different Member States.
- Article 127(2), 132(1) TFEU - smooth operation of payment systems
    - Article 127(2) outlines the primary objective of the European System of Central Banks (ESCB) to maintain price stability. In pursuing this goal, the ESCB is required to support general EU economic policies, contributing to the objectives of the Union.
    - Article 132(1) gives the European Central Bank (ECB) the authority to issue regulations, take decisions, make recommendations, and give advice as needed to fulfill its tasks within the ESCB framework.
- Article 83(1) TFEU - area of freedom, security, and justice
    - Article 83(1) provides a basis for establishing minimum rules for criminal offenses and sanctions in areas of particularly serious crime with a cross-border dimension. This includes terrorism, trafficking, money laundering, and cybercrime.
- And as regards coordination at the EU level - Article 74 TFEU
    - Article 74 allows the Council to adopt measures to ensure cooperation between administrative authorities across Member States. This cooperation is essential for the effective functioning of policies and programs implemented under the TFEU, particularly in areas requiring cross-border enforcement.

In areas that do not fall withing the exclusive competence of the Union, the principle of subsidiarity must be observed

Art 5 TFEU

3. Under the principle of subsidiarity, in areas which do not fall withing its exclusive competence, the Union shall act **only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States**, either at central level or at regional and local level, but can rather, by reason of the scale of effects of the proposed action, be better achieved at Union level

- The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. National Parliaments ensure compliance with the principle of subsidiarity in accordance with the procedure set out in that Protocol

4. Under the principle of proportionality, **the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties**

- The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality

EU interventions in cybersecurity

- 1992, Council Decision 92/242/EEC in the field of security of information systems
- 1995, Council Recommendation 1995/144/EC on common information technology security criteria
- 2001, Communication on Network and Information Security
    - policy measures can reinforce the market process and at the same time improve the functioning of the legal framework
- 2005, Council Framework Decision 2005/222/JHA27 on attacks against information systems
- 2006, Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" COM/2006/0251 final
- 2013, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
- 2012, "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Security Industrial Policy Action Plan for an innovative and competitive Security Industry" (2012) COM/2012/0417 final
- 2020, Joint Communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final
    - The strategy has three areas of action:
        - resilience, technical sovereignty and leadership;
            - Cybersecurity shield
            - Internet of Secure Things
            - DNS4EU
        - operational capacity to prevent, deter and respond;
            - Joint cybersecurity Unit
        - cooperation to advance global and open cyberspace

The EU Security Union Strategy

The strategy covers the period from 2020 to 2025 and focuses on priority areas where the EU can help Member States in fostering security for all those living in Europe, while respecting our European values and principles

- Terrorism and organized crime
    - Organized crime
    - Terrorism and radicalization
- Future-proof security environment
    - Critical infrastructure
    - Cybersecurity
    - Protecting public spaces
- A strong security ecosystem
    - Strengthening research and innovation
    - Cooperation and information exchange
    - Skills and awareness raising
    - Strong external borders

- Tackling evolving threats
  - Hybrid threats
  - Illegal content online
  - Cybercrime
  - Modern law enforcement

EU governance structure

EU governance structure

EU governance structure

Decentralized structure

- Allocation to the three different areas of cybersecurity: Network and information security, cyber crime, and cyber defense

Network and information security

- ENISA
  - Established in 2004, received a new permanent mandate in 2019 by the EU Cybersecurity act
  - Raises awareness and assists the EU, Member States, and public and private stakeholders develop and improve cyber resilience and response capacities
  - Responsible for the preparation of European cybersecurity certification schemes, which will serve as the basis for certification of ICT products, processes, and services
- CERT-EU, CSIRTs, Cooperation Group, CSIRTs Network and FIRST

Cybercrime

- European Cyber crime center (EC3)
  - Operational support and training to the Member States and has become the first hub for expertise on cybercrime operations

Cyberdefense

- European Defense Agency (EDA) and EU Military Staff
  - Advisory function, leaving the operational and strategic realities of defense to the Member States

EU Cybersecurity Ecosystem is structured around four key pillars: **Resilience**, **Law Enforcement**, **Cyber Defense**, and **Cyber Diplomacy**. Each pillar involves various EU organizations and mechanisms working together to enhance cybersecurity across the Union.

Sections and Functions:

1. **Protecting and Supporting EU Citizens**:
   - Focuses on safeguarding the digital well-being of European citizens.
2. **Protecting EU Institutions, Bodies, and Agencies**:
   - Dedicated to the cybersecurity of EU institutions.
3. **Coordinating Networks, Mechanisms, and Supporting Programmes**:
   - Centers on collaboration across networks and programs to support cybersecurity.

The Joint Cyber Unit will support participants to:

- Create **an inventory** of operational and technical capabilities available in the EU;
- Produce **integrated EU cybersecurity situation reports**, including information and intelligence about threats and incidents;
- Deliver the **EU Cybersecurity Incident and Crisis Response Plan**, based on national plans proposed in the revised NIS Directive (NIS2);
- Conclude **memoranda of understanding** for cooperation and mutual assistance;
- Establish and mobilize EU **Cybersecurity Rapid Reaction Teams**;
- **Share information and conclude operational cooperation agreements**.

Information sharing

The more sophisticated the cyber-attacks the closer the collaboration between private and public actors should be

Information sharing mechanisms are fundamental

How private involvement should be framed?

- Security has always been of the most important prerogatives of a state
- BUT technical knowledge of the field lies mostly in hands of private actors

Regulations and directives are two types of EU legal acts with distinct characteristics. A regulation is directly applicable across all Member States immediately upon adoption, ensuring uniformity as it becomes law without requiring national legislation. This is ideal when the EU seeks consistent standards, such as with data protection under the GDPR. In contrast, a directive sets a goal that Member States must achieve but allows them flexibility in how they implement it. Each Member State is required to transpose the directive into its national law, which can vary to accommodate different legal and social contexts. While regulations are uniformly binding in all details, directives bind only as to the result, allowing Member States discretion over the means of achieving it.

💡 Regulation 2019/881 (Cybersecurity act):

- **Point 6** refers to the need for a comprehensive set of EU cybersecurity measures that builds on previous actions and pursues mutually reinforcing objectives. These objectives focus on increasing the cybersecurity capabilities and preparedness of Member States and businesses, enhancing cooperation and information sharing across the EU, and boosting Union-level capabilities to support Member States, especially in large-scale cross-border incidents, while maintaining and improving national responses.
- **Point 29** addresses the role of **ENISA** in fostering public-private cooperation and within the private sector, specifically to protect critical infrastructure. ENISA is tasked with supporting information sharing by offering best practices, tools, procedural guidance, and regulatory advice, including facilitating sectoral information sharing and analysis centers, especially in the sectors listed in Annex II to Directive (EU) 2016/1148.

💡 Directive 2022/2555 (NIS 2):

- **Point 41** highlights the need for Member States to have sufficient technical and organizational capabilities to prevent, detect, respond to, and mitigate cybersecurity incidents and risks. To achieve this, Member States should establish or designate one or more Computer Security Incident Response Teams (CSIRTs) and ensure they are well-resourced and technically capable. These CSIRTs should meet the requirements of the Directive to ensure effective response and cooperation across the EU. Member States can designate existing CERTs as CSIRTs. Additionally, if a CSIRT is part of a competent authority, functional separation should be considered between CSIRT operational tasks (e.g., information sharing) and supervisory tasks to enhance trust with entities.
- **Point 119** addresses the importance of sharing threat and vulnerability intelligence, given the increasing complexity of cyber threats. Regular information sharing boosts awareness of cyber threats, helping entities prevent incidents, contain effects, and recover more effectively. However, uncertainties related to competition and liability rules at the EU level have hindered such intelligence sharing, indicating a need for Union-level guidance to facilitate this process.

Operationalize information sharing

- Public authorities tried to enhance security requesting private companies to share information
- Private actors were reluctant to share voluntarily information related to the activities they carry out
- Private-public Partnerships

Public-private partnerships

Private-public partnerships are defined as “a long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance” (World Bank)

- The different group of actors involved in each sector will determine according to the characteristics of their activities, a relationship more or less strict between private and public actors
- Actors carrying out activities at the physical infrastructure layer have a marginal relationship with the public sector authorities. Whereas private entities providing services and products to consumers have a strict relationship with public authorities

ENISA Study on PPP

Cooperative Models for Public Private Partnership (PPP)

- To provide information about PPPs in Europe through collecting information and analyzing the current status of PPP and to identify main models of this type of collaboration
- To identify current challenges that both the private and public sector face in the process of setting up and developing PPPs
- To formulate and propose recommendations for the development of PPPs in Europe

A public-private partnership (PPP) is a long-term agreement/cooperation/collaboration between two or more public and private sectors and has developed through history in many areas.

PPP is not only about the private-public cooperation. It includes also private-private and public-public relations

Driving forces for the creation of PPP:

- Economic interests
- Regulatory requirements
- Public relations
- Other reasons

Motivations and benefits of Public-Private Partnerships (PPPs) in cybersecurity, highlighting how the **private sector** and **government** each gain from collaboration. The common objective of both sectors is to enhance overall cybersecurity levels.

Key Motivations and Benefits:

For the **private sector**, PPPs provide access to public funds and sector knowledge, including confidential information. They also ensure product quality, offer opportunities to influence legislation, and shape obligatory standards.

For the **government**, PPPs enhance understanding of industry needs, create synergies with private initiatives, and provide access to private sector resources while aligning with international law and regulations.

The **PPP framework** fosters trust, promotes knowledge sharing, enhances cybersecurity resilience, and establishes credible connections between stakeholders. Understanding how PPPs are initiated and evolve—through models like Top Down, Bottom Up, Fire and Forget, or Split and Merge—guides the development of new partnerships.

Types of PPPs

Institutional PPPs

Formed under legal acts related to critical infrastructure protection, they often involve working groups, rapid-response teams, and long-term communities.

Goal-Oriented PPPs

Created to build a cybersecurity culture in member states, these partnerships focus on specific goals and serve as platforms for knowledge exchange and best practices.

Outsourcing Cybersecurity Services

Formed by governments and private sectors, these PPPs raise cybersecurity awareness and act as third-party providers for industry needs while supporting policy-making and implementation.

Hybrid PPPs

Include CSIRTs operating within a PPP framework, tasked with delivering cybersecurity services to public administrations or nationwide as assigned by governments.

Challenges

Despite their benefits, PPPs face significant challenges:

- A shortage of skilled human resources in both public and private sectors.
- Insufficient public budgets and resources to meet private sector expectations.
- Difficulties in establishing a shared understanding and dialogue between sectors.
- Limited awareness and promotion of PPPs among SMEs.
- A lack of leadership and clear legal frameworks

European Cyber Security Organization

The ECSO is a fully self-financed non-profit organization under the Belgian law, established in June 2016. It was created in order to act as the Commission’s counterpart in a contractual public-private partnership covering Horizon 2020 in the years 2016 to 2020. The majority

of ECSO's 250 members belong either to the cybersecurity industry or to research academic institutions in the field. To a lesser degree, ECSO's members also comprise public sector actors and demand-side industries. Besides making recommendations on Horizon 2020, ECSO carries out various activities aiming at community building and industrial development at European level.

EU legislative framework

EU Cybersecurity legislation

The Directive on Resilience of Critical Infrastructures (2008) evolved into the Resilience of Critical Entities (2022). The NIS Directive (2016) was replaced by the NIS 2 Directive (2022). Other key legislation includes the Cybersecurity Act (2018), the Regulation on European Cybersecurity Competence Center and Network (2021), the Cyber Solidarity Act (2023), the Cyber Resilience Act (2024), the Artificial Intelligence Act (2024), and the European Health Data Space (2024).

European Cybersecurity Competence Center and Network

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Center and the Network of National Coordination Centers

- The European Cybersecurity Competence Center (ECCC), together with the Network of National Coordination Centers (NNCCs), is Europe's new framework to support innovation and industrial policy in cybersecurity
- The ECCC, which will be located in Bucharest, will develop and implement, with member states, industry and the cybersecurity technology Community, a common agenda for technology development and for its wide deployment in areas of public interest and in businesses, in particular SMEs
- The Center and the Network together will enhance out technological sovereignty through joint investment in strategic cybersecurity projects

Point 16 explains that the Competence Center should not engage in operational cybersecurity tasks, such as incident monitoring and handling, which are the responsibility of CSIRTs. However, it can support the development of ICT infrastructures for industries, SMEs, research, civil society, and the public sector. While the Competence Center and the Cybersecurity Competence Community may assist CSIRTs in vulnerability reporting, this support should be within their scope and avoid duplicating ENISA's role.

Point 17 highlights that the Competence Centre, the Community, and the Network will benefit from the expertise gained through the EU's public-private partnership with the European Cyber Security Organisation (ECSO) under Horizon 2020. They will also draw on lessons from pilot projects (CONCORDIA, ECHO, SPARTA, and CyberSec4Europe) and the EU FOSSA initiative to manage and represent the Community effectively within the Competence Center.

The Competence Center should facilitate and coordinate the work of the Network

- The Network should be made up of one national coordination center from each Member State
- National coordination centers which have been recognized by the Commission as having the necessary capacity to manage funds to fulfill the mission and objectives laid down in this Regulation should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out their activities in relation to this Regulation
- National coordination centers should be public sector entities, or entities with a majority of public participation, performing public administrative functions under national law, including by means of delegation, and they should be selected by Member States
- National coordination centers should have the necessary administrative capacity, should possess or have access to cybersecurity industrial, technological and research expertise and should be in a position to effectively engage and coordinate with the industry, the public sector and the research community

Resilience of critical entities directive

Directive (EU) 2022/2557 on the resilience of critical entities

The **European Critical Infrastructure (ECI) Directive** of 2008 applies only to the energy and transport sectors, providing a process for identifying and designating ECIs whose disruption would impact at least two Member States. It sets protection requirements for ECI operators and relevant national authorities. So far, 94 ECIs have been designated, mostly in energy and concentrated in a few Central and Eastern European countries. However, EU efforts on critical infrastructure resilience also encompass broader sectoral and cross-sectoral actions, including climate protection, civil protection, foreign direct investment, and cybersecurity. Additionally, Member States have implemented their own varying measures in this area.

Directive on the resilience of critical entities

The current risk landscape for critical infrastructure has become more complex since 2008, now involving climate-exacerbated natural hazards, state-sponsored hybrid threats, terrorism, insider threats, pandemics, and industrial accidents. Operators face challenges in adopting technologies like 5G and unmanned vehicles, which bring both operational advantages and new vulnerabilities. Increased

interdependence among sectors means that disruptions in one sector can trigger cascading effects across others, potentially impacting multiple Member States or the entire EU. The scope now covers ten sectors, including energy, transport, finance, health, digital infrastructure, and space. Member States are required to identify critical entities based on national risk assessments and apply obligations, especially to entities of European significance that provide essential services across multiple Member States.

The main changes in critical infrastructure policy emphasize a shift from **protection to resilience**. While protection focuses on preventing incidents through risk assessment, resilience accepts that incidents will occur and incorporates both preventive and responsive measures. There are no established standards to evaluate resilience effectively.

The scope has also shifted from **European Critical Infrastructures to Critical Entities**, adopting a more bottom-up, agent-based approach. The policy now covers a wider range of **11 critical sectors** (including energy, transport, and others) and recognizes the increasing inter-dependencies among sectors, countries, and physical-digital systems.

The policy approach has broadened from focusing primarily on terrorism to an **all-hazards approach**, addressing various risks.

Regarding **cybersecurity coordination**, the new approach aligns with the NIS 2 Directive, which enhances resilience for "essential" and "important" entities across sectors. Competent authorities for critical entities and those for NIS 2 will collaborate, ensuring resilience against both cyber and non-cyber risks. Critical entities under NIS 2 face broader obligations to manage non-cyber risks, and digital infrastructure's physical security is integrated into cybersecurity risk management and reporting under NIS 2.

NIS Directive

EU Directive 2016/1148 concerning measures for a high level of common security of network and information systems across the Union
Art. 1(1): This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market

Art 1(7): Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify
incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.

Objectives

This paragraph discusses cybersecurity challenges in the European Union, highlighting several key issues:

1. Current cybersecurity capabilities are inadequate for ensuring high-level network and information systems security across the EU
2. There's significant disparity in preparedness levels between Member States, leading to:
   - Fragmented approaches
   - Uneven protection for consumers and businesses
   - Compromised overall security levels across the Union
3. Two major problems are identified:
   - Lack of common requirements for essential service operators
   - Lack of common requirements for digital service providers
4. These gaps make it impossible to establish an effective EU-wide cooperation mechanism
5. The paragraph
   concludes by noting the crucial role that academic institutions
   (universities and research centers) play in advancing research,
   development, and innovation in these areas.

The central theme is that fragmentation and lack of standardization in cybersecurity measures across EU member states is hampering effective protection at the Union level.

Objectives of NIS directive

- **Union-Level Cooperation**: A Cooperation Group is to be established at the Union level to facilitate strategic cooperation and information exchange among Member States. Additionally, a Computer Security Incident Response Teams (CSIRTs) network will be created to promote operational cooperation.
- **National Strategy and Competent Authorities**: Member States must adopt a national strategy for network and information security and designate the national competent authorities. Each Member State should also designate at least one competent CSIRT for essential services.
- **Compliance by Operators and Providers**: Operators of essential services (OESs) and digital service providers (DSPs) are required to comply with established security-related requirements.

National Frameworks

Article 7: National Strategy on the Security of Network and Information Systems

1. **National Strategy Requirement**: Each Member State must adopt a national strategy to ensure the security of network and information systems. The strategy should outline strategic objectives, policies, and measures to maintain high security levels across sectors listed in Annex II and services in Annex III. It should address the following key points:
   - Objectives and priorities for network and information security.
   - Governance framework, defining roles and responsibilities of government bodies and relevant actors.
   - Measures for preparedness, response, and recovery, including public-private cooperation.
   - Education, awareness-raising, and training programs related to security.
   - Research and development plans for network and information security.
   - A risk assessment plan to identify potential security risks.
   - A list of stakeholders involved in implementing the strategy.
2. **ENISA Assistance**: Member States may seek ENISA's assistance when developing their national strategies.

Article 9: Computer Security Incident Response Teams (CSIRTs)

1. **Designation of CSIRTs**: Each Member State must designate one or more CSIRTs responsible for risk and incident handling, ensuring they cover the sectors and services specified in Annex II and III. CSIRTs should follow a well-defined process and may be established within a competent authority.
2. **Resource Allocation**: Member States must ensure CSIRTs have adequate resources to perform their tasks effectively, as outlined in Annex I. They should also ensure secure and efficient cooperation within the CSIRT network (Article 12).
3. **Infrastructure**: Member States must ensure CSIRTs have access to a secure and resilient communication infrastructure at the national level.
4. **CSIRT Remit**: Member States must inform the Commission about the remit and key elements of their CSIRTs' incident-handling processes.
5. **ENISA Assistance**: Member States may request ENISA's assistance in developing national CSIRTs.

Target = Operators of essential services and Digital service providers

Operators of essential services

Art 5)

1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory
2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Art 4, shall be as follows:
   a. An entity provides a service which is essential for the maintenance of critical societal and/or economic activities
   b. The provision of that service depends on network and information systems
   c. An incident would have *significant disruptive effects* on the provision of that service

Critical incidents

Art 6) Significant disruptive effect

1. When determining the significance of a disruptive effect as referred to in point (c) of Art 5(2), Member States shall take into account at least the following cross-sectoral factors:
   a. The number of users relying on the service provided by the entity concerned;
   b. The dependency of other sectors referred to in Annex II on the service provided by that entity;
   c. The impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
   d. The market share of that entity;
   e. The geographic spread with regard to the area that could be affected by an incident;
   f. The importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service

Operators of essential service

Consistency approach in OES identification

1. To reduce the risks related to cross-border dependencies;
2. To guarantee a level playing field for operators in the internal market;
3. To reduce the risk of divergent interpretations of the Directive;
4. To develop a comprehensive overview of the level of cyber resilience across the EU

Security requirements - OSE

Art 14 Security requirements and incident notification

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.
2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

Incident notification - OSE

Art 14 Security requirements and incident notification

3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.
4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:
    a. The number of users affected by the disruption of the essential service;
    b. The duration of the incident;
    c. The geographical spread with regard to the area affected by the incident.

Notification to the public

Competent authorities should prioritize maintaining trusted, informal information-sharing channels. When incidents are reported, they must balance public interest in being informed with the potential reputational and commercial risks to the operators of essential services. Additionally, authorities and CSIRTs should ensure that information about product vulnerabilities remains confidential until appropriate security fixes are released.

Digital service providers

Many businesses in the Union depend on digital service providers, whose services are crucial for the smooth functioning of various operations, including those of essential service operators. Since disruptions in these digital services can impact key economic and societal activities, this Directive applies to providers offering such essential digital services. These providers play a vital role in ensuring business continuity, participation in the internal market, and cross-border trade within the Union.

Security requirements - DSP

Article 16 outlines security requirements and incident notification obligations for digital service providers:

1. **Security Measures**: Member States must ensure that digital service providers implement appropriate technical and organizational measures to manage security risks related to their network and information systems. These measures should be proportionate to the risk and consider system security, incident handling, business continuity, monitoring, auditing, and international standards.
2. **Risk Mitigation**: Providers must take steps to prevent and minimize the impact of incidents on the services they offer, ensuring continuity of those services.
3. **Incident Notification**: Providers must notify the competent authority or CSIRT without delay if an incident significantly impacts the provision of services. The notification should help assess any cross-border impact but does not increase the notifying party's liability.
4. **Impact Assessment**: When determining if an incident is substantial, factors such as the number of users affected, duration, geographical spread, service disruption, and impact on economic and societal activities must be considered. Notification obligations only apply if the provider can assess the incident's impact based on these parameters.

Different approach towards DSP

Digital service providers should ensure security measures appropriate to the risks their services pose, considering their importance to other businesses. Since essential service operators face higher risks due to their critical role, digital service providers have lighter security requirements. They can implement measures they deem suitable to manage risks, but due to their cross-border nature, they should follow a more unified approach at the Union level. Implementing acts will help define and guide these security measures.

NIS Evaluation

Broad and abstract - pros and cons

Uniform and continuous testing and control is not compulsory

Limited role of law enforcement authorities

Directive (EU) 2022/2555 (NIS 2) expands the scope of the previous NIS Directive to include new sectors critical for the economy and society. It removes the distinction between operators of essential services and digital service providers. Additionally, it strengthens security requirements by introducing a risk management approach, ensuring that companies take appropriate measures to manage and mitigate cybersecurity risks effectively.

NIS 2 Directive

- **Medium-Sized Enterprises**: The Directive applies to public or private entities listed in Annex I or II that qualify as medium-sized enterprises according to the criteria in Article 2 of the Annex to Recommendation 2003/361/EC, or exceed those size thresholds, and operate within the Union. The exception to Article 3(4) of that Recommendation applies for the purposes of this Directive.
- **Entities Providing Critical Services**: The Directive also applies to entities of the types listed in Annex I or II, regardless of their size, if they meet one or more of the following conditions:
  - Provide services such as public electronic communications, trust services, or domain name services.
  - Are the sole provider in a Member State of a service critical for maintaining societal or economic activities.
  - Their service disruption could significantly impact public safety, security, or health.
  - Their service disruption could pose systemic risks, particularly with cross-border impacts.
  - They are critical due to their specific importance at a national or regional level, or within interconnected sectors.
  - They are public administration entities at central or regional government levels, providing services whose disruption could severely affect societal or economic activities.
- **Critical Entities**: The Directive applies to entities identified as critical under **Directive (EU) 2022/2557**, regardless of their size.
- **Domain Name Registration Services**: The Directive applies to entities providing domain name registration services, regardless of their size.

Security requirements

- **Risk Management Requirements**: Member States must ensure that essential and important entities implement appropriate technical, operational, and organizational measures to manage risks to the security of their network and information systems. These measures should prevent or minimize the impact of incidents on both service recipients and other services. The measures must be proportionate to the risks posed, considering the entity's exposure to risks, size, and the potential severity of incidents, including societal and economic impacts.
- **All-Hazards Approach**: The risk-management measures must adopt an all-hazards approach to protect network and information systems, and their physical environments. These measures must include, at a minimum:
  - Risk analysis and information system security policies.
  - Incident handling procedures.
  - Business continuity measures, such as backup management and crisis management.
  - Supply chain security, focusing on relationships with suppliers and service providers.
  - Security in system acquisition, development, maintenance, and vulnerability management.
  - Policies for assessing the effectiveness of cybersecurity measures.
  - Cyber hygiene practices and cybersecurity training.
  - Cryptography and encryption policies.
  - Human resources security, access control, and asset management.

- Use of multi-factor or continuous authentication, secured communication systems, and emergency communication solutions, as needed.

Notification of incidents

1. **Incident Notification**: Member States must ensure that essential and important entities notify their CSIRT or competent authority without delay about significant incidents affecting the provision of their services. Entities should also inform service recipients if the incident is likely to affect them. The notification must include information that allows the CSIRT or competent authority to assess any cross-border impact. The act of notification does not increase the entity's liability. If an entity notifies the competent authority, the authority must forward the information to the CSIRT. For cross-border or cross-sector incidents, Member States must ensure timely information sharing with relevant contacts.
2. **Communication with Service Recipients**: When applicable, Member States must ensure that entities communicate with service recipients about significant cyber threats, advising them on measures they can take to address the threat. Entities should also inform recipients of the threat itself when appropriate.
3. An incident is considered significant if:
   - **(a)** It causes or could cause severe operational disruption or financial loss for the entity.
   - **(b)** It affects or could affect other individuals or entities, causing considerable material or non-material damage.
4. **Reporting Obligations**: Member States must ensure that entities report significant incidents to the CSIRT or competent authority within specified timeframes:
   - **Early Warning (within 24 hours)**: The entity must provide an early warning, including whether the incident is suspected to be caused by unlawful acts or could have a cross-border impact.
   - **Incident Notification (within 72 hours)**: The entity must submit an incident notification, updating the early warning and providing an initial assessment of the incident's severity, impact, and indicators of compromise.
   - **Intermediate Report (upon request)**: The entity must provide a status update if requested by the CSIRT or competent authority.
   - **Final Report (within one month)**: A detailed final report is due within one month, covering:
     - A detailed incident description, severity, and impact.
     - Likely threat type or root cause.
     - Mitigation measures.
     - Cross-border impact, if applicable.
   - If the incident is ongoing at the time of the final report, a progress report is required, with a final report within a month of incident resolution.

Trust Service Providers: For significant incidents affecting trust services, the notification must be made within 24 hours of becoming aware, instead of the usual 72 hours.

Supervision - essential entities

- **Effectiveness and Proportionality**: Member States must ensure that supervisory and enforcement measures imposed on essential entities are effective, proportionate, and dissuasive, considering the specifics of each case.
- **Supervisory Powers**: Competent authorities must have the power to subject essential entities to:
  - **On-site inspections and off-site supervision**, including random checks by trained professionals.
  - **Regular and targeted security audits** carried out by independent bodies or competent authorities.
  - **Ad hoc audits** following significant incidents or violations of the Directive.
  - **Security scans** based on objective, non-discriminatory, and transparent risk assessments, with the entity's cooperation where necessary.
  - **Requests for information** to assess cybersecurity risk-management measures, including policies and compliance with reporting obligations.
  - **Requests for access to data, documents, and evidence** needed for supervisory tasks.

  The targeted security audits must be based on risk assessments, and their results must be shared with the competent authority. The costs for audits performed by an independent body are generally borne by the audited entity, unless the competent authority decides otherwise in justified cases

Supervision - important entities

- **Ex Post Supervisory Measures**: If there is evidence or information suggesting that an important entity is not complying with the Directive (specifically Articles 21 and 23), Member States must ensure that competent authorities take action through ex post supervisory measures. These measures must be effective, proportionate, and dissuasive, considering each case's circumstances.
- **Supervisory Powers**: Competent authorities must have the power to subject important entities to:
  - **On-site inspections and off-site supervision** conducted by trained professionals.
  - **Targeted security audits** carried out by an independent body or competent authority.
  - **Security scans** based on objective, non-discriminatory, and transparent risk assessment criteria, with the entity's cooperation where necessary.
  - **Requests for information** to assess the entity's cybersecurity risk-management measures and compliance with reporting obligations.
  - **Requests for access to data, documents, and information** necessary for supervisory tasks.
  - **Requests for evidence** of implemented cybersecurity policies, such as security audit results by qualified auditors.

  The targeted security audits must be based on risk assessments, and their results should be made available to the competent authority. The audited entity generally bears the costs of independent audits unless the competent authority decides otherwise in specific cases

Sanctions

General Conditions for Imposing Administrative Fines on Essential and Important Entities

1. **Effective, Proportionate, and Dissuasive Fines**: Member States must ensure that administrative fines imposed for infringements of the Directive are effective, proportionate, and dissuasive, considering the specific circumstances of each case.
2. **Additional to Other Measures**: Administrative fines are imposed in addition to the measures outlined in Articles 32 and 33, including inspections, audits, and security scans.
3. **Criteria for Imposing Fines**: When deciding whether to impose a fine and determining its amount, the competent authorities must consider at least the elements provided in Article 32(7), which includes factors such as the severity of the infringement.
4. **Fines for Essential Entities**: Essential entities that infringe Articles 21 or 23 are subject to administrative fines of up to **EUR 10,000,000** or **2% of the total worldwide annual turnover** of the undertaking to which the entity belongs (whichever is higher).
5. **Fines for Important Entities**: Important entities that infringe Articles 21 or 23 are subject to administrative fines of up to **EUR 7,000,000** or **1.4% of the total worldwide annual turnover** of the undertaking to which the entity belongs (whichever is higher).

From NIS Directive to Italian implementation

Existing legal framework

Legislative Decree No. 82 of 2005 (Digital Administration Code)

- Art 51: initial intervention on data security

Law No. 144/2005 on urgent measures to combat international terrorism

- Art. 7a on cyber security: cyber protection services of critical digital infrastructures of national interest were allocated to the Ministry of the Interior

Law No. 134/2012 on Italian Digital Agenda

- Creation of "Agenzia per l'Italia Digitale" coordinating actions in the field of innovation to promote ICT technologies to support public administrations, guaranteeing the realisation of the objectives of the Italian Digital Agenda,in coherence with the European Digital Agenda

Prime Minister's Decree of January 24, 2013, on cyber protection and national cybersecurity

- Coordination of cybersecurity-related activities involving public administrations and the intelligence community

National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace and Cybersecurity

- Internal organization to enable timely and coordinated responses to cyber threats targeting national assets

Set of Interventions

- Decreto Legislativo 65/2018:

  The Legislative Decree of May 18, 2018, No. 65, implements EU Directive 2016/1148 to enhance network and information security across the European Union. Key points include:

- **Objective (Article 1)**: Establish a high level of security for networks and information systems at the national level, contributing to EU-wide security.
- **Incident Reporting (Articles 12 and 14)**: Essential Service Operators (OES) and Digital Service Providers (DSP) are required to report incidents to the CSIRT, while for other entities, reporting is optional.
- **Non-Compliance Penalties (Article 21)**:
  - Failure to implement proper technical and organizational security measures by OES or DSP can lead to fines from €9,000 to €120,000.
  - If OES or DSP fail to notify the Italian CSIRT of significant incidents, fines range from €25,000 to €125,000.
  - OES relying on third-party DSPs for critical services face fines from €12,000 to €120,000 if they fail to report incidents

- Decreto Legge 105/2019 (Legge 133/2019):

  The **National Cybersecurity Perimeter (PSNC)** in Italy extends cybersecurity measures beyond the EU's NIS Directive to include public and private entities essential to national security. Its goal is to secure networks, information systems, and IT services for key national entities. Standards are set to minimize risks, and D.P.C.M. 131/2020 defines criteria for including entities based on essential functions and services.

- DPCM 131/2020

  The **Essential Functions** under Italy's National Cybersecurity Perimeter include maintaining government continuity, state defense, public safety, justice, economic systems, and transportation (Art. 2).

  Essential Services cover activities critical to state functions, rights protection, supply continuity, infrastructure, logistics, high-tech sectors, and any sectors vital to national autonomy, competitiveness, and economic development.

  The Cybersecurity Perimeter applies to networks, systems, and IT services where disruptions could threaten national security.

- DPCM 81/2021

  Entities within Italy's **National Cybersecurity Perimeter** must engage in **prevention** and **incident notification and response**.

  Procedure:

  - Entities are notified of inclusion in the perimeter and must prepare a list of their networks, systems, and IT services within six months, updating this list annually.
  - They must conduct risk assessments on ICT assets, evaluate the impact of disruptions, and adopt mitigation measures following EU and international standards, specifically the NIST cybersecurity framework.

  Incident Notification:

  - Incidents are classified by severity, with notification deadlines based on severity level. Reports are sent to the Italian CSIRT, and non-compliance may result in significant penalties.

- Presidential decree 54/2021

  Entities within Italy's **National Cybersecurity Perimeter** must inform the **National Evaluation and Certification Center (CVCN)** of any outsourced ICT products or services.

  - **CVCN Role**: The CVCN evaluates the security of ICT goods, systems, and services intended for use within the perimeter, as outlined in the Decree of June 15, 2021.
  - **Notification Requirements**: Entities planning to acquire ICT products for strategic areas must submit a detailed notification to the CVCN, covering the product's use, category, security measures, and risk analysis.
  - **Process**:
    - The CVCN responds with guidelines within 60 days.
    - Required tests on hardware and software are conducted at CVCN facilities or accredited locations.
    - CVCN provides the security assessment outcome and usage guidelines.

- Decr. Legge 82/2021

  Italy's **National Cybersecurity System** is governed by the **Italian Cybersecurity Authority (ACN)**, an independent agency responsible for technical cybersecurity functions.

  - **ACN**: Functions with administrative and financial autonomy, carrying out specialized tasks with limited political influence to safeguard fundamental rights. The ACN is directed by the **Presidente del Consiglio** and monitored by **COPASIR** (Parliamentary Security Committee).
  - **Governance Structure**:

- The **Presidente del Consiglio** leads national cybersecurity strategy and oversees the ACN.
- **ACN** handles technical aspects of cybersecurity.
- The **Interministerial Committee for Cybersecurity (CIC)** provides political guidance, advice, and oversight on cybersecurity policies.

Italian Cybersecurity Authority

The **Italian Cybersecurity Agency (ACN)** is an autonomous administrative body responsible for Italy's national cybersecurity efforts.

- **Structure and Autonomy**: The ACN operates with administrative and financial independence but is subject to the **Presidente del Consiglio**'s directives and **COPASIR** oversight to ensure political impartiality, especially for protecting fundamental rights.
- **Objectives**: Focus on safeguarding national cybersecurity interests, developing prevention, monitoring, detection, and response capabilities against cyber threats.
- **Key Tasks**:
  - Drafting the national cybersecurity strategy and coordinating public-private sector activities.
  - Enhancing digital industry security, including certifications for products and systems.
  - Providing advisory opinions on legislative measures to maintain a coherent national cybersecurity framework.
  - Coordinating European and international cybersecurity cooperation.
  - Supporting research, innovation, and skill development in cybersecurity.
  - Inspecting and enforcing cybersecurity compliance within the **National Cybersecurity Perimeter (PSNC)**.
- **Role**: Functions as the national supervisory authority, **CSIRT-Italy**, central contact for network security, national certification authority, and **National Evaluation and Certification Center (CVCN)**.

Italian CSIRT

Tasks:

- **Incident Monitoring**: Tracking cybersecurity incidents nationwide.
- **Alerts and Information Sharing**: Issuing pre-alarms, alerts, and updates on risks and vulnerabilities, including website publications on new threats.
- **Incident Response**: Actively intervening in cybersecurity incidents.
- **Risk Analysis**: Conducting dynamic risk and incident assessments.
- **Situational Awareness**: Maintaining an overview of the national cybersecurity landscape.
- **International Collaboration**: Participating in the CSIRT network, working with **ENISA** (European Union Agency for Cybersecurity).

Implementation of NIS 2 Directive

The **Legislative Decree No. 138 of September 4, 2024**, implements EU Directive 2022/2555, setting cybersecurity standards across the EU and superseding the previous NIS Directive.

- **Identification of Essential and Important Entities**: The **ACN** will compile a list of involved companies and public administrations by April 2025. All entities must register on the ACN's platform.
- **Security Obligations**: ACN will define specific security requirements based on risk exposure, entity size, incident probability, and impact severity.
- **Sanctions**:
  - Penalties vary based on the type of violation, including non-compliance, lack of notification, or registration failures.
  - For **Essential Entities (EEs)**: fines up to €10 million or 2% of annual global turnover.
  - For **Important Entities (IEs)**: fines up to €7 million or 1.4% of global turnover.
  - Additional fines for registration and communication failures, capped at 0.1% for EEs and 0.07% for IEs.
  - Repeated violations can triple fines, and ignoring ACN warnings can lead to suspension of certifications or authorizations.

EU Cybersecurity act

Regulation (EU) 2019/881 (Cybersecurity Act) establishes **ENISA** (European Union Agency for Cybersecurity) and focuses on ICT cybersecurity certification. It addresses three key factors:

1. **Global Leadership**: Aiming for the EU to take a leading role in the global cybersecurity market.
2. **Addressing Cyberattack Gaps**: Responding to the limitations of existing frameworks, which struggled to address recent cyberattacks effectively.
3. **Geopolitical Opportunity**: Reacting to the growing debate on the security of information systems and networks, aligning with the EU's geopolitical strategy.

ENISA

Strengthening the role of ENISA

Article 3 Mandate of the **Cybersecurity Act** outlines the role of **ENISA** in achieving a high level of cybersecurity across the EU:

1. **Support and Expertise**: ENISA supports Member States, EU institutions, and other stakeholders, acting as a key reference point for cybersecurity advice and expertise.
2. **Reducing Market Fragmentation**: ENISA helps harmonize cybersecurity laws and regulations across Member States to reduce fragmentation.
3. **Independence and Coordination**: ENISA operates independently, ensuring it complements, rather than duplicates, national efforts and leverages existing Member State expertise.
4. **Resource Development**: ENISA is tasked with developing the necessary technical and human resources to fulfill its cybersecurity duties.

ENISA - Objectives

- Empowering Communities
- Cybersecurity Policy
- Operational Cooperation
- Capacity Building
- Trusted Solutions
- Foresight
- Knowledge

Certification schemes

Certification systems

Recital 69 of the Cybersecurity Act emphasizes the need for a unified European cybersecurity certification framework. Key points include:

- **Common Approach**: Establishing a European certification framework for ICT products, services, and processes to be recognized across all EU Member States.
- **Building on Existing Systems**: Leveraging existing national and international certification schemes, like SOG-IS, for a smooth transition to the new framework.
- **Dual Purpose**: The framework aims to build trust in certified ICT products and services and reduce the proliferation of conflicting national certification schemes, lowering costs for businesses in the digital single market.
- **Standards**: Certification schemes should be non-discriminatory and based on European or international standards, unless such standards are inadequate for achieving EU objectives

Certification schemes - definition

Article 2 defines:

- **European Cybersecurity Certification Scheme**: A set of Union-level rules, technical requirements, standards, and procedures for certifying ICT products, services, or processes.
- **National Cybersecurity Certification Scheme**: A set of rules, technical requirements, standards, and procedures established by a national authority for certifying ICT products, services, or processes within the scope of that specific national scheme.

Certification schemes - procedure

Article 47

Specific ICT products, services, or processes are included in the Union rolling work programme for cybersecurity certification based on factors such as the existence of national certification schemes that could lead to fragmentation, relevant EU or national laws or policies, market demand, changes in the cyber threat landscape, and requests from the European Cybersecurity Certification Group (ECCG) for specific schemes. The European Commission also takes into account feedback from the ECCG and the Stakeholder Certification Group when drafting the work programme.

Article 51

European cybersecurity certification schemes aim to protect data against unauthorized access, processing, or disclosure throughout its lifecycle, while safeguarding it from accidental destruction, loss, alteration, or unavailability. They ensure that access to data or services is restricted to authorized individuals or systems, dependencies and vulnerabilities are identified and documented, and data, service, or function access, usage, and processing are recorded and monitored. These schemes also enable the verification of who accessed or processed data, services, or functions, ensure ICT products, services, and processes are free from known vulnerabilities, and support timely recovery of data and services in case of incidents. They further guarantee that ICT products, services, and processes are secure by design and default, while maintaining up-to-date software and hardware with secure update mechanisms to address known vulnerabilities.

Certification schemes - governance

Article 58 - National Cybersecurity Certification Authorities

Each Member State must designate one or more national cybersecurity certification authorities, or, with agreement from another Member State, designate authorities from that country. These authorities must be independent in terms of organization, funding, and decision-making. Member States are responsible for ensuring that these authorities have adequate resources to perform their tasks effectively.

Article 97 - Certification Application and Accreditation

Once a European cybersecurity certification scheme is adopted, manufacturers or service providers can submit certification applications to any accredited conformity assessment body in the EU. These bodies must be accredited by national accreditation bodies, with accreditation lasting up to five years and renewable under certain conditions. National accreditation bodies can restrict or revoke accreditation if requirements are not met or if regulations are violated.

Certification schemes - conformity assessment

- A European cybersecurity certification scheme may allow manufacturers or providers of ICT products, services, or processes to perform a conformity self-assessment. This is only permitted for low-risk products or services, corresponding to the "basic" assurance level.
- Manufacturers or providers can issue an EU statement of conformity, declaring that their ICT product, service, or process meets the requirements of the scheme. By doing so, they assume responsibility for ensuring compliance.
- The manufacturer or provider must make the EU statement of conformity, along with technical documentation and other relevant information, available to the national cybersecurity certification authority and ENISA for a specified period.
- Issuing the EU statement of conformity is voluntary unless required by Union or Member State law.
- EU statements of conformity are recognized across all Member States.

Certification schemes

1. **Centralised System**: In a centralised certification system, a single, central authority (such as the European Union or a national body) is responsible for overseeing and managing the certification process. This central body sets the standards, approves certification bodies, and issues the certifications. The goal is to ensure uniformity and consistency across the system
2. **Granular System**: A granular certification system involves multiple levels or categories of certification, each targeting specific areas of ICT products, services, or processes. In this system, certifications may vary depending on factors such as the type of product, its risk level, or its application. The approach allows for more tailored and detailed assessments of conformity.
3. **Legal Effect**: Legal effect refers to the binding nature of the certification. In some cases, certifications may have legal consequences, meaning that once a product, service, or process is certified, it is considered to comply with specific laws or regulations. This could impact market access, liability, or compliance obligations.

Proposal for a revision of the Cybersecurity Act

The proposal amends Regulation (EU) 2019/881 to include **managed security services** as subjects for cybersecurity certification schemes. Managed security services encompass activities like cybersecurity risk management, incident response, penetration testing, security audits, and consultancy.

Article 51a outlines the security objectives for certification schemes for managed security services, which include:

1. Ensuring service providers have highly competent staff with technical expertise, experience, and professional integrity.

2. Ensuring the provider maintains high-quality internal procedures for service delivery.
3. Protecting data from unauthorized access, storage, disclosure, destruction, or alteration.
4. Ensuring the timely restoration of access to data, services, and functions after incidents.
5. Restricting data access to authorized personnel only.
6. Recording and enabling assessment of data usage, access, and processing.
7. Ensuring that the ICT products, services, and processes used are secure by default, free from known vulnerabilities, and regularly updated with the latest security patches.

Cybersecurity Standardization

Standards are documents that define specifications, procedures, and guidelines to ensure safety, consistency, and reliability in products, services, and systems. These standards are based on general agreements and validated by legal entities, serving as guidelines or models in specific contexts (e.g., ISO/IEC).

In the context of cybersecurity, standards focus on security features in applications and cryptographic algorithms, emphasizing security controls, processes, procedures, and guidelines aimed at preventing or mitigating cyberattacks and reducing cyber threat risks.

Advantages of standards include:

- Time savings, cost reduction, and increased profits
- Enhanced user awareness and minimized risks
- Business continuity and compliance with industry best practices
- Opportunities for international comparisons of security systems

Classification of standards:

- Information security (e.g., ISO 27000 series, NIST, SOX)
- Information security governance

Key distinction:

- **Cybersecurity standards** provide detailed methods and expectations for completing processes.
- **Cybersecurity frameworks** are broader guidelines covering various components or domains without specifying the exact steps to follow.

Families of IS standards

1. **ISO 27000 Series**: This is the central category, with several ISO/IEC standards branching out
2. **BSI (British Standards Institution)**: This includes several BSI standards
3. **SoGP**: Refers to another group of standards, likely specific to certain operational guidelines (though this part is less defined in the image).
4. **Industry Related Standards**: This section includes various industry-specific standards

Families of IS frameworks

- **NIST SP 800 Series**: This is the central category, with several NIST (National Institute of Standards and Technology) frameworks
- **COBIT**: Another prominent framework, COBIT (Control Objectives for Information and Related Technologies), is also mentioned as a key reference in the diagram, often used for IT governance and management.

EU Common criteria certification scheme

First Cybersecurity certification scheme

Commission implementing regulation (EU) 2024/482 of 31 January 2024

Laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

Background - European level

The **SOG-IS MRA** (Senior Officials Group Information Systems Security Mutual Recognition Agreement), established in response to EU Council Decisions in 1992 and 1995 and updated in 2010, aims to standardize IT security evaluation across Europe. Its key objectives

include coordinating Common Criteria (CC) protection profiles and certification policies among European Certification Bodies to ensure alignment with the international CCRA group, as well as developing protection profiles in response to EU directives involving IT security.

Participants in the MRA are government organizations or agencies from EU and EFTA countries, committed to ensuring high and consistent standards in IT product evaluations to enhance trust in their security, increasing the availability of evaluated, security-enhanced IT products, avoiding duplicate evaluations, and improving efficiency and cost-effectiveness in evaluation and certification processes.

In June 2023, the SOG-IS MRA Management Committee approved the adoption of the CC:2022 version of Common Criteria for issuing certificates.

Background - International level

ISO/IEC 15408 (Common Criteria) is an international standard for IT product and system security evaluation, consisting of three main parts:

1. **Part 1** – Introduction and General Model: Provides an overview of IT security evaluation concepts and a general evaluation model.
2. **Part 2** – Security Functional Requirements: Defines standard functional components for expressing security requirements for Targets of Evaluation (TOEs).
3. **Part 3** – Security Assurance Requirements: Establishes assurance components for evaluating the trustworthiness of TOEs.

The standard includes a catalogue of components addressing various functional and assurance aspects, though it is too specialized for broader cybersecurity taxonomy purposes.

Common Criteria Recognition Arrangement (CCRA) allows licensed laboratories to evaluate products against specific security properties. Certified products receive a certification recognized by all CCRA signatories, based on the evaluation results and supported by guidelines for applying criteria to specific technologies.

EUCC certification scheme

The **EUCC (European Cybersecurity Certification) scheme**, first proposed on July 1, 2020, is a candidate cybersecurity certification intended to replace the SOG-IS Mutual Recognition Agreement (MRA) schemes. It aims to strengthen the Internal Market and enhance the security of ICT products, especially those with built-in security functions (e.g., firewalls, encryption devices, routers, smartphones, etc.).

Key Features of the EUCC Scheme:

- **Assurance Levels:** Offers two levels of security assurance, 'substantial' and 'high,' suitable for products with demanding security requirements. It does not include a basic level, thus excluding self-assessment options.
- **Objective:** To provide consumers with an impartial security assessment of ICT products, boosting confidence and trust in certified products through detailed analysis and testing against specific security standards.

The existing **Common Criteria (CC)** scheme, recognized by 15 EU countries and over 30 other nations, has certified more than 4,500 products. Within the EU, specific national schemes operate under Common Criteria principles, managed by agencies such as ANSSI (France), BSI (Germany), and OCSI (Italy). These schemes follow similar evaluation criteria, security requirements, and assurance levels.

The proposal establishes rules for implementing **Regulation (EU) 2019/881** concerning the adoption of the **European Common Criteria-based cybersecurity certification scheme (EUCC)**. This scheme, based on Common Criteria standards, sets out requirements and guidelines for certifying the security of ICT products within the EU, aiming to harmonize cybersecurity standards across Member States and increase trust in certified products.

EUCC certification scheme

To obtain an EUCC certificate, the applicant must provide documentation on the intended use of the ICT product and an analysis of associated risk levels. This allows the conformity assessment body to verify that the chosen assurance level is appropriate. If the same body handles both evaluation and certification, the applicant only needs to submit this information once.

A **technical domain** is a framework for ICT products with specific and similar security functions that address common types of attacks, aiding in consistent evaluations.

Two main technical domains currently used for certification are:

- **AVA_VAN.4**: For "smart cards and similar devices," where security relies on tailored hardware elements (e.g., smart card hardware, Trusted Platform Modules).
- **AVA_VAN.5**: For "hardware devices with security boxes," using a physical protective enclosure ("Security Box") to resist direct attacks (e.g., payment terminals, tachographs, and Hardware Security Modules).

Conflict between security and privacy

Values protected within cybersecurity

Identification and implementation of measures and techniques for the protection of information from: unauthorized access, use, modification, destruction, disclosure or disruption

Values protected: security, privacy, fairness, accountability

Security

Security is the state of being free from danger or threat. It encompasses protection against intended harm, distinguishing itself from safety, which refers to protection from accidental or unintentional danger. Security is characterized by the absence of danger or threat.

Privacy

Informational privacy concerns what information about an individual is (or isn't) known to or shared with others. It involves a distinction between confidentiality or secrecy of data and control over what data is shared with whom.

Fairness

Cybersecurity threats and measures impact individuals in different ways, raising issues of equality, justice, non-discrimination, and democracy. Fairness in cybersecurity addresses the need for equitable treatment and outcomes for all individuals.

Accountability

Accountability relates to transparency, openness, and explainability. It involves two scenarios: one in which someone harms another or infringes on their rights, and another in which a power imbalance exists, where the more powerful agent can introduce rules or measures that may harm the less powerful.

Privacy v security

Security is attained at the cost of privacy. Security helps to achieve privacy. Privacy requires some degree of cybersecurity. Privacy is attained at the cost of security. Privacy contributes to security.

GDPR - Data protection

Legal sources

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 04.05.2016.

Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n 196)

- Decreto legislativo 10 agosto 2018, n 101

Personal data - definition

Personal data are defined as information that identifies or makes identifiable, directly or indirectly, a natural person and that can provide information on their characteristics, habits, lifestyle, personal relationships, health status, economic situation, etc

- Data allowing direct identification and data allowing indirect identification
- Sensitive data and judical data
- New data?
    - Data relating to electronic communications, geolocation data

Actors - definitions

Data subject is the natural person to whom the personal data relate (Article 4(1)(1) GDPR)

Data Controller is the natural person, public authority, company, public or private body, association, etc, who takes the decisions on the purposes and means of processing (Article 4(1)(7) GDPR)

Data processor is the natural or legal person whom the controller requires to perform specific and defined tasks of management and control on its behalf of the processing of data (Article 4(1)(8) GDPR)

Scope of application of GDPR

Regulation (EU) 2016/679 governs the processing of personal data irrespective of whether or not is is carried out in EU:

- either when carried out by data controllers or data processors established in the EU or in a place subject to the law of an EU Member State by virtue of public international law

- or when the controller or processor is not established in the Euopean Union but the processing activities concern
  - the offering of goods or the provision of services to the said data subjects in the European Union, irrespective of whether payment by the data subject is compulsory
  - the monitoring of their behavior to the extent that this behavior takes place within the European Union

Rights of the data subject

The data subject has the right to ask the data controller whether their personal data has been processed. If the data has been processed, they have the right to obtain a copy of the data and be informed about the purposes of the processing, the categories of personal data involved, the recipients of the data, the data's storage period, its origin, the identification details of those processing the data, the existence of automated decision-making processes (including profiling), and the rights provided by the Regulation.

The data subject may also request that their personal data be rectified if inaccurate or incomplete, erased, restricted in its processing, or transferred to another data controller, provided the processing is based on consent or a contract concluded with the data subject and is carried out by automated means.

Additionally, the data subject has the right to object to the processing of their personal data for reasons related to their particular situation, specifying the grounds in the request. They may also object to the processing of their data for direct marketing purposes without having to provide any reasons.

Right to be forgotten

Right to erasure of one's personal data in an enhanced form:
Obligation for data controllers (if they have "made public" the personal data of the data subject) to inform other data controllers processing the deleted personal data of the erasure request, including "any link, copy or reproduction" (Art 17(2)).

Data processing

Any processing of personal data must comply with the following principles

- Lawfulness, correctness and transparency of the processing, with regard to the person concerned
- purpose limitation of processing, including the obligation to ensure that any further processing is not incompatible with the purposes of data collection
- data minimization: data must be adequate relevant and limited to what is necessary in relation to the purposes of the processing
- accuracy and updating of data, including the timely deletion of data that are inaccurate in relation to the purposes of processing
- storage limitation: data must be kept for no longer than is necessary for the purposes for which they are processed
- integrity and confidentiality: it is necessary to ensure the adequate security of personal data being processed

Lawful data processing - legal basis

Lawful data processing requires a valid legal basis, which can include consent from the data subject, fulfillment of contractual obligations, protection of vital interests of the data subject or a third party, compliance with legal obligations to which the data controller is subject, processing for the public interest or in the exercise of public authority, and overriding legitimate interests of the data controller or third parties to whom the data is disclosed. For special categories of personal data, processing is generally prohibited, except under specific conditions.

Consent

The validity of consent requires that the data subject has been informed about the processing of their personal data, in accordance with Articles 13 or 14 of the Regulation. Consent must be expressed by the data subject freely, unambiguously, and specifically for each purpose of processing if multiple purposes are involved. The request for consent must be distinct from other requests addressed to the data subject. Additionally, consent does not need to be "documented in writing," nor is a "written form" required.

Information about data processing

It must be provided to the data subject before processing, before the data are collected

The content is provided for in Articles 13(1) and 14(1)

- identity of the data controller
- purpose of processing
- rights of the data subject
- contact details of the DPO

- legitimate interest
- possible transfer to third countries
- period of data retention
- right to lodge a complaint with the supervisory authority
- possible automated decision-making process

The information is in principle given in writing and preferably in electronic format

It must be comprehensible and transparent to the data subject, through the use of clear and plain language

Data transfer to third countries

The transfer of personal data to countries outside the European Union is prohibited, except in the following cases:

- adequacy to the third country recognized by a decision of the European Commission
- in the absence of a Commission adequacy decision, appropriate contractual or contractual safeguards
- in the absence of any other prerequisite, use of exceptions to the prohibition of transfer applicable in specific situations

Data protection Supervisory Authorities

The Article 29 Working Party has become the European Board of Supervisors (EDPB)

National supervisory authorities

- The Italian Data Protection Authority

One stop shop mechanism

The tasks and powers of the Supervisory Authorities

Monitoring and supervision, Advisory functions, Investigative powers, Handling complaints, Corrective powers

Complaints in case of violation

Complaint before Supervisory authority

- preliminary investigation and possible formal administrative procedure that may lead to the adoption of remedies and administrative sanctions

The decision of the supervisory authority may be challenged in court

Administrative sanctions under the GDPR (Art 83)

Administrative sanctions imposed by the DPA

The principles of administrative sanctions

Two groups of fines under the GDPR:

- up to 10M or 2% of the annual global turnover if higher
- up to 20M or 4% of the annual global turnover if higher

The accountability principle in the data protection field

The principle of accountability requires both the data controller and processors to ensure that personal data processing complies with the relevant rules and be able to prove this compliance at any time. It is primarily focused on the data controller and adopts a risk-based approach, meaning that the level of compliance and safeguards must reflect the risks associated with processing activities. The "elements" of accountability involve actions such as documentation, internal policies, and measures to ensure adherence to data protection regulations.

The accountability principle under the GDPR

Adoption of **codes of conduct, certification mechanisms, data protection seals and marks** as facilitating tools to prove compliance with the obligations of the controller (Art 24 par 3 GDPR) and of the processor (Art 28 par 5 GDPR) as well as mitigating factors of administrative sanctions (Art 83 par 2 GDPR)

Records of processing activities (Art 30 GDPR)

Technical and organizational measures to ensure a level of security appropriate to the risk (Art 32 GDPR)

Notification of a personal data breach to the DPA (Art 33 GDPR)

Data Protection Impact Assessment (Art 35 GDPR)

From ACCOUNTABILITY to LIABILITY

Article 82 GDPR (Right to compensation and liability)

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation **shall have the right to receive compensation from the controller or processor for the damage suffered**
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation**.** A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller
3. **A controller or processor shall be exempt fromliability under paragraph 2** if it proves that it is not in any way responsible for the event giving rise to the damage

GDPR - Risk assessment and data breach

Risk in GDPR

Art. 24 GDPR Technical and organisational measures

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

Those measures shall be reviewed and updated where necessary."

Art. 25 data protection by design and by Default

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to

Art. 32 GDPR Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    a. the pseudonymisation and encryption of personal data;
    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Art 35 DPIA

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

What is a risk?

A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood.

Risk catalogue

Recital 75

The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular:

- where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed;
- or where processing involves a large amount of personal data and affects a large number of data subjects.

DPIA

The overall effects of data processing can include damage to reputation, discrimination, identity theft, financial loss, physical or psychological harm, loss of control over personal data, and other economic or social disadvantages. Additionally, individuals may face an inability to exercise their rights, access services, or take advantage of opportunities due to improper processing of their data.

Risk assessment

“Risk assessment” can be defined as the coordinated activities to direct and control an organization with regard to risk

Elements to be considered in the risk assessment: origin, nature, severity, **likelihood, impact** on the rights and freedoms of people

Recital 76

The likelihood and severity of the risks to rights and freedoms of individuals should be determined by reference to:

- The nature
- Scope
- Context
- Purposes of processing

Level of Impact	Description
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc)
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra cost, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc)
Very High	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc)

DPIA

In line with the risk-based approach carrying out a DPIA is not mandatory for every processing operation.

- DPIA is only required where a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons” (Article 35(1)).
- The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers’ general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects.

In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons”.

What is a DPIA?

The GDPR does not formally define the concept of a DPIA as such, but its minimal content is specified by Article 35(7):

- "(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned";

Which processing operations are subject to a DPIA?

Apart from exceptions, where they are "likely to result in a high risk".

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.

Even though a DPIA could be required in other circumstances, Article 35(3) provides some examples when a processing operation is "likely to result in high risks":

- "(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person12;
- (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- (c) a systematic monitoring of a publicly accessible area on a large scale".

When isn't a DPIA required?

WP29 considers that a DPIA is not required in the following cases:

- where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons"
- when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used;
- when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed;
- where a processing operation, pursuant to point (c) or (e) of article 6(1), has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis;
- where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required;

How to carry out a DPIA? At what moment should a DPIA be carried out?

The DPIA should be carried out "prior to the processing". This is consistent with data protection by design and by default principles

The DPIA should be seen as a tool for helping decision-making concerning the processing.

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance.

Carrying out a DPIA is a continual process, not a one-time exercise.

Who ia obliged to carry out the DPIA?

The controller is responsible for ensuring that the DPIA is carried out

Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task

The controller must also seek the advice of the Data Protection Officer (DPO).

If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information

The controller must “seek the views of data subjects or their representatives” “where appropriate”

Sanctions

Non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority.

- Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)),
- Carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)),
- Failing to consult the competent supervisory authority where required (Article 36(3)(e)),

.. can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

Security and data breach

Risk in GDPR

Art. 32 GDPR Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    a. the pseudonymisation and encryption of personal data;
    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Personal data breach

art. 4(12) : A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Not all violations are data breaches
    - A security breach where there is no evidence that it has led to “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”
- Unlawful processing of personal data that is not due to a security incident.

Data breach management framework

Recital 87

It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject

Prevent

1. Educate
2. Minimize (data collection, access to data, data stores, ...)
3. Dispose securely
4. Secure mobile devices (encryption, updates & patches, ..)
5. Secure networks (VPN)
6. Keep software & hardware up-to-date and maintained
7. Manage contractors

8. Develop & clearly communicate policies
9. Prepare for the worst (incidence response, disaster recovery)
10. Audit

Detect

To identify a security incident, it is essential to determine what happened, when it occurred, who was involved, and where it took place. A significant issue is the breach-detection gap, as about 90% of compromises happen within seconds or minutes, but detection within seconds or hours accounts for only around 25% of breaches (ETL 2016). Tools for detection include logging and monitoring, as well as intrusion detection and alerts.

Understanding the root cause involves determining the source of the breach. Was it due to a firewall with an open port, malware on the system, an email phishing attack, outdated antivirus software, or an employee who accidentally disclosed personal data? Tools for this phase include forensic analysis and audits.

Once the breach is identified and its cause understood, the incident must be escalated and reported internally to the relevant teams for further action.

Evaluate

- To determine if it's a personal data breach, assess if there was unauthorized access, disclosure, or loss of personal data that could harm data subjects.
- Verify technical and organizational measures by reviewing security policies, audits, and controls like encryption and access restrictions.
- Notify a competent authority if the breach risks individuals' rights, within 72 hours of discovery.
- Notify affected individuals if the breach poses a high risk to their rights, considering factors like the data type, number of people affected, and time between breach and detection.

Mitigate

Take immediate actions by isolating the affected system, changing passwords, and removing compromised webpages if possible. Ensure that systems are no longer at risk by fixing the issue. Document all actions taken and implement corrective measures to prevent future breaches. Finally, notify relevant parties both internally and externally.

Communicate (1)

From processor to controller (internal)

- Art. 33 (2) GDPR : the processor must notify the controller immediately after becoming aware of the data breach
- Art. 28(3)(f) GDPR : Processors also must assist controllers in ensuring compliance with the latter’s obligation to notify a breach to the DPA

Communicate (2)

From controller to DPA

- Art. 33(1) GDPR : In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent …
- unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. […].
- Art. 33 (4) GDPR : Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay

Communicate (3)

Notification to DPA

- Nature of the breach, categories and approximate number of data subjects, categories and approximate number of personal data records concerned.
- Name and contact information of DPO or other contact point.
- Likely consequences of the breach.
- Description of the measures taken or proposed to be taken in order to address the breach, as well as measures for the mitigation of possible adverse effects of the breach.
- Additional information

Communicate (4) to the data subjects

According to Art. 33(3) of the GDPR, if a breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller must notify the data subject without undue delay. However, there are exceptions:

- If the data controller has implemented appropriate technical and organizational measures, such as encryption, which were applied before the breach, rendering the personal data unintelligible to unauthorized persons.
- If subsequent measures have been taken to ensure that the high risk to data subjects no longer materializes.
- If notifying the data subjects would involve disproportionate effort, in which case public communication may be used instead.

Communicate (5) to the data subjects

Information to be provided to individuals

- Name and contact information of DPO or other contact point.
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Communicate (5) to the public

There is no legal obligation to communicate with the broader public unless the breach involves a high risk to the rights and freedoms of individuals and notifying data subjects directly would be disproportionate. In such cases, public communication may be used.

Data breach transparency plays a key role in building trust between data subjects and controllers. It is also an important aspect of an organization’s assets, as a strong compliance framework can enhance the company’s value, particularly in scenarios like mergers or takeovers. Additionally, transparency helps protect the organization's reputation by demonstrating accountability and responsibility in handling personal data.

European Data strategy

Communication, A European strategy for data, 19.2.2020, COM(2020) 66 final

“The European data space will give businesses in the EU the possibility to build on the scale of the Single market. Common European rules and efficient enforcement mechanisms should ensure that:

- data can flow within the EU and across sectors;
- European rules and values, in particular personal data protection, consumer protection legislation and competition law, are fully respected;
- the rules for access to and use of data are fair, practical and clear, and there are clear and trustworthy data governance mechanisms in place;there is an open, but assertive approach to international data flows, based on European values.”

Challenges for data economy

The value of data comes from its use and reuse, supporting the public good through various interactions like G2B, B2B, B2G, and G2G. Market power imbalances can occur when data is controlled by a few entities.

Data interoperability, quality, structure, and integrity are key for maximizing data's value, especially with AI. Proper data governance, supported by the right infrastructures and technologies, ensures effective management. Empowering individuals to exercise their rights is crucial for data control and protection.

Data Act

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)

Article 1 Subject matter and scope

- This Regulation establishes harmonized rules on the making available of product and service data to users of connected products or related services, the making available of data from data holders to recipients, and the provision of data from data holders to public sector bodies, the European Commission, the European Central Bank, and Union bodies when required for tasks in the public interest. It also covers facilitating switching between data processing services, safeguarding against unlawful third-party access to non-personal data, and developing interoperability standards for accessing, transferring, and using data.
- This Regulation applies to manufacturers of connected products and providers of related services in the Union, regardless of their location, users of connected products or related services in the Union, and data holders making data available to recipients in the Union, irrespective of their location. It also applies to data recipients in the Union, public sector bodies, the European Commission, the European Central Bank, and Union bodies requesting data for public interest tasks, and the data holders providing such data. Furthermore, it includes providers of data processing services to customers in the Union, regardless of their location, and participants

in data spaces, vendors of applications using smart contracts, and individuals involved in deploying smart contracts for others in executing agreements.

Actors

(11) ‘data subject’ means data subject as referred to in Article 4, point (1), of Regulation (EU) 2016/679;

(12) ‘user’ means a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services;

(13) ‘data holder’ means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service;

(14) ‘data recipient’ means a natural or legal person, acting for purposes which are related to that person’s trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law

Data Act: B2G data exchange

Chapter V - Making data available to public sector bodies, the Commission, the European Central Bank and Union bodies on the basis of an exceptional need

Article 14 - Obligation to make data available on the basis of an exceptional need

Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates **an exceptional need**, as set out in Article 15, to use certain data, including the relevant metadata necessary to interpret and use those data, to carry out its statutory duties in the public interest, data holders that are legal persons, other than public sectors bodies, which hold those data shall make them available upon a duly reasoned request

Data act and cybersecurity

Article 15 - Exceptional need to use data

1. An exceptional need to use certain data within the meaning of this Chapter shall be limited in time and scope and shall be considered to exist only in any of the following circumstances:
    - (a) where the data requested is necessary to respond to a public emergency and the public sector body, the Commission, the European Central Bank or the Union body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions;
    - (b) in circumstances not covered by point (a) and only insofar as non-personal data is concerned, where:
        - a public sector body, the Commission, the European Central Bank or a Union body is acting on the basis of Union or national law and has identified specific data, the lack of which prevents it from fulfilling a specific task carried out in the public interest, that has been explicitly provided for by law, such as the production of official statistics or the mitigation of or recovery from a public emergency; and
        - the public sector body, the Commission, the European Central Bank or the Union body has exhausted all other means at its disposal to obtain such data, including purchase of non-personal data on the market by offering market rates, or by relying on existing obligations to make data available or the adoption of new legislative measures which could guarantee the timely availability of the data

B2G data exchange

(29) ‘public emergency’ means an exceptional situation, limited in time, such as a public health emergency, an emergency resulting from natural disasters, a human-induced major disaster, **including a major cybersecurity incident**, negatively affecting the population of the Union or the whole or part of a Member State, with a risk of serious and lasting repercussions for living conditions or economic stability, financial stability, or the substantial and immediate degradation of economic assets in the Union or the relevant Member State and which is determined or officially declared in accordance with the relevant procedures under Union or national law;

Data Act and Cybersecurity

Example

A large healthcare provider is targeted by a cyberattack that happened through ransomware inside a DICOM file image of an MRI scan.

The DICOM file infects the doctor’s computer and then reaches the hospital’s Picture Archiving and Communication System (PACS).

The ransomware proliferates to the whole hospital network shutting down all the operations and causing data and service unavailability.

Recital (64)

In the case of public emergencies, such as public health emergencies, emergencies resulting from natural disasters including those aggravated by climate change and environmental degradation, as well as human-induced major disasters, such as major cybersecurity incidents, the public interest resulting from the use of the data will outweigh the interests of the data holders to dispose freely of the data they hold. In such a case, data holders should be placed under an obligation to make the data available to public sector bodies, the Commission, the European Central Bank or Union bodies upon their request. The existence of a public emergency should be determined or declared in accordance with Union or national law and based on the relevant procedures, including those of the relevant international organisations. In such cases, the public sector body should demonstrate that the data in scope of the request could not otherwise be obtained in a timely and effective manner and under equivalent conditions, for instance by way of the voluntary provision of data by another enterprise or the consultation of a public database.

Article 17 Requests for data to be made available

1. When requesting data pursuant to Article 14, a public sector body, the Commission, the European Central Bank or a Union body shall:
    a. specify the data required, including the relevant metadata necessary to interpret and use those data;
    b. demonstrate that the conditions necessary for the existence of an exceptional need as referred to in Article 15 for the purpose of which
    the data are requested are met;
    c. explain the purpose of the request, the intended use of the data requested, including, where applicable, by a third party in accordance with paragraph 4 of this Article, the duration of that use, and, where relevant, how the processing of personal data is to address the exceptional need;
    d. specify, if possible, when the data are expected to be erased by all parties that have access to them;
    e. justify the choice of data holder to which the request is addressed;
    f. specify any other public sector bodies or the Commission, European Central Bank or Union bodies and the third parties with which the data requested is expected to be shared with;
    g. where personal data are requested, specify any technical and organisational measures necessary and proportionate to implement data protection principles and necessary safeguards, such as pseudonymisation, and whether anonymisation can be applied by the data holder before making the data available;
    h. state the legal provision allocating to the requesting public sector body, the Commission, the European Central Bank or the Union body the specific task carried out in the public interest relevant for requesting the data;
    i. specify the deadline by which the data are to be made available and the deadline referred to in Article 18(2) by which the data holder may decline or seek modification of the request;
    j. make its best efforts to avoid compliance with the data request resulting in the data holders' liability for infringement of Union or national law.

Article 17 requests for data to be made available

2. A request for data made pursuant to paragraph 1 of this Article shall:
    a. be made in writing and expressed in clear, concise and plain language understandable to the data holder;
    b. be specific regarding the type of data requested and correspond to data which the data holder has control over at the time of the request;
    c. be proportionate to the exceptional need and duly justified, regarding the granularity and volume of the data requested and frequency of access of the data requested;
    d. respect the legitimate aims of the data holder, committing to ensuring the protection of trade secrets in accordance with Article 19(3), and the cost and effort required to make the data available;
    e. concern non-personal data, and only if this is demonstrated to be insufficient to respond to the exceptional need to use data, in accordance with Article 15(1), point (a), request personal data in pseudonymised form and establish the technical and organisational measures that are to be taken to protect the data;
    f. info m the data holder of the penalties that are to be imposed pursuant to Article 40 by the competent authority designated pursuant to Article 37 in the event of non- compliance with the request; [...]

Article 18 - Compliance with requests for data

1. A data holder receiving a request to make data available under this Chapter shall make the data available to the requesting public sector body, the Commission, the European Central Bank or a Union body without undue delay, taking into account necessary technical, organisational and legal measures

Autonomous driving vehicles

Connectivity

- Vehicle-to-Network (V2N)
- Vehicle-to-Vehicle (V2V)
- Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V)
- Vehicle-to-Person (V2P)
- Vehicle-to-Device (V2D) and Vehicle-to-Everything (V2X)

Current available features of Avs

- Up to today most functions have been primarily designed to assist drivers rather than replace them by providing warnings, or taking control of the vehicles in limited situations.
- In the future, with fully developed AVs, these functions are part of the driving process and, essentially, contribute to replacing the driver

The role of AI in Autonomous vehicles

- Sense
- Perceive & Localize
- Scene representation
- Plan & Decide
- Control

AI technologies in AV

Object recognition

- Detecting (localization) and classifying objects in an image

Segmentation

- A label is assigned to each region to classify them into prescribed categories

Vehicle localization

- Technique used to estimate using a sequence of images captured over time by the camera mounted on the vehicle

Tracking of objects

- Technique used to determine the dynamics of moving objects

Cybersecurity issues

◦ Intentional threats
◦ malevolent exploitation of the limitations and vulnerabilities present in AI and ML methods to cause intended offence and harm
◦ Unintentional threats
◦ side effects of benevolent usages, due to open issues inherent in the trustworthiness, robustness, limitations and safety of current AI and ML methods

Threat Type	Description	Real-World Examples	Potential Impacts
Remote Hacking	Unauthorized access to vehicle systems via wireless communication	Jeep Cherokee hack (2015)	Vehicle control takeover, disabling functions, safety risks
Sensor Manipulation	Interference with sensors like LiDAR, radar, cameras	Tesla autopilot deception (2016)	False obstacle detection, erratic behavior, collisions
Data Breaches	Unauthorized access to sensitive data stored or transmitted by the vehicle	Electric vehicle manufacturer server hack (2020)	Privacy violations, identity theft, compromised decision-making

DoS Attacks	Overloading vehicle's systems to disrupt normal operations	DDoS attacks on vehicle-to-infrastructure networks	Performance degradation, connectivity loss, vehicle immobilization

Countermeasure	Description	Benefits
Intrusion Detection Systems	Monitoring network traffic for malicious activity	Real-time threat detection, anomaly identification
Encryption	Security data in transit and at rest	Protects data integrity and confidentiality
Regular Updates	OTA updates for software and firmware	Addresses vulnerabilities, enhances functionality
Authentication Protocols	Ensuring only authorized access to vehicle systems	Prevents unauthorized access, secures communication

European interventions

1. 2016, the European Commission adopted a European Strategy on Cooperative Intelligent Transport Systems,
2. In 2016, the Member States and the European Commission launched the C Roads Platform to link C-ITS deployment activities,
3. In 2018, the European Commission published the EU Strategy for mobility of the future
4. In 2019, the European Commission has set up a Commission Expert group on cooperative, connected, automated and autonomous mobility, named "CCAM"
5. In September 2020, report on Ethics of Connected and Automated Vehicles
6. Regulation 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users (Vehicle General Safety regulation)

International interventions: UN Regulations No. 155 and 156

UN Regulation No. 155 on Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

- requires a Certificate of Compliance for Cyber Security Management System from a vehicle manufacturer in order to have its vehicle approved for use on public roads
  - 'a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyberattacks'
  - Such asprocesses used for the identification of risks to vehicle types and processes used for testing the cyber security of a vehicle type (e.g. mitigation methods of different cybersecurity risks, including measures to prevent and detect unauthorized access shall be employed).
- Objective: ensure no one can gain unauthorised access to the vehicle's system

UN Regulation No. 156 concerning Uniform provisions concerning the approval of vehicles with regards to software update and software update management

- requirements on how to update the software of the vehicle
  - Certificate of compliance for Software Update Management System
  - It is a systematic approach defining organisational processes and procedures to comply with the requirements for delivery of software updates
  - Such as
    - aprocess whereby any interdependencies of the updated system with other systems can be identified
    - a process to establish the compatibility of the update with the target vehicle configuration

EU legislation

Vehicle General Safety Regulation 2019/2144

- Entered into force 6 July 2022
- Objectives: Introduce mandatory advanced driver assistant systems to improve road safety and establishes the legal framework for the approval of automated and fully driverless vehicles in the EU.

Vehicle general safety regulation

(26) The connectivity and automation of vehicles increase the possibility for **unauthorised remote access to in-vehicle data and the illegal modification of software over the air**. In order to take into account such risks, **UN Regulations or other regulatory acts on cyber security should be applied on a mandatory basis** as soon as possible after their entry into force.

(27) Software modifications can significantly change vehicle functionalities. Harmonised rules and technical requirements for software modifications should be established in line with the type-approval procedures. Therefore, UN Regulations or other regulatory acts regarding software update processes should be applied on a mandatory basis as soon as possible after their entry into force. However, those **security measures should not compromise the obligations of the vehicle manufacturer to provide access to comprehensive diagnostic information and in-vehicle data relevant to vehicle repair and maintenance.**

Article 4 General obligations and technical requirements

5. Manufacturers shall also ensure that vehicles, systems, components and separate technical units comply with the applicable requirements listed in Annex II with effect from the dates specified in that Annex, with the detailed technical requirements and test procedures laid down in the delegated acts and with the uniform procedures and technical specifications laid down in the implementing acts adopted pursuant to this Regulation, including the requirements relating to:

- (a) restraint systems, crash testing, fuel system integrity and high voltage electrical safety;
- (b) vulnerable road users, vision and visibility;
- (c) vehicle chassis, braking, tyres and steering;
- (d) on-board instruments, electrical system, vehicle lighting and protection against unauthorised use including cyberattacks;
- (e) driver and system behaviour; and
- (f) general vehicle construction and features

Article 11 Specific requirements relating to automated vehicles and fully automated vehicles

1. In addition to the other requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it that are applicable to vehicles of the respective categories, automated vehicles and fully automated vehicles shall comply with the technical specifications set out in the implementing acts referred to in paragraph 2 that relate to:
    a. systems to replace the driver's control of the vehicle, including signalling, steering, accelerating and braking;
    b. systems to provide the vehicle with real-time information on the state of the vehicle and the surrounding area;
    c. driver availability monitoring systems;
    d. event data recorders for automated vehicles;
    e. harmonised format for the exchange of data for instance for multi-brand vehicle platooning;
    f. systems to provide safety information to other road users.

However, those technical specifications relating to driver availability monitoring systems, referred to in point (c) of the first subparagraph, shall not apply to fully automated vehicles.

2. The Commission shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications for the systems and other items listed in points (a) to (f) of paragraph 1 of this Article, and for the type-approval of automated and fully automated vehicles with regard to those systems and other items in order to ensure the safe operation of automated and fully automated vehicles on public roads.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2)

Internet of Things

IoT definition

There is no universally accepted definition of the Internet of Things (IoT), and its elements can vary, including the technology, tools, and applications involved. According to the International Telecommunication Union, IoT is described as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."

The IoT ecosystem consists of objects connected to the network through sensors, which interface with the physical world and interact with each other. These objects exchange information about their status and the surrounding environment without the need for human intervention.

Technical structure

The technical structure of IoT is typically divided into three layers: the **perception layer**, which involves the sensors and devices gathering data; the **processing layer**, which handles the data processing and decision-making; and the **application layer**, where the processed data is used to provide services and functionalities to users.

IoT technical architecture - security risks

At the **information level**, key risks include ensuring the integrity of data, protecting anonymity, maintaining confidentiality, and safeguarding privacy.

At the **access level**, the primary concerns are access control, authentication, and authorization to ensure only authorized individuals or systems can access the data and services.

At the **functional level**, the focus is on resilience to attacks or failures and enabling self-organization to allow the system to adapt to changing conditions or threats.

IoT and data protection

There is no direct binary connection between a data processor and a data subject in IoT systems. The data collected can produce valuable insights, or "fruits," which can be complex both subjectively and objectively. Various types of data can be collected, creating a diverse set of challenges.

The WP29 Opinion 8/2014 on recent developments in the Internet of Things highlights several privacy and data protection concerns posed by IoT. These include both new and traditional challenges, amplified by the exponential growth in data processing. The eight main issues identified are:

1. Lack of transparency in IoT systems.
2. The involvement of various actors, often unknown to users.
3. Loss of control over data processing through IoT devices.
4. Difficulty in obtaining valid user consent, with the quality of consent often compromised.
5. Lack of granularity in IoT services, forcing users to accept all data processing aspects or refuse the service entirely.
6. The possibility of processing more data than necessary for the original purpose.
7. The use of data from different sources and devices for purposes other than originally intended.
8. Security risks in the transmission of personal data between devices, central services, or other devices.

Compatibility level

Specific and adequately informed consent is necessary for data processing.

Regulation 1807/2018 on the free flow of data ensures the movement of data within the EU while protecting privacy.

The **purpose principle** requires data to be used only for specified purposes.

Data storage limits ensure data isn't kept longer than necessary.

Transfers to third countries must comply with data protection requirements.

Identification of data processor ensures clarity on responsibilities.

Privacy by design and security by design

Accountability standards

- Pseudonyms and Reducing the Amount of Data Collected
- Consent to Transparent Terms of Processing
- Design of Privacy Policies
- Secure Transmission and Retrieval of Data

Cybersecurity issues

Article 13 Cyber Resilience Act

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Part 1 of Annex I.
2. For the purposes of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimizing cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.

Security requirements include a risk-based approach considering the CIA triad (Confidentiality, Integrity, Availability), ensuring data minimization, resilience against DoS attacks, avoiding network effects, implementing security by design with mitigation measures, maintaining a record of internal activities, and providing updates, including automatic ones.

Vulnerability handling requirements are also risk-based, requiring tests and security updates to be provided for free to users, along with information sharing, particularly with manufacturers of third-party components

Privacy by design and security by design

Market interventions:

- ioXt Security Pledge
    1. No universal passwords: The product shall not have a universal password; unique security credentials will be required for operation.
    2. Secured interfaces: All product interfaces shall be appropriately secured by the manufacturer.
    3. Proven cryptography: Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.
    4. Security by default: Product security shall be appropriately enabled by default by the manufacturer.
    5. Signed software updates: The product shall only support signed software updates.
    6. Automatically applied updates: The manufacturer shall act quickly to apply timely security updates.
    7. Vulnerability reporting program: The manufacturer shall implement a vulnerability reporting program, which shall be addressed in a timely manner.
    8. Security expiration date: The manufacturer shall be transparent about the period of time that security updates will be provided.

Liability for damages of IoT

Liability for damages is addressed in **Article 82 GDPR**, which establishes liability for parties involved in the processing of personal data. It also coordinates with the **Product Liability Directive**, which provides for compensation for damages resulting from defective products.

Liability in Artificial Intelligence

The **Proposal for an AI Liability Directive** aims to enhance the functioning of the internal market by establishing uniform rules for non-contractual civil liability for damage caused by AI systems. Its goals include promoting trustworthy AI, ensuring victims of AI-related damage receive equivalent protection to those harmed by products, and reducing legal uncertainty for businesses involved in AI. This will prevent fragmented national liability rules for AI.

The directive provides **extra-contractual** liability rules, meaning compensation can be claimed regardless of a contractual relationship between the victim and the liable party. It covers damages to individuals or businesses caused by the fault or omission of an AI provider, developer, or user in areas such as health, property, and privacy. However, it excludes transport-related liability, the revision of the Product Liability Directive, the Digital Services Act, and criminal liability.

Article 4 introduces a **presumption of causality**, simplifying claims by linking non-compliance with Union or national law to AI system output or its failure to produce relevant results. If a victim can show fault and a probable causal link between the AI's performance and the harm, the court can presume the non-compliance caused the damage, making it easier for victims to claim compensation. However, the burden of proof is not fully reversed.

Internet of Health Things

IoT

The ecosystem consists of objects connected to the network through sensors, which interface with the physical world, interact with each other, and exchange information about their status and the surrounding environment, all without human intervention. This applies to **health devices**.

The **perception layer** includes wearable and implanted devices, as well as hospitals.

The **processing layer** involves middleware services.

The **application layer** encompasses high-level services.

GDPR application

Processing of health data is defined under **Article 4(15) GDPR**, where health data are described as "personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about their health status." **Recital 35** further clarifies that health data covers the data subject's past, current, or future health conditions.

- Lawful processing
  - art. 9 GDPR
    - Processing of special categories of data only in case of specific legal basis: consent by the data subject, data processing carried out to protect the vital interests of the data subject or another natural person when the data subject is physically or legally incapable of giving consent, data manifestly made public by the data subject, data processing aimed at preventive or occupational medicine and also data processing for reasons of public interest in the area of public health.

Security requirements

- Art. 32 GDPR
  - data controller should “implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk” to protect personal data from unauthorised or unlawful processing and against accidental loss, destruction or damage.
- What happens in case of violation?
- CNIL decision SAN-2022-009, 15 April 2022 :
  - French Data Protection Authority imposed an administrative fine of 1.5 million euros on a company dealing with medical data which failed to comply with Arts 28, 29, and 32 GDPR.
  - The security of personal data was not ensured, as numerous technical and organisational breaches in terms of security were found: lack of a specific procedure for data migration operations; lack of encryption of personal data stored on the problematic server; no automatic deletion of data after migration to the other software; no authentication required from the Internet to access the public area of the server; use of user accounts shared by several employees on the private area of the server; lack of a procedure for monitoring and reporting security alerts on the server.

Medical Device Regulation application

Medical Devices Regulation 2017/745

- Art. 2(1) MDR
  - A medical device is “any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for the purpose of diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability; investigation, replacement or modification of the anatomy or of a physiological or pathological process or state; and providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.
  - NB inclusion of ‘software’ among the types of medical devices, both stand-alone software and software connected to other software, and software offered as a service to another medical device.

Medical v wellness devices/software

- If the purpose is among the ones listed, the device/software qualifies as a medical device
  - art 2 (12) MDR : the purpose is indicated by the manufacturer. Therefore, it is up to the manufacturer to provide information about the device's purpose on the label, in the instructions for use or in promotional or sales materials or statements.
  - BUT IoT devices that do not have a medical purpose are not subject to the MDR. However, they may still be used in medicine as they collect health-related data.

IOMT

- certification procedure requiring compliance with a minimum essential quality and safety criteria defined in Annex I MDR.

Notification procedure

Art. 87 MDR : In case of a serious incident, the manufacturer must report the incident to the relevant competent authority.

Art. 2 (65) MDR, a serious incident is “any incident that directly or indirectly led, might have led, or might lead to any of the following:

- the death of a patient, user or other person,

- the temporary or permanent serious deterioration of a patient's, user's or other person's state of health,
- a serious public health threat.

Timeline:

- 2 days after the manufacturer becomes aware in case of a serious public health threat
- 10 days after the causal relationship between the device and serious incident is established/suspected in case of death or a severe unanticipated deterioration in a person's state of health
- 15 days after the causal relationship between the device and serious incident is established/suspected to any other serious incident.

Manufacturers must

- conduct investigations as soon as they are informed that a serious incident has occurred
- take corrective actions for medical or technical reasons to prevent or reduce the risk of a serious incident, i.e., field safety corrective actions (FSCA)
    - the return of a device to the supplier or a recall, a device exchange, a device modification, retrofit by the purchaser of manufacturer’s modification or design change, a device destruction, advice given by the manufacturer regarding the use of the device, recommended inspections/examination by the device user, changes of software/firmware in the device, including device update.
- As soon as the manufacturer decides to implement any of these measures, the device users should be informed through a field safety notice (FSN) to ensure that required actions are followed and completed in a timely manner.

Interplay between GDPR and MDR

Medical IoT should comply at the same time with the GDPR and the MDR requirements.

- Are the national notification bodies in charge of verifying compliance with MDR requirements also asked to verify compliance with GDPR?
- To what extent, for instance, is the DPIA carried out by the manufacturer as a data controller sufficient to demonstrate the security measures provided in the MDR?

CRA application

IoHT are products with digital elements

- Art. 2(68) CRA “any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.”

CRA’s scope of application does not cover products with digital elements that are covered by the definition of medical devices

- IoMT subject to the MDR security and safety requirements
- IoHT subject to the CRA requirements for cybersecurity

Art. 13 CRA

- Before they are put on the market, products with digital elements must be designed, developed and manufactured in such a way as to ensure an appropriate level of cybersecurity.
- Products must be delivered without known exploitable vulnerabilities and deployed in a secure default configuration.
- Annex 1 –Security and vulnerability handling equirements

Notification

- Art. 14 CRA
- Manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA.
    - an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it
    - unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability
    - unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available

Open issues

Open issues include the need for **coordination between horizontal legislation and sector-specific ones**, such as distinguishing between medical and health devices and addressing generic standards in the **Cyber Resilience Act (CRA)**.

Notification overload is another concern, with issues such as overlapping timelines, different authorities, and varying content requirements for notifications.

Cloud computing

Definition technical

According to National Institute of Standards and Technology (NIST) a 'computing capacity' will qualify as a 'cloud service' if it has the following five characteristics:

1. 'on- demand self- service'
2. 'broad network access'
3. 'resource pooling'
4. 'rapid elasticity' and
5. 'measured service'.

Models of Cloud services

- Infrastructure as a Service, Platform as a Service, Software as a Service

Types of cloud services

Private cloud, Community cloud, Public cloud, Hybrid cloud

Cloud service levels

- the data level, representing the data household of cloud computing, with both stored data anddataintransit;
- the application level, representing installed applications using the cloud computing resources (hardware and software);
- the network level, representing the network elements/service used by the cloud computing node, including security elements responsible for the network protection;
- the host level, representing all elements supporting the virtualisation functions, such as the virtual server, virtual machines and the hypervisor.

Cybersecurity in Cloud service

ENISA Cloud Cybersecurity Market Analysis, March 2023

"Various gaps in the cloud cybersecurity market emerge through mismatches in deployment of cybersecurity functions between the demand side and supply side. The market gaps are rooted in concerns about the management of various threats and unclear distributions responsibilities about the implementation and maintenance of cloud cybersecurity functions."

Stakeholders involved in cloud computing include the demand side, which consists of end users of cloud services, and the supply side, which includes cloud service providers (CSPs) and cloud enablers. Additionally, organizations conducting research and development (R&D) in cloud computing and regulatory bodies overseeing activities related to cloud computing play crucial roles.

The relationship between cybersecurity and cloud computing is multi-dimensional. Companies in the cybersecurity market contribute to cloud computing by offering security from the cloud, security for the cloud computing infrastructure (e.g., securing stack components), and security in the cloud, such as ensuring data confidentiality. On the other hand, companies in the cloud computing market offer public cloud services, independent software vendors, and managed cloud services, along with cloud brokers and other related offerings.

Specific Features

The Cloud contract includes a set of technical elements that applies regardless of the type of service covered by the contract itself:

1. the data are no longer stored on the user's 'physical' servers but are allocated on the provider's systems (except for local copies)
2. the service provider's infrastructure is shared among many users (multi-tenant model), so adequate levels of security are essential
3. use of the service is via the web through the Internet, which therefore assumes a central role for the qualitỳ of the services used and supplied
4. services that can be acquired from the service provider are on a pay-as-you-go basis to cope with any needs that may arise with elastic and simplified
   implementation systems (e.g. when more disk space or more computing power is needed).

Definition of processing operation and its context

Personal data processed	Contact information (patient's last and first name, address, telephone number, email address), contact information of relatives for emergency cases, social insurance number, medical appointments, medical examination results, pathologies, allergies, diagnosis and treatment plans (medical information), administrative and financial information (invoices, hospitalization papers, etc)
Processing Purpose	Provision of healthcare services (diagnosis, treatment, hospitalization), treatment planning and billing
Data Subject	Patients, relatives, doctors, nurses
Recipient of the Data	Doctors and nurses, administration and accounting department, public health system, patients
Data Processor	IaaS Cloud service provider

Data protection challenges

Privacy by design techniques, Data management, Data deletion, Data portability

Cybersecurity challenges

Access control, audit, authorization, availability, chain of trust, chain of responsibility, compliance, confidentiality, cybersecurity incident management, identification and authentication, integrity, mutli-tenancy, network security, privacy, storage, transparency, visibility, non-repudiation

Cybersecurity architecture in cloud computing

Access Control	Controls access to data and systems through authentication and authorization mechanisms	Authentification and authorization
Encryption	Converts data into a coded format to prevent unauthorized access, applied to data at rest and in transit	Applied to different levels (storage, network or application)
Data Backup & Recovery	Ensures data can be recovered in the event of a breach or system failure, stored in a secure location	Data backups in separate cloud service or on-premise data center
Network Security	Protects against cyber attacks and unauthorized access	firewalls, IDS/IPS, and VPNs
Compliance	Adherence to relevant regulations and standards, like GDPR and PCI DSS, is vital for strong cybersecurity	

Cybersecurity challenges

Acquisition refers to the seizure and collection of remote data, large data volumes, and distributed and elastic data potentially linked to the allegation or incident in the cloud environment.

Preservation involves maintaining the integrity of digital artifacts through imaging, hashing, and duplication functions to ensure the evidence remains unaltered.

Examination is the process of reviewing the forensic data collected during the acquisition phase to generate input for further forensic analysis.

Analysis involves the detailed examination of the data, including data fusion and correlation, to draw reasoned conclusions.

Reporting refers to the presentation of the results, documenting the findings of the forensic analysis.

Digital Services Act - DSA

E-Commerce Directive (Directive 2000/31/EC)

Scope: all information society services (ISS) established in a MS [*including online intermediaries such as mere conduits*]

Objective: contribute to the proper functioning of the internal market

Country of origin principle: derogation only opossible on the basis of limited reasons and procedural requirements

Limited liability exemption for intermediaries, without prejudice to court orders [now replaced by DSA]

DSA features

The aim of this regulation is to ensure online safety, reduce the spread of illegal and harmful content, promote a more open and transparent internet, safeguard freedom of speech, and improve protection for minors.

It has a horizontal application, covering all types of online intermediaries and illegal content.

The regulation is neutral in that illegality is defined by national or EU law, but injunctive relief is always possible in line with national legislation and the conditions set out in the Digital Services Act (DSA).

It harmonizes liability exemptions, ensuring it does not attribute liability for content, while establishing self-standing due diligence obligations for those involved.

Very large online platforms	Online platforms and search engines with over 45 million users in the EU
Online platforms	Online marketplaces, app stores, collaborative economy platforms, social networks…
Hosting services	Cloud services, webhosting…
Intermediaries	Internet access providers, domain name registries

Notice and action

The continuity between the Digital Services Act (DSA) and the E-Commerce Directive is found in Articles 4, 5, and 6 of the DSA, which correspond to Articles 12, 13, and 14 of the E-Commerce Directive. Both sets of articles make a distinction between different types of online service providers: mere conduit, caching, and hosting. Liability can arise from any type of illegal content, regardless of its nature or origin.

The DSA introduces novelties, such as Article 6(3), which addresses liability under consumer protection law, and the exception of liability, which is linked to the fulfillment of due diligence obligations.

Existing CJEU jurisprudence

ISP should be a neutral actor: no active role that could give the ISP knowledge of or control over the content (Recital 18)

Mere conduit, caching and hosting ISP are different = mere technical and automatic processing should be adapted to the type of services

Existing CJEU caselaw

Good samaritan clause - Art 7 DSA

- Exemption of liability still applies in case of voluntary measures aimed at tackling illegal content

Public Scrutiny

The design of platforms' systems prioritizes societal risks and interests. A dynamic approach is used to identify and address emerging societal risks. This approach covers the core design of a service, including its terms and conditions, algorithmic systems, and optimization choices. Robust oversight is essential and includes independent audits, regulatory supervision, and public scrutiny through transparency reports, data access for researchers, consultation on guidelines, and involvement in risk assessment and mitigation design.

Governance and enforcement

At the national level, the Digital Services Coordinator (DSC) is an independent authority responsible for coordinating with other national competent authorities, and directly supervising and enforcing compliance. The European Board for Digital Services is an ad-hoc independent advisory group, composed of national Digital Services Coordinators, chaired by the Commission, and tasked with advising DSCs and the Commission, while issuing recommendations. The European Commission has direct enforcement powers over Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), advises on cross-border disputes, and intervenes following DSC requests.

There is no legal obligation to communicate with the broader public unless the breach involves a high risk to the rights and freedoms of individuals and notifying data subjects directly would be disproportionate. In such cases, public communication may be used.

Data breach transparency plays a key role in building trust between data subjects and controllers. It is also an important aspect of an organization’s assets, as a strong compliance framework can enhance the company’s value, particularly in scenarios like mergers or takeovers. Additionally, transparency helps protect the organization's reputation by demonstrating accountability and responsibility in handling personal data.