



EUPC Digital Playbook

2nd Edition | October 2025



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex

The EU Policy Centre (EUPC)

Advocating for policies that support innovation and growth, contributing to the development of regulatory frameworks, and shaping regulatory conversations around several EUPC clusters

EUPC Clusters



The EUPC Cyberspace & Digital Economy Cluster (1/2)

The EUPC Cyberspace & Digital Economy Cluster makes Deloitte’s insights and research on cyber and digital public policy issues and legislation available to key policy makers and to Deloitte’s clients, building relationships between professionals, business leaders, and decision-makers



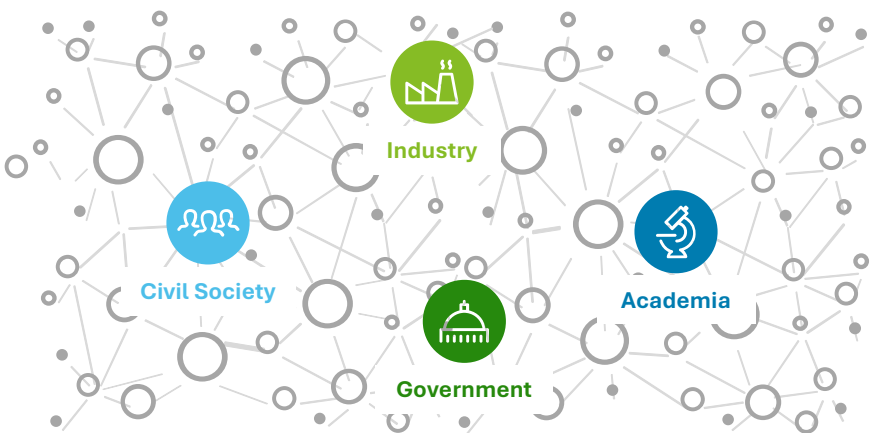
The EUPC Cyberspace & Digital Economy Cluster (2/2)

The EUPC Cyberspace & Digital Economy Cluster adopts an ecosystem approach, enabling a constant flow of information between our network and the institutions to deliver useful insights to our clients and be the strategic advisor of choice on EU cyber and digital policy

GOAL & APPROACH

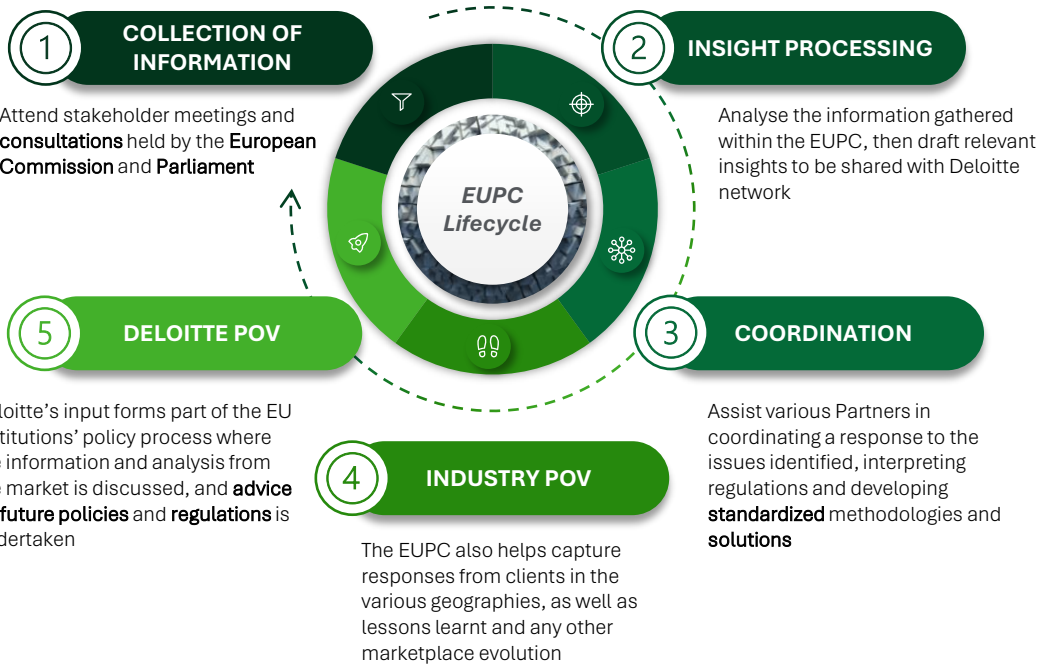
The EUPC goal is to achieve a **strategic advisor position** for **EU cyber and digital policy**, built on Deloitte’s extensive experience in various geographies and industries

EUPC ECOSYSTEM APPROACH



By leveraging relationships with different key organisations, such as governments, think-tanks, NGOs, universities and private companies in different geographic areas, the EUPC has the goal to establish a **new ecosystem** where each stakeholder can thrive

EUPC LIFECYCLE





Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex

Sections of the EUPC Digital Playbook

The EUPC Digital Playbook explores the growing complexity of EU digital and cyber legislation, showing both the new market opportunities and the regulatory challenges they bring. It also highlights where different rules connect and support each other

EU 2024-2029 Digital & Cyber Goals

The EU Commission will strengthen its competitiveness and innovation capabilities along three pillars:

CLOSING THE INNOVATION GAP WITH THE US AND CHINA

A JOINT ROADMAP FOR DECARBONISATION AND COMPETITIVENESS

INCREASING SECURITY, REDUCING EXCESSIVE DEPENDENCIES

ILLUSTRATIVE

From slide 10

Focus on EU Cyber Defence Innovation

The EU Commission pursues strategic autonomy through four goals and seven key priorities. Specifically, EU efforts in strengthening cyber defence capabilities such as innovation in cyber defence are discussed

ILLUSTRATIVE

From slide 18

EU Digital Legislation and Key Sectors Overview

The EU legislative landscape is mapped across cybersecurity, platform economy, AI & Data, Digital Finance and Digital Identity across six key sectors from Energy & Resources to Life Sciences & Healthcare

ILLUSTRATIVE

From slide 22

EU Digital Legislation Detail Cards

Through the Detail Cards, each legislation is broken down into its core components. This structure allows to quickly navigate complex regulations, understand their specific obligations, and identify potential overlaps across the legislative framework

ILLUSTRATIVE

From slide 28

Key Sectors Use Cases

Leveraging the regulatory analysis, stakeholder obligations across various sectors have been grouped into seven categories and applied to illustrative use cases to identify possible synergies and intersections

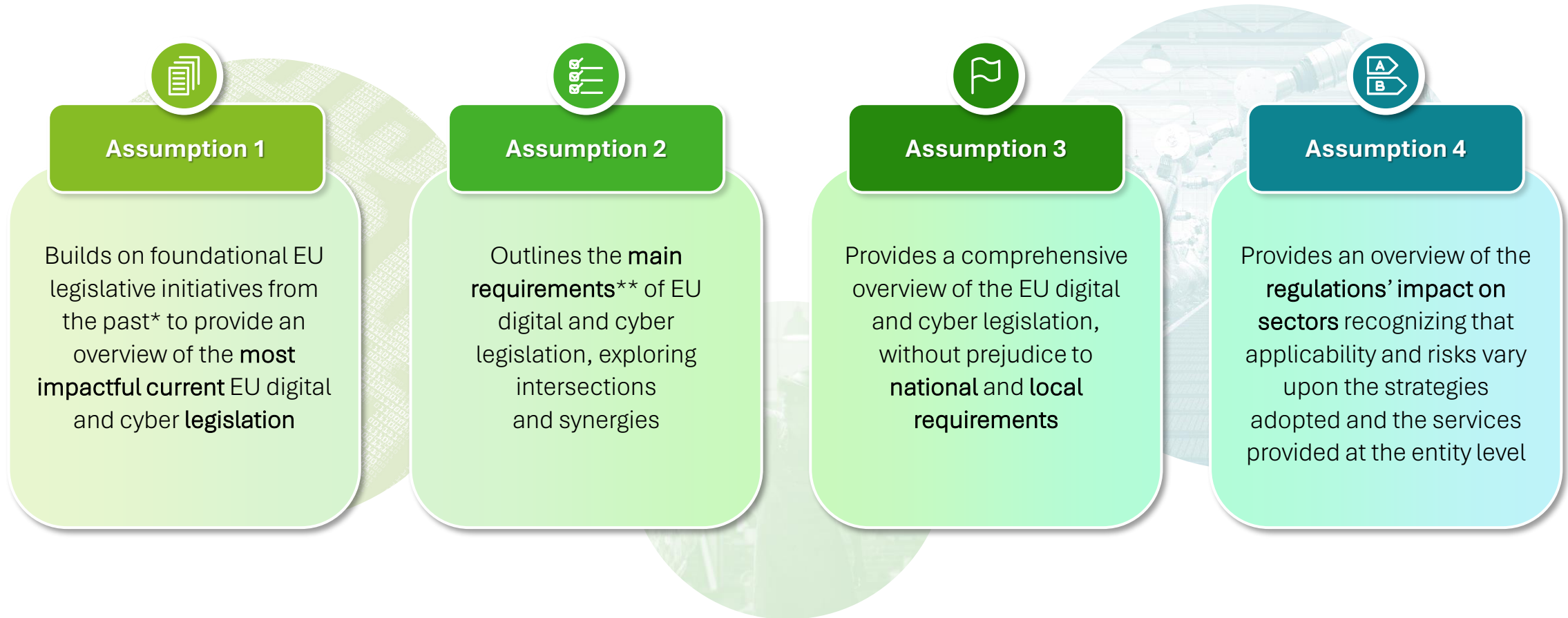
ILLUSTRATIVE

From slide 48

Assumptions of the EUPC Digital Playbook

Given the broad scope and impact of EU digital and cyber legislation, the Playbook adopts four key assumptions to define and narrow its focus

Key Assumptions



(*) For the scope of the EUPC Digital Playbook, the GDPR has been considered as a foundational element of the identified EU digital and cyber legislation

(**) The EUPC Digital Playbook offers a synthesis of the primary requirements of EU digital and cyber legislation; consequently, the wording used throughout the document is consistent with the wording used in the legislations



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex

The EU’s Role in the Evolving Digital and Geopolitical Order

Maintaining technological sovereignty and strategic influence in a rapidly evolving global tech ecosystem remains a key challenge for the EU

OVERDEPENDENCE ON NON-EU COMMS PROVIDERS



- Reliance on non-EU providers exposes EU organisations to vulnerabilities, including disruptions due to geopolitical tensions, hindering strategic autonomy
- **Example:** An American company has 7000 satellites compared with 630 for the European EUTELSAT

Solution

Investments from public and private sources, along with improved access to venture capital to boost innovation and expand strategic technologies

FALLING BEHIND OTHER REGIONS TECH DEVELOPMENT



- EU digital regulations are increasingly intertwined with international trade and policy and frameworks'
- Rapid progress in global AI infrastructure present challenges for the EU's AI Infrastructure
- Example: The EU currently contributes a modest share (7%) to global GenAI development, highlighting the need to strengthen its position in emerging digital technologies

Solution

AI Continent Action Plan is designed to bridge the growing technological divide with other regions

REGULATION & INNOVATION



- The EU’s proactive regulatory stance has historically served as a strategic tool to shape global standards and assert political influence – often referred to as the “Brussels Effect”
- Today, this regulatory strength is increasingly viewed as a double-edged sword, with concerns that it may inadvertently constrain innovation and competitiveness within the bloc
- Examples: AI Act, NIS2 Directive

Solution

Simplification and reduction of administrative burdens for EU companies

The 2024-2029 European Commission

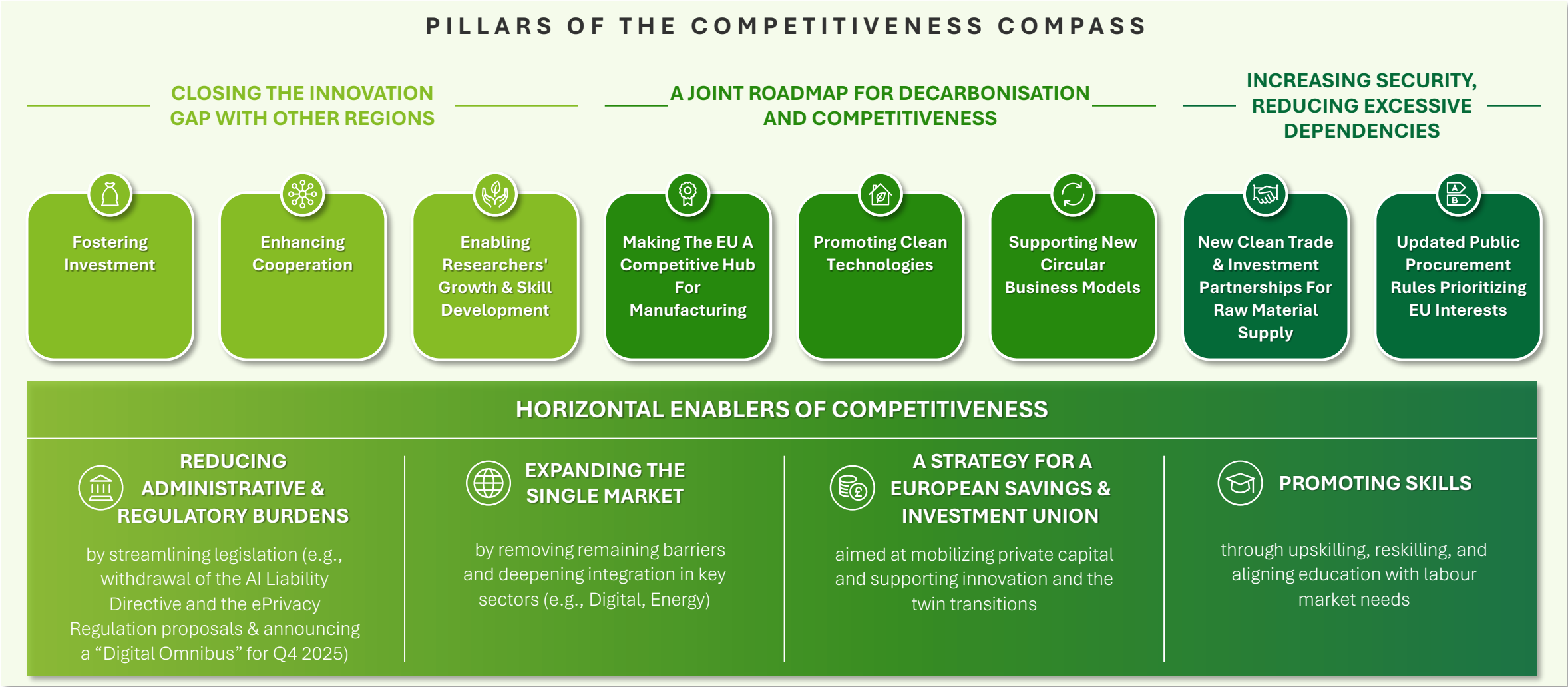
During the 2024-2029 mandate, the European Commission will focus on strengthening and harmonising its competitiveness and innovation capabilities across the Member States. While previously a standalone priority, digital transformation now spans multiple policy streams, reflecting its continued strategic importance

Goals and Key Priorities of the 2024-2029 European Commission



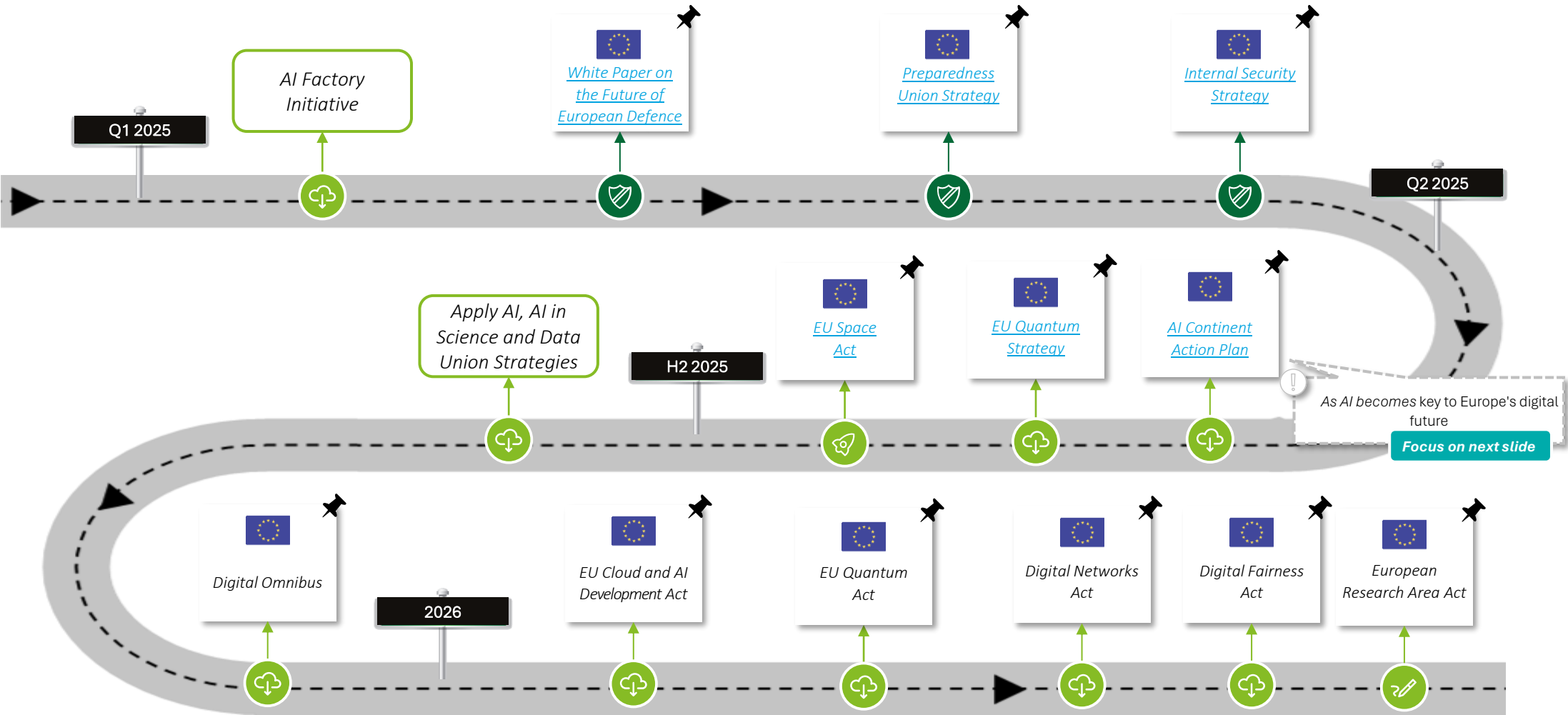
The Competitiveness Compass

Based on the Draghi & Letta reports, the European Commission has launched this initiative to streamline business, boost progress, and ensure Europe's prosperity



Cyber and Digital initiatives within the Competitiveness Compass

The following timeline provides an overview of all the key documents that currently and will continue to shape digital and cyber domains in the EU



Securing Europe’s AI Future: Urgent Investment in Infrastructure and Innovation

The EC proposes a total investment of €200 billion from public and private funding in AI and AI infrastructure, including in AI Gigafactories and generative AI applications, over the coming years in reaction to competitiveness and autonomy concerns

AI Continent Action Plan

KEY DOMAINS					KEY ACTIONS
Computing and infrastructure	Data	Skills	Promoting wide adoption	Enabling regulatory implementation	
To achieve resilient and independent EU-wide AI infrastructure, the Plan will focus on building data centres capable of running large AI models. The data centres are called: • AI Factories • AI Gigafactories	To provide more high-quality data for innovators, the Data Union Strategy (in Q3 2025) will create a genuine single market for data adapted to EU business cases. Data Labs will be embedded within AI Factories and Gigafactories to guarantee better data usage for both private and public organisations	To enforce AI skills, including basic AI literacy and diverse talent, the Plan will foster the following: • Leveraging European Digital Innovation Hubs to expand AI training and upskilling • Promoting AI literacy for all through awareness campaigns and public engagement	€700M has been allocated to incentive companies across industries to apply AI. Critically, the Plan encourages the increase of EU providers of and AI solutions for business to address strategic autonomy	Maintaining to facilitate compliance with the AI Act, particularly for smaller innovators. Companies are complaining because too complex and costly. Set up a service desk at commission for companies	▪ Startup and Scaleup Strategy – Q2 2025 ▪ AI Act Service Desk – July 2025 (launch) ▪ Apply AI Strategy – Q3 2025 ▪ Data Union Strategy – Q3 2025 ▪ Cloud and AI Development Act – Q4 2025 (proposal) ▪ Digital Omnibus Simplification Package – Q4 2025 ▪ AI in Science Strategy – Q2 2025

The 2019-2024 EU Commission: EU Cybersecurity Strategy for the Digital Decade

The EU Cybersecurity Strategy for the Digital Decade represents a cornerstone, setting out how the EU will shield its people, businesses and institutions from cyber threats, while advancing international cooperation and leading in securing a global and open Internet

EU Cybersecurity Strategy for the Digital Decade

RESILIENCE, TECHNOLOGICAL SOVEREIGNTY, AND LEADERSHIP

EU efforts to strengthen infrastructure and service resilience focus on:

 **Rules on Network and Information Systems**
increase the level of cyber resilience of all relevant sectors, public and private, essential for the economy and society

 **Building a European Cyber Shield**
through the creation of a network of SOC's across the EU under the Cyber Solidarity Act

 **Ultra-secure communication infrastructure**
to ensure the security and safety of critical missions and operations managed by the EU and its Member States

 **Securing broadband mobile networks**
through the EU 5G Toolbox, establishing a comprehensive and objective risk-based approach to 5G cybersecurity



BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER, AND RESPOND

Developing EU capabilities to prevent, deter, and respond to cyber incidents are achieved through:

 **Establishing the Joint Cyber Unit (JCU)**
serving as a virtual and physical platform for cooperation against major cross border cyber incidents and threats

 **Tackling cybercrime**
supporting the integrated approach between ENISA and Europol to ensure a coherent and effective response

 **Reinforcing EU cyber diplomacy toolbox**
further defining the EU cyber deterrence posture and updating the implementing guidelines of the toolbox

 **Boosting cyber defence capabilities**
through the review of the Cyber Defence Policy Framework to enhance cooperation between EU actors



ADVANCING A GLOBAL AND OPEN CYBERSPACE COOPERATION

Promoting European engagement and leadership in the international standardization processes is created by:

 **EU leadership in cyberspace**
stepping up its engagement in international and European standardization bodies (e.g., the ISO, the ITU)

 **Strengthening global capacities**
supporting EU partners in increasing their cyber resilience and capacities to investigate and prosecute cybercrime

 **Cooperation with partners**
strengthening and expanding its cyber dialogues and digital partnerships with third countries, regional bodies and international organisations



The 2019-2024 EU Commission: EU Digital Strategy for the Digital Decade

To ensure that digital solutions will support Europe in its pursuit of digital transformation in a way that benefits people while respecting the Union’s values, the European Commission developed the EU Digital Strategy for the Digital Decade

EU Digital Strategy for the Digital Decade

TECHNOLOGY THAT WORKS FOR THE PEOPLE

Development and deployment of technologies that impact people’s lives and respect EU values by:



Deploying innovative digital capacities

in the areas of AI, cyber, super and quantum computing, quantum communication and blockchain



Strengthening digital skills

through the Digital Education Action Plan, as well as a reinforces Skills Agenda and Youth Guarantee



Investing in the EU Gigabit connectivity

launching initiatives aimed at accelerating the roll-out of ultra-fast broadband for homes, schools and hospitals



Promoting trustworthy & ethical AI

by introducing trustworthy AI standards through the AI Act



A FAIR AND COMPETITIVE DIGITAL ECONOMY

The development of a single market fair and competitive for companies of all sizes and sectors is achieved by:



Fostering a frictionless single market

through clear and proportionate rules that are effectively and uniformly enforced across the EU



Focusing on a data-agile economy

by increasing access to high-quality data while ensuring that personal and sensitive data is safeguarded



Proposing an Industrial Strategy Package

Including actions to facilitate the transformation towards clean, circular, digital and competitive EU industries



AN OPEN, DEMOCRATIC AND SUSTAINABLE SOCIETY

A European way to digital transformation enhancing democratic values and fundamental rights through:



Developing a trustworthy digital environment

empowering citizens to take control of their data and engage confidently



Promoting an approach to digital transformation

grounded in the EU’s democratic values and fundamental rights



Supporting sustainability and climate goals

by contributing to a climate-neutral, resource-efficient digital economy





Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



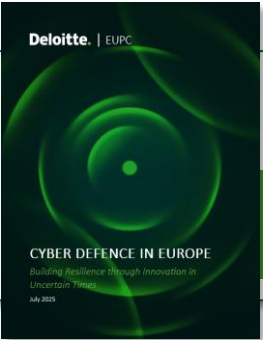
Key Sectors Use Cases



Annex

Cyber Defence in Europe: Building Resilience through Innovation in Uncertain Times

The EUPC published a paper investigating the benefits of innovation in cyber defence across four analytical perspectives – technology, policy, governance, and capabilities – and identifying best practices from the EU and its Member States



In an increasingly fragmented international landscape, defence has reemerged as a central theme in both national and international discussions – particularly in the realm of cyber defence, as nations seek to counter threats from emerging technologies and the broader cyberspace

“It is imperative for the EU to strategically direct innovation efforts towards the development of long-term EU cyber defence capabilities and the enhancement of European strategic autonomy” – Edoardo Giglio

KEY RESULTS

TECHNOLOGY

- Reduced barriers between civil and military domains require fostering dual-use innovations, specifically targeting AI and quantum technologies development
- Development of EU-native cyber defence technologies is crucial also to reduce dependencies on third-countries and enhance European strategic autonomy

POLICY

- Define a unified and coordinated innovation strategy
- Support cyber defence through harmonised legislation
- Establish a set of policy instruments that encourage the development of innovative cyber defence technologies

GOVERNANCE

- Establish a centralised governance mechanism to support cyber defence and ensure alignment among EU institutions and Member States
- Expand investment programmes
- Enhance collaboration among public and private stakeholders
- Enhance EU-NATO dialogues and EU-UK cyber dialogues to strengthen cooperation and limit redundancies

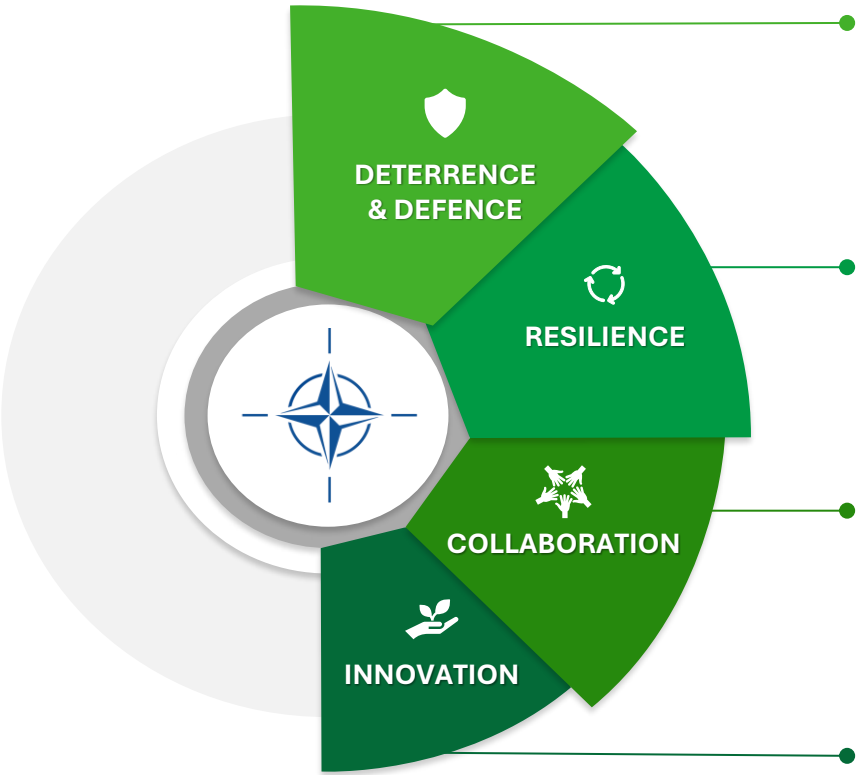
CAPABILITIES

- Integrate successful national approaches at the EU level, the EU can enhance its cyber defence while prioritising EU-sponsored initiatives over fragmented national efforts
 - Finland's robust defence and security industry network
 - Estonia's Market-Oriented Defence Innovation Driven by Industry and Supported by the Ministry of Defence
 - France's Centralized Cybersecurity and Cyber Defence Governance Model Led by the Ministry of Defence

NATO's Efforts on Cyber Defence

The geopolitical instability is prompting NATO to strengthen cyber resilience, enhance deterrence and defence capabilities, foster collaboration, and leverage civilian innovation

- A **secure cyberspace** is crucial to NATO's operations and core missions of **collective defence, crisis management, and cooperative security**
- As the indispensable **forum for transatlantic cooperation on security aspects**, NATO is determined to stay ahead of the curve by focusing on **enhancing the Allies' cyber defence capabilities** while **strengthening the Alliance resilience against cyber threats**
- In line with these efforts, in July 2021, the Allies endorsed the **NATO 2030 Agenda**, aimed at ensuring the Alliance remains **prepared, strong, and united** to face a more unpredictable and competitive world



NATO's current efforts on cyber defence

Increase in **defence spending** and **modernisation of defence capabilities** to enhance collective defence, by approving a new generation of **regional defence plans**

Development of **Alliance-wide resilience objectives** to guide **nationally-tailored resilience goals and implementation plans**, in alignment with NATO's broader posture and plans

Launch of **ad-hoc programmes** (e.g., Cyber Defence Pledge, Virtual Cyber Incident Support Capability) aimed at **enhancing Allies' cyber defences capabilities** while **strengthening national networks and infrastructures**

Launch of the **Defence Innovation Accelerator for the North Atlantic (DIANA)** to boost **cooperation on critical technologies** and **harness civilian innovation** by engaging with academia and the private sector

Challenges and Opportunities in the EU Cyber Defence Innovation Sphere

In alignment with NATO strategic objectives, the EU is focusing on addressing challenges and seizing opportunities through innovation and enhanced collaboration in the cyber defence domain

CURRENT EFFORTS

- The EU's Cybersecurity Strategy for the Digital Decade (2020) promotes cooperation among EU Member States in research and innovation, seeking synergies between civil and defence industries
- The EU Policy on Cyber Defence (2022) aims to reduce dependencies on critical cyber technologies and strengthen European Defence Technological and Industrial Base (EDTIB)
- Henna Virkkunen's Mission Letter (2024) emphasizes how Europe's digital and defence industrial can drive productivity across the region
- The report by Mario Draghi, "The Future of European Competitiveness – A Competitiveness Strategy for Europe" (2024), explores the new market opportunities of the defence industry and its role in enhancing EU competitiveness
- The EU-NATO First Structured Dialogue on Cyber (2024) builds on previous joint efforts, aimed to consolidate cyber defence coordination
- The 2025 The Hague NATO summit (2025) focuses on building defence capabilities and spending

CHALLENGES



The need to **reduce European dependency on critical cyber technologies** and **strengthen its Defence Technological and Industrial Base (EDTIB)**



The need for **investment in emerging and disruptive technologies**, while **ensuring secure systems in a post-quantum world**



The increasing **sophistication and multi-layered nature of cyber threats**, coupled with pressing need for **actionable measures to improve coordination**



The need for **specialized cyber skills for defence professionals**

OPPORTUNITIES

Technologies' dual use potential enables the joint work of cybersecurity, cyber defence, R&D, and innovation actors. **Outreach to research institutions and startups** is advised

By investing in **critical cyber technologies**, the European Defence Fund can play a role in **reducing dependencies and advance civil and military capabilities**

Focus on **technologies** like quantum computing, AI, secured cloud and post-quantum cryptography to ensure **European defence systems remain secure**

Initiatives like **Horizon Europe** can play a role in developing the **next generation of defence technologies**

Alignment of EU and focus on building defence capabilities to enhance **shared situational awareness** and **cyber defence capacity**

Commitment of NATO and EU Member States to **substantially increase expenditure** on Europe's **defence and security**, and to **invest better together**

Synergies between EU-level institutions to build **cyber defence skills** (e.g., ENISA, European Defence Agency – EDA, European Security and Defence College – ESDC)



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



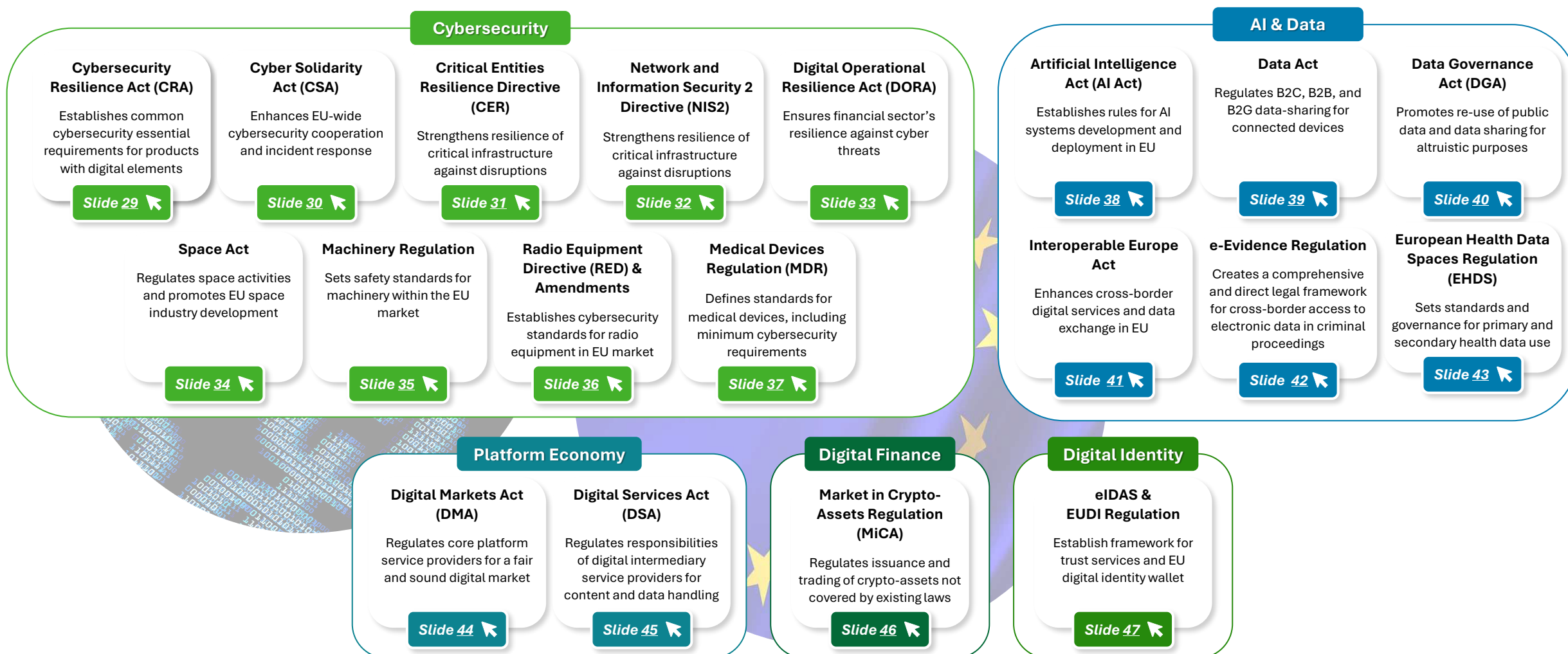
Key Sectors Use Cases



Annex

An ever-changing EU cyber and digital regulatory landscape

Over the past few years, there has been a wave of new* cyber and digital EU legislation**, requiring public and private entities to navigate a complex environment of new regulatory requirements



(*) Even though a deep dive on the GDPR is not provided in a dedicated detail card, GDPR has been considered as a foundational element of the identified EU digital and cyber legislation, and its intersections with other regulations have been considered in the key sectors' use cases

(**) As the EU cyber and digital regulatory landscape evolves, the EU Policy Centre Playbook will be updated accordingly

Key Sectors

To assess the impact of the EU digital and cyber legislation on public and private entities, the Playbook identifies different key sectors*



Energy & Resources

This sector includes public and private entities operating in the following industries: **electricity, district heating and cooling, oil, gas, hydrogen, drinking water, wastewater and waste management**



Financial Services

This sector includes financial entities such as **banking institutions** (i.e., credit institutions), **insurance companies** and **financial market infrastructures** (i.e., operators of trading venues and central counterparties, CCPs)



Life Sciences & Healthcare

This sector includes public and private entities such as **healthcare service providers**, EU reference laboratories, **research and development of medicinal products**, manufacturers of **pharmaceutical products** and **pharmaceutical preparations**



Manufacturing & Consumer

This sector includes private entities operating in the following industries: **manufacturing of medical devices, computer, electronic and optical products, electrical equipment, machinery, motor vehicles, trailers and semi-trailers, other transportation equipment, manufacturing of consumer products**



Technology, Media & Telecommunications

This sector includes public and private entities operating in the following industries: **digital infrastructure services, ICT service management, intermediary services, core platform services, qualified / non-qualified trust services, telecommunications, network connectivity**

Use Cases

For each sector identified by the Playbook, illustrative use cases have been developed to support readers understand potential applications of the identified EU legislation

Illustrative entities subject to EU digital legislation for each sector



**Energy &
Resources**



**Financial
Services**



**Life Sciences &
Healthcare**



**Manufacturing &
Consumer**



**Technology, Media &
Telecommunications**

**Transmission System
Operator**

Slide 50 ➤

**Health Insurance
Provider**

Slide 55 ➤

**Medical Imaging
Equipment
Manufacturer**

Slide 60 ➤

**Automotive Supplier of
Smart and/or Data-
driven Aftermarket
Components**

Slide 65 ➤

**Augmented Reality (AR)
and Virtual Reality (VR)
Headsets Manufacturer**

Slide 70 ➤

**Cloud Computing
Service Provider**

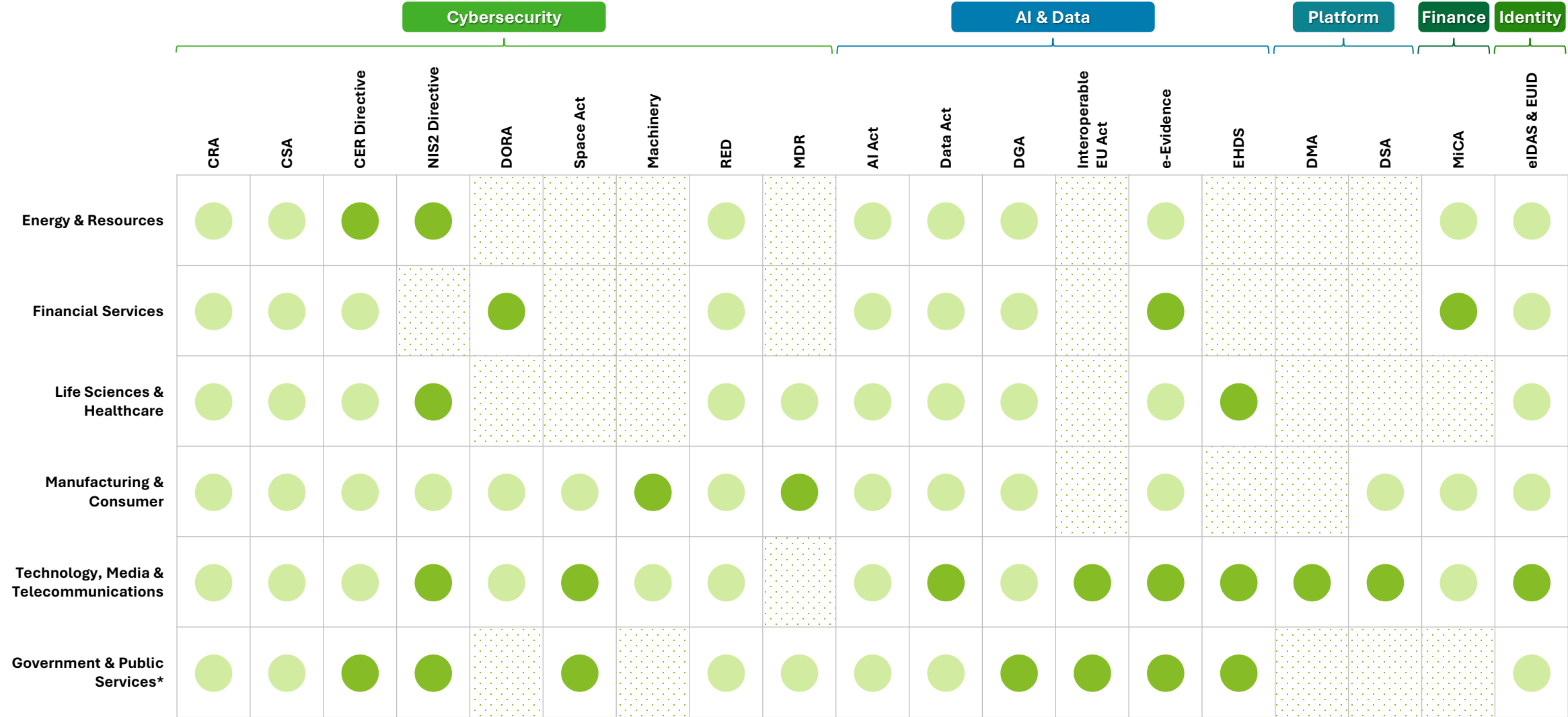
Slide 75 ➤

**Operator of Ground-
based Infrastructure
supporting the provision
of Space-based Services**

Slide 80 ➤

EU Digital legislation impact on key sectors

Below a high-level representation of the impact of the analysed EU cyber and digital legislation across sectors



Entity specificities driving the applicability of the EU digital and cyber legislation

As today's businesses are highly complex, the impact of EU digital and cyber legislation shall be evaluated from an entity perspective, taking into account the specific strategies and services of each entity, rather than focusing solely on the broader sector



Same sector, different strategies



Sector: Consumers



Sub-sector: Retail, Wholesale & Distribution



Company 1: Part of the clothing industry, Company 1 is expanding its presence in the **Metaverse** to promote its products and strengthen its position in the digital domain



Company 2: Part of the large organised distribution industry, Company 2 heavily relies on **IoT devices** and **robots** to speed up and improve production



Depending on their **strategies** towards the digital domain and digital products, Companies 1 and 2 might be subject to **different regulations**, and might be exposed to compliance **risks** that do not always **affect** their sector



Same sector, different services



Sector: Technology, Media & Telecommunications (TMT)



Sub-sector: Telecommunications, Media & Entertainment



Company 1: A network provider has a banking license to offer full **banking services** to its customers, acting as a banking institution



Company 2: A network provider focuses exclusively on core telecom business and **does not** have a banking license, providing potential financial services through partner banks



Due to the different scope of the **services** provided, Company 1 has to comply with **DORA** requirements as a **banking institution**, while Company 2 does not. Regulatory compliance and consequent risks **differ** despite the two Companies being the same type of entity



*The impact of the EU digital and cyber legislation on clients should always be considered on a **case-by-case basis***



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex

Cyber Resilience Act (CRA)

CRA aims to strengthen cybersecurity rules to ensure more secure hardware and software products. In particular, CRA creates the conditions for the development of secure products with digital elements by ensuring that manufacturers take security seriously throughout a product’s lifecycle

Description

- The CRA:
- Imposes obligations upon economic operators to ensure that cybersecurity is taken into account throughout the **entire supply chain** and **lifecycle** of products that are connected either directly or indirectly to another device or to a network, namely **products with digital elements**
 - Identifies essential requirements for the design, development and production of **products with digital elements**, and obligations for economic operators in relation to those products with respect to cybersecurity
 - Introduces essential cybersecurity requirements for the **vulnerability handling processes** put in place by **manufacturers** to ensure the security of products with digital elements throughout their lifecycle
 - Sets rules on **market surveillance**, including monitoring, and enforcement of the rules and requirements.

In order to establish a clear and coherent framework for the cybersecurity of products with digital elements and facilitate compliance by economic operators with CRA requirements, the **EU Commission**, the **European Standardization Organisations (ESOs)** and **ENISA** are working on **defining a set of harmonized security standards** mapped upon the essential product and incident handling process specified in the Regulation

Applicable key sectors

- | | |
|--|---|
|  Energy & Resources |  Manufacturing & Consumer |
|  Financial Services |  Technology, Media & Telecommunications |
|  Life Sciences & Healthcare |  Government & Public Services |

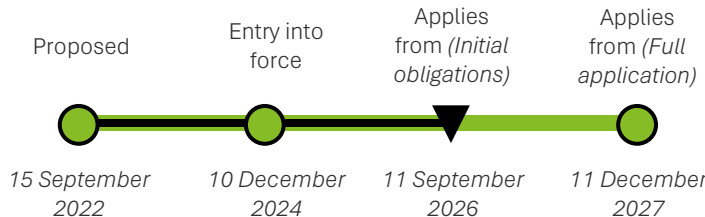
This Regulation applies to:

- | | |
|--|--|
| <ul style="list-style-type: none"> Manufacturers (or entities that market under their name products with digital elements manufactured by others) Authorized representatives of manufacturers Importers | <ul style="list-style-type: none"> Distributors of products with digital elements Any other natural or legal person who is subject to obligations laid down by CRA |
|--|--|

- Intersection with other EU law:**
- | | |
|--|--|
| <ul style="list-style-type: none"> AI Act Cybersecurity Act Decision 768/2008/EC EHDS Machinery Regulation New Legislative Framework (NLF) | <ul style="list-style-type: none"> NIS2 RED and amendments Regulation (EU) 2017/745 Regulation (EU) 2017/746 Regulation (EU) 2019/2144 Space Act |
|--|--|

- Regulatory Stakeholders:**
- | | |
|--|--|
| <ul style="list-style-type: none"> European Commission European Standardization Organisations ENISA | <ul style="list-style-type: none"> National cybersecurity certification authorities National CSIRTs Market surveillance authority |
|--|--|

Timeline



Cyber Solidarity Act (CSA)

CSA aims to strengthen common EU detection, situational awareness, and response capabilities, to gradually build an EU-level cybersecurity reserve with services from trusted private providers, and to support testing of critical entities

Description

Cyber Solidarity Act aims to **support detection** and **awareness** of **significant** or **large-scale cybersecurity threats** and **incidents**, bolster **preparedness** and protect **entities** operating in **sectors of high criticality** or **other critical sectors**, such as hospital and public utilities. Further, it aims to strengthen solidarity at EU level, **concerted crisis management** and **response capabilities** across Member States, and contribute to ensuring a **safe** and **secure digital landscape** for citizens and businesses.

The objectives of the EU Cyber Solidarity Act will be implemented through the following actions:

- Deployment of a pan-European infrastructure of **National Cyber Hubs (European Cybersecurity Alert System)** to build and enhance **common detection** and **situational awareness capabilities**
- Creation of a **Cyber Emergency Mechanism** to support Member States in preparing for, responding to and immediate recovery from **significant** and **large-scale cybersecurity incidents**. Support for incident response shall also be made available to European institutions, bodies, offices and agencies of the Union (EUIBAs)
- Establishment of a **European Cybersecurity Incident Review Mechanism** to review and assess **specific significant** or **large-scale incidents**

Applicable key sectors


Energy & Resources


Manufacturing & Consumer


Financial Services


Technology, Media & Telecommunications


Life Sciences & Healthcare


Government & Public Services

This Regulation applies to:

- *Users (i.e., Member States, cyber crisis management authorities, CSIRTs, CERT-EU Union institutions, bodies and agencies, Competent authorities such as Computer Security Incident Response Teams and cyber crisis management authorities of DEP-associated third countries)*
- *Entities operating in sectors of high criticality*
- *Trusted providers*

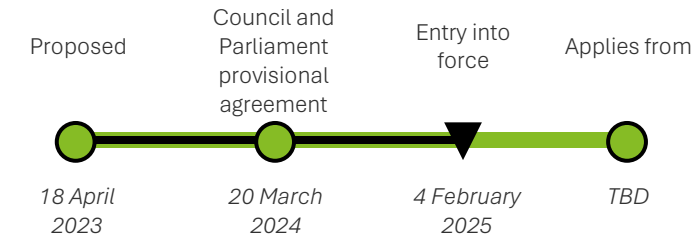
Intersection with other EU law:

- *NIS2 Directive*
- *Cybersecurity Act*
- *Regulation (EU) 2021/694 (eIDAS)*

Regulatory Stakeholders:

- *European Commission*
- *ENISA*
- *NIS Cooperation Group*
- *CSIRTs’ competent authority*

Timeline



Critical Entities Resilience Directive (CER Directive)

The Critical Entities Resilience Directive (CER Directive) enhances the resilience of critical entities to ensure the continuous provision of essential services across the EU, imposing obligations on Member States and promoting cooperation and information sharing

Description

The CER Directive aims to create a robust framework for the resilience of critical entities, ensuring the continuous provision of essential services across the EU and enhancing the overall security and stability of the internal market

In particular, the CER Directive:

- Mandates Member States to adopt resilience strategies by 17 January 2026, including strategic objectives, governance frameworks, and risk assessments
- Imposes obligations on Member States to identify and support critical entities in enhancing their resilience
- Requires critical entities to implement measures to prevent, protect against, respond to, and recover from incidents, including physical protection, risk management, and business continuity plans
- Establishes rules for supervision, enforcement, and advisory missions to assess compliance, including on-site inspections, audits, and penalties for non-compliance
- Promotes cooperation and information sharing among Member States and the Commission through the Critical Entities Resilience Group
- Ensures coordinated implementation with Directive (EU) 2022/2555, linking physical security and cybersecurity
- Encourages the use of European and international standards for security and resilience measures

Applicable key sectors



Energy & Resources



Manufacturing & Consumer



Financial Services



Technology, Media & Telecommunications



Life Sciences & Healthcare



Government & Public Services

This Regulation applies to:

- *Public and private entities identified by Member States as critical entities, which provide essential services crucial for maintaining vital societal functions, economic activities, public health activities and safety or operating critical infrastructure for these essential services*
- *Significant critical entities which provide essential services in six or more Member States*

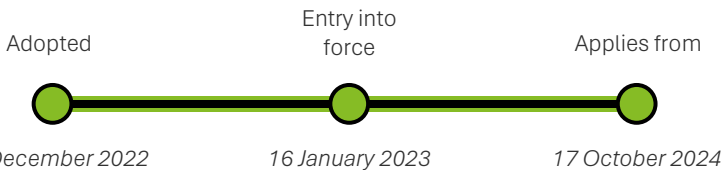
Intersection with other EU law:

- *Directive (EU) 2022/2555 (NIS2)*
- *Regulation (EU) 2022/2554 (DORA)*
- *Regulation (EU) 2016/679 (GDPR)*
- *Directive (EU) 2016/680 (LED)*

Regulatory Stakeholders:

- *European Commission*
- *Critical Entities Resilience Group*
- *Member States*
- *Single Points of Contacts*

Timeline



Network and Information Security Directive 2 (NIS2 Directive)

In response to the growing threats posed by digitization and the resulting increase in cyber-attacks, the EU’s co-legislators adopted measures to ensure a high level of cybersecurity across the Union by strengthening security requirements for entities operating in “highly critical” and “critical” sectors

Description

Directive NIS2 aims to address shortcomings of the previous NIS Directive and subsequent implementation at the national level. In this regard, Directive NIS2 adopts a **clear size-cap rule** for the identification of public and private entities falling within the scope of its provision. On such basis, the Directive further distinguishes between “**essential**” and “**important**” entities depending on both the size and sector in which they operate, imposing different sets of obligations accordingly.

More specifically, to comply with NIS2, Member States:

- Shall ensure the **management bodies of covered entities approve all the necessary measures to comply with cybersecurity risk management obligations**, oversee its implementation and can be held liable for infringements by the entities
- Shall ensure that **entities** within the scope of the Directive **design, approve and implement risk management frameworks**, namely all appropriate and proportionate technical, operational and organisational measures to manage information and ICT risks, and to minimise the impact of incidents
- Shall ensure that **entities** within the scope of the Directive **notify national CSIRTs** of any incident that has a significant impact on the provision of their services
- May require entities within the scope of the Directive to **use certain ICT products, services and processes** that are **certified** under a scheme adopted pursuant to the Cybersecurity Act

Applicable key sectors



Energy & Resources



Financial Services



Life Sciences & Healthcare



Manufacturing & Consumer



Technology, Media & Telecommunications



Government & Public Services

This Directive applies to:

- Public or private entities operating in “Highly critical” or “Critical” sectors (e.g., energy, transportation, health) qualified as “medium” or “large” enterprises under Recommendation 2003/361/EC
- Providers of public electronic communications networks or of publicly available electronic Communications services
- Trust service providers
- Top-level domain name registries and domain name system service providers
- Providers of domain name registration services
- Public administration entities of central government
- Public administration entities at local level (discretionary)
- Educational institutions (discretionary)

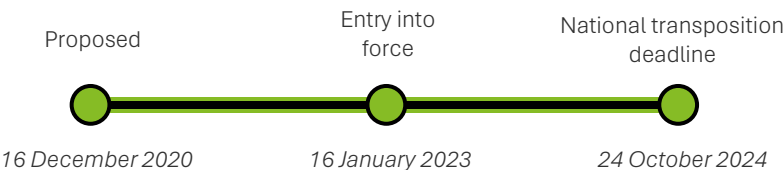
Intersection with other EU law:

- CRA
- Cybersecurity Act
- DORA
- Directive 2022/2557/EU (CER)
- Directives 2002/58/EC, 2011/93/EU and 2013/40/EU

Regulatory Stakeholders:

- ENISA
- NIS Cooperation Group
- National supervisory authorities
- National CSIRTs

Timeline



Digital Operational Resilience Act (DORA)

DORA is the EU's digital operational resilience and cybersecurity regulation for the financial sector and aims to transform financial players' ICT risk management processes to increase their resilience to major security incidents

Description

DORA impacts **financial players** by requiring the **transformation of governance** (top management, control functions, operational functions, business), a revision of the **operating model**, and the definition of a new **strategic risk management** approach.

Financial entities are required to build capabilities against relevant risk scenarios by identifying **critical functions/services**, mapping their **value chain** and defining “**acceptable**” risk levels to be monitored on an ongoing basis.

DORA is structured in 5 pillars:

- ICT risk management
- ICT incident management
- Digital operational resilience testing
- ICT third party risk management
- Threat intelligence and information sharing.

Top management plays a central role in defining, approving, overseeing, and being **accountable** for the implementation of a solid and documented **ICT risk management framework**, as well as a **digital operational resilience strategy** outlining how all security policies, procedures, tools and methods will be applied in practice, including the identification of the ICT risk tolerance within the overall risk appetite of the entity.

Financial Entities, other than micro-enterprises, shall assign responsibility for ICT risk management and oversight to an **independent** control function

Applicable key sectors



- This Regulation applies to:**
- Credit and payment institutions
 - Insurance, reinsurance companies and intermediaries
 - Account information service providers
 - Electronic money institutions
 - Investment enterprises
 - service providers for cryptocurrencies
 - Central securities depositories
 - Central counterparties
 - Trading venues and trade repositories
 - Alternative investment fund managers
 - Management company
 - Data communications service providers
 - Occupational pension institutions
 - Credit rating agencies
 - Critical benchmark index administrators
 - Crowdfunding service providers
 - Securitization data repositories third-party ICT service providers

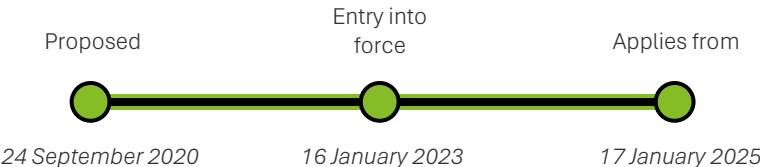
Intersection with other EU law:

- CRA
- NIS2 Directive

Regulatory Stakeholders:

- European Commission
- European Central Bank
- European Banking Authority
- European Insurance and Occupational Pensions Authority
- European Securities and Markets Authority
- National supervisory authorities

Timeline



Space Act

The EU Space Act is a legislative initiative by the European Commission that introduces a harmonised framework for space activities across the Union. The proposal, published on 25 June 2025, aims to ensure safety, resilience, and environmental sustainability, while boosting the competitiveness of the EU space sector

Description

The European Commission has identified the EU Space Act as a key priority, as outlined in the Draghi and Letta reports, and in the Competitiveness Compass and related work programme for 2025.

The proposed Regulation lays down rules for the establishment and functioning of the internal market of space-based data and space services and is structured around **three key pillars**:

- 1. Safety:** The Act introduces robust rules for tracking space objects and mitigating space debris, preserving Europe’s secure and uninterrupted access to space
- 2. Resilience:** Tailored cybersecurity requirements will strengthen protection of European space infrastructure and ensure business continuity
- 3. Sustainability:** Operators will need to assess and reduce the environmental impact of their space activities, while benefiting from support for innovation in emerging technologies like in-orbit servicing and debris removal.

The new rules will apply to both EU and non-EU operators providing space services in Europe. Proportional requirements will be scaled based on company size and risk profile, ensuring a fair, innovation-friendly regulatory environment.

Finally, a targeted support package will help businesses and Member States transition smoothly. Special attention is given to reducing administrative burdens and facilitating compliance, especially for start-ups, SMEs and small mid-caps.

Applicable key sectors



Energy & Resources



Manufacturing & Consumer



Financial Services



Technology, Media & Telecommunications



Life Sciences & Healthcare



Government & Public Services

This Regulation applies to:

- Space operators
- Collision avoidance space services providers
- Primary providers of space-based data
- International organisations providing in the Union space services or space-based data generated by space objects placed on an orbit not further than GEO and operated by

such international organisations

Intersection with other EU

law:

- NIS2 Directive
- CRA
- CER Directive
- Decision 676/2002/EU
- Directive (EU) 2018/1972
- Decision no 243/2012/EU

Regulatory Stakeholders:

- European Commission
- European Union Agency for the Union Space Programme
- European Space Agency (ESA)
- National Competent Authority
- National Qualified Technical Body for Space Activities

Timeline



Machinery Regulation

The Machinery Regulation sets a modernized legal framework for safe, sustainable and compliant machinery in the EU market, reflecting technological evolution

Description

Regulation (EU) 2023/1230, adopted on 14 June 2023, replaces Directive 2006/42/EC and sets **out essential health and safety requirements for the design, construction, and placing on the market of machinery and related products** (e.g. safety components, lifting accessories, interchangeable equipment, etc.). It aims to ensure safety, technological adaptability (including AI and digital documentation), and the free circulation of compliant machinery within the internal market.

More specifically, the Regulation proposes:

- **Increased legal certainty**, through uniform application
- Integrated provisions for **machinery with safety functions** that are **AI-powered**
- Integrated provisions for **cyber-safety** for **compliance**-relevant software data and safety control systems
- A **conformity assessment** of machinery presenting a higher risk factor
- Updated **product category-specific provisions**
- Conditions under which the instructions for use and the declaration of conformity can be provided in a digital format

Applicable key sectors



Energy & Resources



Financial Services



Life Sciences & Healthcare



Manufacturing & Consumer



Technology, Media & Telecommunications



Government & Public Services

This Regulation applies to:

- *Manufacturers (or entities that market under their name machinery and related products manufactured by others)*
- *Any other natural or legal person who is subject to obligations laid down by Machinery Regulation*
- *Authorized representatives of manufacturers*
- *Importers*
- *Distributors*

Intersection with other EU law:

- Directive (EU) 2014/35
- Directive (EU) 2014/53
- Regulation (EU) 2013/167
- Regulation (EU) 2013/168
- Regulation (EU) 2018/858
- Regulation (EU) 2018/1139
- Regulation (EU) 2019/881
- Regulation (EU) 2019/1020

Regulatory Stakeholders:

- *European Commission*
- *National Competent Authorities*
- *Notified Bodies*
- *Standardization bodies*
- *Economic operators (e.g., manufacturers, importers, distributors)*

Timeline



Radio Equipment Directive (RED) and amendments on “common charging” solution

The Radio Equipment Directive 2014/53/EU (RED) establishes a regulatory framework for the placing on the market of radio equipment. On November 2022 and June 2023, the Commission has published two amendments to the RED, also introducing a “common charging” solution to promote the use of common chargers for mobile phones and other portable electronic devices

Description

RED ensures a single market for **radio equipment** by setting essential **requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum**.

Among those, RED introduces specific requirements related to the use of **network resources, the protection of personal of users’ personal data and privacy**, as well as the integration of **anti-fraud features** (Article 3, par. 3), letters d), e) and f).

In 2022, the EU Commission adopted **Delegated Regulation (EU) 2022/30**, further specifying **cybersecurity requirements** under Art. 3(3) of RED for wireless devices. **Economic operators shall take into account such requirements while designing and Manufacturing & Consumer covered products.**

Recently, **RED has been amended** by Directive (EU) 2022/2380 which defines requirements for a “**common charging**” solution. In addition, Commission Delegated Regulation (EU) 2023/1717 updates the references to the **technical specifications** for wired charging. These requirements will apply to all handheld mobile phones, tablets, digital cameras, headphones, headsets, portable speakers, handheld videogame consoles, e-readers, earbuds, keyboards, mice, and portable navigation systems.

Applicable key sectors

- | | |
|--|---|
|  Energy & Resources |  Manufacturing & Consumer |
|  Financial Services |  Technology, Media & Telecommunications |
|  Life Sciences & Healthcare |  Government & Public Services |

This Directive applies to:

- Manufacturers (or entities that market under their name radio equipment manufactured by others)
- Importers
- Distributors of radio equipment
- Authorised representatives of manufacturers

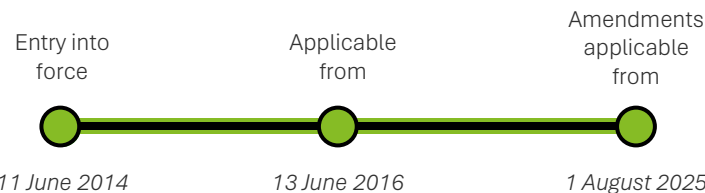
Intersection with other EU law:

- Cyber Resilience Act
- Decision No 676/2002/EC
- Directive 98/34/EC
- Directive 2002/21/EC
- Directive 2014/35/EU
- Directive 2014/30/EU
- Regulation (EC) No 765/2008
- Regulation (EU) No 182/2011
- Regulation (EU) No 1025/2012

Regulatory Stakeholders:

- European Commission
- Telecommunication Conformity Assessment and Market Surveillance Committee
- Notified bodies
- Market surveillance authorities
- Spectrum authorities

Timeline



Medical Devices Regulation (MDR) and Guidance on Cybersecurity for medical devices

The MDR aims to set standards of quality and safety for medical devices, including minimum cybersecurity requirements for hardware, IT network characteristics and IT security measures. These requirements are thoroughly specified in the “Guidance on Cybersecurity for medical devices”

Description

Regulation EU/2017/745 (MDR) sets high **quality and safety standards for medical devices** to address common safety concerns and ensure the smooth functioning of the internal market for medical devices. The Regulation applies to “**medical devices**”, namely any **instrument, apparatus, appliance, and software intended to be used for human beings for medical purposes**, such as the diagnosis, prevention, monitoring, prediction and treatment of diseases.

With regard to cybersecurity, the Regulation requires medical device manufacturers to set out **minimum requirements** for hardware, IT network characteristics, **and IT security measures**, including protection against unauthorised access, necessary for the intended use of software.

With specific regard to devices incorporating software (or software considered as devices in itself), the Regulation provides that the **software shall be developed and manufactured in accordance with the state of the art**, taking into account **SDLC principles, risk management, verification and validation**.

In addition to the general provisions of the Regulation, the cybersecurity **requirements** for medical devices **are thoroughly specified in the “Guidance on Cybersecurity for medical devices”**, drafted by the Medical Device Coordination Group established by the MDR

Applicable key sectors

**Energy & Resources**

**Financial Services**

**Life Sciences & Healthcare**

**Manufacturing & Consumer**

**Technology, Media & Telecommunications**

**Government & Public Services**

This Regulation applies to:

- Manufacturers of medical devices

Intersection with other EU law:

- AI Act
- NIS2 Directive and Cyber Resilience Act
- Machinery Directive

Regulatory Stakeholders:

- European Commission
 - Medical Device Coordination Group
- National competent authorities

Timeline



Artificial Intelligence Act (AI Act)

The AI Act aims to strengthen the safety and trustworthiness of artificial intelligence (AI) and to promote the deployment of AI systems in the EU. Its goal is to create an environment in which the opportunities of AI can be safely harnessed, while adequately safeguarding the fundamental rights of individuals and promoting a sound and competitive market

Description

The AI Act sets out rules for **developers, deployers and users of AI systems** with the aim to **drive innovation** as well as to **safeguard fundamental rights** of individuals from the risks posed by AI systems.

The Regulation distinguishes between i) prohibited AI practices, ii) high-risk AI systems, iii) general-purpose AI models, and iv) other basic AI systems. It then sets out different obligations depending on the subjective scope and type of AI system or model. With regard to **high-risk AI systems**, the AI Act requires for example:

- Adoption of a comprehensive **AI risk management framework**, including ex-ante testing of the system as well as post-market monitoring
- Draft of **technical documentation** before the system is placed on the market or put into service
- Design of **accurate, robust and (cyber)secure systems**, ensuring human oversight, and the adoption and ongoing updating of internal policies, procedures and instructions.

Failure to comply with:

- The prohibition of AI practices (Art. 5) can lead to **a fine** of up to €35M or 7% of the company's total annual worldwide turnover
- Specific obligations imposed upon providers, importers distributors or deployers can lead to **a fine** up to 15M or up to 3% of the company's total worldwide annual turnover

Applicable key sectors



Energy & Resources



Manufacturing & Consumer



Financial Services



Technology, Media & Telecommunications



Life Sciences & Healthcare



Government & Public Services

This Regulation applies to:

- *Providers*
- *Deployers*
- *Importers*
- *Distributors*

Intersection with other EU law:

- *CRA*
- *Cybersecurity Act*
- *Regulation (EU) 2019/1020 on market surveillance and compliance of products*
- *Directive 2013/36/EU*
- *on access to the activity of credit institutions*
- *Medical Devices Regulation (MDR)*

Regulatory Stakeholders:

- *AI Office (within the European Commission)*
- *European Artificial Intelligence Board*
- *National Competent Authorities (at least one notifying authority and one market surveillance authority)*

Timeline



Data Act

The Data Act aims to improve individuals' and businesses' access to data in the EU market, especially regarding the Internet of Things (IoT) domain. The act encourages access to data while ensuring fair access and users' rights regarding data sharing, storage, and processing

Description

As a horizontal legislation, the Data Act aims to increase **legal certainty and safeguards** by introducing specific obligations in the context of **B2C, B2B, and B2G data-sharing agreements**. In particular, the Data Act **regulates** the **sharing of “product data”**, namely data generated by connected devices (e.g., IoT devices), for commercial purposes.

It introduces a set of measures aimed at:

- Clearly defining **acceptable uses of data** and the associated terms, while also maintaining incentives for data holders to **invest in high-quality data generation**
- Reducing the abuse of **contractual imbalances** that impede equitable data-sharing, **to avoid unjust contractual terms** imposed by a party with a considerably stronger market position
- Establishing **rules** that allow **public sector bodies to access and use data** held by the private sector for specific public interest purposes
- Defining **rules** that set the **framework for customers** to effectively switch between different providers of data-processing services to facilitate interoperability and unlock the EU cloud market

For the purpose of supporting the negotiation of fair data-sharing agreements, the **EU Commission will develop non-binding model contract clauses**

Applicable key sectors



This Regulation applies to:

- Data holders*
- Data recipients*
- Users*
- Cloud-service providers*

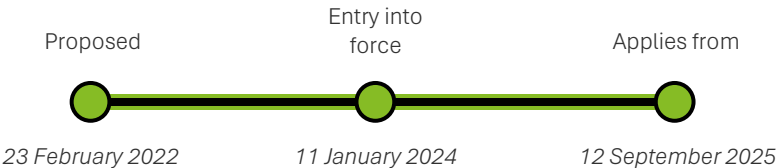
Intersection with other EU law:

- Database Directive*
- DGA*
- EHDS*
- GDPR*

Regulatory Stakeholders:

- European Commission*
- European Data Protection Supervisor*
- European Data Innovation Board*
- National Competent Authorities*

Timeline



Data Governance Act (DGA)

The European Strategy for Data recognises data as a critical component of the EU economy and promotes the creation of a single market where data can move safely to foster growth and digital transformation. In this context, the Data Governance Act regulates the re-use and sharing of data to safeguard citizens’ trust

Description

The DGA is a cross-sectoral regulation that covers the **re-use of publicly held data** (both personal and non-personal), promotes data sharing through providers of data intermediation services (such as data marketplaces), and encourages **data sharing** for altruistic purposes. Data intermediaries will act as neutral third parties connecting data holders with data users.

The DGA sets out:

- Conditions under which **public authorities** may allow the re-use of data that are subject to the rights of others
- A **notification and supervisory framework** for data intermediation service providers
- A **framework for the voluntary registration** of entities collecting and processing data made available for altruistic purposes;
- A **framework for the establishment of the European Data Innovation Board** (EDIB)

Data intermediation service providers shall not use data for their own purposes and shall be free from any conflict of interest. For this purpose, the Commission has recently adopted an implementing regulation on the **design of common logos** to identify data intermediation service providers and data altruism organisations. In addition, data intermediation services providers shall not use data that they intermediate for financial purposes

Applicable key sectors


Energy & Resources


Manufacturing & Consumer


Financial Services


Technology, Media & Telecommunications


Life Sciences & Healthcare


Government & Public Services

This Regulation applies to:

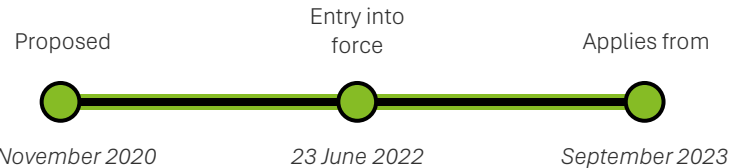
- Data Intermediation Services Providers (DISPs)
- Data Brokering Services Providers
- Registered Data Altruism Organisations

- Intersection with other EU law:**
- Directive (EU) 2019/1024
 - DMA
 - GDPR
 - Directive 2000/31/EC
 - Directive 2001/29/EC
 - Directive 2004/48/EC
 - Directive 2007/2/EC
 - Directive 2010/40/EU
 - Directive (EU) 2015/849
 - Directive (EU) 2016/943
 - Directive (EU) 2017/1132
 - Directive (EU) 2019/790
 - Regulation (EC) No 223/2009
 - Regulation (EU) 2018/858
 - Regulation (EU) 2018/1807

Regulatory Stakeholders:

- European Commission
- European Data Innovation Board
- National Competent Authorities

Timeline



Interoperable Europe Act

The Interoperable Europe Act sets out the framework for advancing trans-European digital public services and ensuring the cross-border interoperability of the network and information systems used to provide or manage public services across the EU

Description

The 2030 Digital Compass outlined the importance of ensuring interoperability across all levels of government and public services, through the establishment of a strong and strategic interoperability policy. To this end, on 13 March 2024 the European Parliament and the Council of the European Union adopted the Interoperability Europe Act, with the purpose of **strengthening the European market** by promoting **cross-border interoperability of trans-European digital public services**.

To achieve this goal, the Regulation proposes:

- A **structured and co-owned EU cooperation** on interoperability that brings together public administrations, supported by public and private actors
- The execution of **mandatory interoperability assessments in relation to binding requirements** before taking a decision on new or substantially modified binding requirements, aiming to discover legal, organisational, semantic and technical barriers to cross-border interoperability
- The **share and reuse of interoperability solutions** among public sector bodies, powered by a one-stop-shop for solutions and community platform, the “Interoperable Europe Portal”
- **Interoperability enablers and support measures**, including the European Interoperability Framework, regulatory sandboxes and GovTech incubators, as well as training and capacity-building programmes, to promote policy experimentation, skills development and the reuse of interoperability solutions

Applicable key sectors



Energy & Resources



Manufacturing & Consumer



Financial Services



Technology, Media & Telecommunications



Life Sciences & Healthcare



Government & Public Services

This Regulation applies to:

- *Union entities and public sector bodies that regulate, provide, manage or implement trans-European digital public services*
- *Private stakeholders and service providers who collaborate with public administrations*
- *Civil society organisations, research institutions, and GovTech startups that contribute to innovation in public service delivery*

Intersection with other EU law:

- GDPR 182/2011
- Regulation (EU) 2018/1725
- Directive (EU) 2016/680
- Regulation (EU) 2016/679
- Regulation (EU) No 1025/2012

Regulatory Stakeholders:

- *European Commission*
- *European Economic and Social Committee*
- *European Committee of the Regions*
- *National digital transformation authorities*
- *Government Chief Information Officers*

Timeline



e-Evidence Regulation

The e-Evidence Regulation package aims to streamline the process of accessing electronic evidence across EU Member States. It applies to a broad range of electronic service providers offering services within the EU, including cloud services, social media platforms, and email providers

Description

The e-Evidence package, consisting of a Regulation and a Directive, will make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals.

The package will establish:

- **European Preservation Orders (EPO)**, which is a legal instrument that allows judicial authorities to directly request electronic evidence from service providers in another EU country
- **European Preservation Order (EPO-PR)**, which is a legal instrument designed to ensure that electronic evidence is preserved while a European Production Order is being processed ensuring it cannot be deleted or altered
- **Decentralised IT-systems** through which all communication between authorities and service providers can take place in a secure and reliable way, ensuring authentication of all participants
- **Legal representatives** to be designated by service providers within the EU for receiving orders.

The new rules will enter into force on 17 August 2023 and will apply as of 17 February for the Directive and 17 August 2026 for the Regulation

Applicable key sectors



Energy & Resources



Manufacturing & Consumer



Financial Services



Technology, Media & Telecommunications



Life Sciences & Healthcare



Government & Public Services

This Regulation applies to:

- *Service providers which offer services in the Union*

Intersection with other EU law:

- GDPR
- Directive (EU) 2016/680
- Directive 2014/41/EU
- Directive 2002/58/EC
- Directive (EU) 2018/1972
- Directive (EU) 2015/1535
- Directive (EU) 2017/541
- Directive 2011/93/EU
- Directive (EU) 2019/713
- Directive 2013/40/EU

Regulatory Stakeholders:

- *European Commission*
- *Council of the European Union*
- *European Judicial Network (EJN)*
- *Eurojust*
- *European Data*
- *Protection Supervisor*
- *National Issuing Authority*
- *National Enforcing Authority*
- *National Competent Courts*
- *National Central Authorities*

Timeline



European Health Data Space Regulation (EHDS)

The proposed Regulation aims to establish the European Health Data Space to support individuals in taking control of their own health data, to support the use of health data to improve healthcare delivery, research, innovation and policy making, and to enable the EU to unlock the potential of a safe and secure exchange, use and reuse of health data

Description

The proposed Regulation EHDS aims to establish rules, common standards and practices, as well as a governance framework for the **“primary” and “secondary” use of health data**. The Regulation improves individuals’ access to and control over their personal electronic health data, while also enabling certain data to be reused for public interest, policy support, and scientific research purposes.

More specifically, the Regulation:

- Sets rules for the placing on the market, making available on the market or put into service of **electronic health records (EHR) systems**
- Defines rules for the **secondary use** of electronic health data
- Establishes a **mandatory cross-border infrastructure** for **primary use** of electronic health data across the Union, as well as for **secondary use**
- Establishes the **European Health Data Space Board** (EHDS Board) to facilitate the **cooperation and information exchange** among Member States

Applicable key sectors



This Regulation applies to:

- | | |
|--|---|
| • Health data holders | interoperable with MyHealth@EU |
| • Data users to whom electronic health data are made available by data holders | • Manufacturers and suppliers of Electronic Health Record (EHR) systems |
| • Controllers and processors of electronic health data | • Market surveillance authorities responsible for EHR systems |
| • Controllers and processors established in a third country that has been connected to or is | • Health professionals, researchers and laboratories |

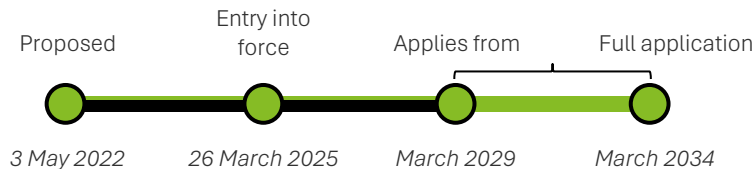
Intersection with other EU law:

- | | |
|--|-----------------------------------|
| • AI Act | (CBHC Directive) |
| • CRA | • GDPR |
| • Data Act | • In Vitro Diagnostics Regulation |
| • Data Governance Act | • Medical Devices Regulation |
| • Cross-border healthcare collaborations Directive | • NIS2 Directive |

Regulatory Stakeholders:

- | | |
|------------------------------------|---------------------------------------|
| • European Commission | • National digital health authorities |
| • European Health Data Space Board | |

Timeline



Digital Markets Act (DMA)

The DMA is a competition law that aims to ensure fair competition among stakeholders operating in the digital space through obligations and prohibitions limiting the power of gatekeepers

Description

The Digital Markets Act aims to establish a **fair and more contestable digital market** by identifying **gatekeepers** (i.e., large digital platforms providing core platform services) and making them comply with a set of obligations, such as:

- **Prohibition of combining personal data** across different gatekeeper services and / or platforms
- **Obligation** to allow users to **uninstall any pre-installed software** and allow the installation of third-party software
- **Prohibition** on giving **preferential treatment** to treat their own services or products.

Non-compliance can result in **a fine** of up to 10% of global annual turnover for businesses. Providing incorrect and / or misleading information to authorities can also lead to **a fine** up to 1% of global annual turnover.

As of October 2025, the EU Commission designated as gatekeepers: **Alphabet, Amazon, Apple, Booking.com, ByteDance, Meta, Microsoft, and Booking**. In addition, **23 core platform services** provided by the gatekeepers have been identified. The six gatekeepers will have to ensure full compliance with the DMA obligations for each of the designated core platform services.

First rounds of mandatory compliance reports have been published by the Gatekeepers on the Commission website.

Applicable key sectors



This Regulation applies to:

- *Core platform service providers (e.g., online intermediation services, online search engines, online social networks, video-sharing platforms) designated as “gatekeepers” by the EU Commission in accordance with Article 3, DMA*

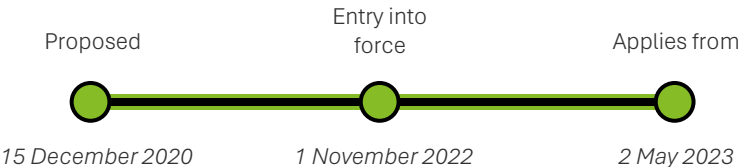
Intersection with other EU law:

- *Data Governance Act*
- *GDPR*

Regulatory Stakeholders:

- *National Competent Authorities*
- *European Commission*
- *European Data Protection Supervisor*
- *European Data Protection Board*

Timeline



Digital Services Act (DSA)

The DSA aims to create a transparent and accountable online environment by setting out rules framing the responsibilities of digital intermediary service providers with regard to the content transmitted or displayed on their network, in order to strengthen the protection of users’ fundamental rights online

Description

The DSA aims to ensure user **safety online** and create an **open and competitive online platform market** by preventing harmful activities online and the spread of disinformation.

The DSA introduces a **liability regime** for “**digital intermediary service providers**”. It dictates who is responsible for the content that is transferred or displayed on a communications network. Among other requirements, providers must provide **transparency in their advertising practices**, perform **risk assessments** and take responsibility for the **removal** of content after it has been flagged.

The DSA introduces different sets of obligation based on the role, size and impact on the digital ecosystem of digital intermediary service providers.

As of October 2025, **20 Very Large Online Platforms (VLOPs)** and **Very Large Online Search Engines (VLOSEs)** were designated. Furthermore, the first round of DSA audit reports was published on the Commission website.

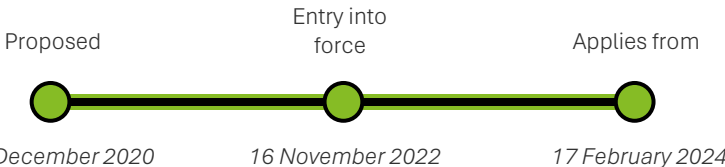
Applicable key sectors

 Energy & Resources	 Manufacturing & Consumer
 Financial Services	 Technology, Media & Telecommunications
 Life Sciences & Healthcare	 Government & Public Services

- This Regulation applies to:**
- Intermediary service providers, namely:*
- *Very large online platforms (i.e., having a number of average monthly active recipients of the service equal or higher than 45 million)*
 - *Online platforms*
 - *Hosting service providers (including cloud and webhosting services)*
 - *Intermediary service providers (including Internet access providers and Domain Name Registries)*

- Intersection with other EU law:**
- *EU law on consumer protection (e.g., Regulations (EU) 2017/2394 and (EU) 2019/1020, Directives 2001/95/EC, 2005/29/EC, 2011/83/EU and 2013/11/EU, Council Directive 93/13/EEC, and on the protection of personal data, in particular the GDPR)*
 - *Other EU law regulating the provision of information society services and intermediary services in the internal market (e.g., Directive 2010/13/EU, Reg. EU/2019/1148, EU/2019/1150, EU/2021/784, EU/2021/1232)*
- Regulatory Stakeholders:**
- *European Commission*
 - *European Board for Digital Services*
 - *National Competent Authorities*

Timeline



Markets in Crypto-Assets Regulation (MiCA)

The size and scope of the crypto-asset market has grown exponentially in recent years, with little regulatory guidance in face of the rapid growth of the market and the advancement of new types of crypto assets. To this end, the EU co-legislators have adopted the Markets in Crypto-Assets Regulation (MiCA)

Description

As part of the Digital Finance Package, the MiCA lays down harmonised requirements and obligations for the offer to the public and admission to trading on a **crypto-asset trading platform**. In particular, the Regulation covers crypto-assets that are not currently regulated by existing financial services legislation, and introduces key **transparency, disclosure, authorisation and supervisory obligations** for those issuing and trading **asset-referenced tokens (ARTs)** and **e-money tokens (EMTs)**.

The aims of the Regulations are threefold:

- Provide an appropriate level of **consumer protection** by imposing strict transparency obligations on issuers, offerors, traders, and providers of crypto-assets
- Support **market integrity** and **financial stability**
- Facilitate the use of **distributed ledger technology** in financial markets.

Offers to the public of asset-referenced tokens in the Union or applications for admission to trading of such crypto-assets should only be permitted where the competent authority has authorised the issuer of such crypto-assets and approved the relevant crypto-asset white paper.

Credit institutions authorised under Directive 2013/36/EU should not need any further authorisation under this Regulation to offer or seek admission to trading of asset-referenced tokens

Applicable key sectors

 Energy & Resources	 Manufacturing & Consumer
 Financial Services	 Technology, Media & Telecommunications
 Life Sciences & Healthcare	 Government & Public Services

This Regulation applies to:

- Issuers of Asset Reference Tokens (ARTs) and e-Money Tokens (EMTs)
- Crypto-Asset Service Providers (CASPs)

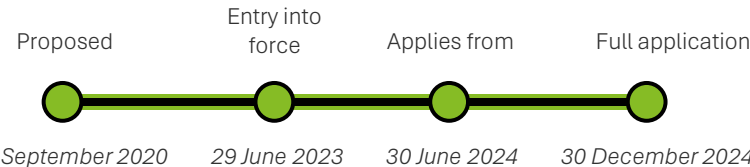
Intersection with other EU law:

- Anti-money laundering and countering the financing of terrorism (AML/CFT) legislation
- Directive 2013/36/EU
- Directive 2024/65/EU (MiFID II)
- DORA
- Electronic Money Directive II (EMD2)

Regulatory Stakeholders:

- European Commission
- European Securities and Markets Authority (in cooperation with European Banking Authority, European Insurance and Occupational Pensions Authority and the European Central Bank)
- National supervisory authorities

Timeline



European Digital Identity Regulation (EUDI)

The European Digital Identity Regulation (EUDI) will revolutionise digital identity in the EU by enabling the creation of a universal, trustworthy, and secure European digital identity wallet

Description

The new **Regulation** establishing a framework for a **European Digital Identity** (EUDI Regulation) builds on the 2014 Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).

The EUDI regulation addresses the shortcomings of eIDAS by improving the effectiveness of the current framework for digital Identity and **extending** its **benefits** to the **private sector**.

Member States will be mandated to offer citizens and businesses **digital wallets**, which can link their national digital identities with proof of other personal attributes like driving licenses, diplomas, and bank accounts. These wallets may be issued either by public authorities or recognised private entities. The aim is to provide Europeans with **full control over** their **data** while accessing online services, eliminating unnecessary data sharing.

The EUDI Regulation is **aligned** with existing **cybersecurity legislation** and mandates compliance with cybersecurity requirements.

Moreover, it will **expand** the scope of **trust services** to include recording of electronic data in an electronic ledger, the management of remote electronic signature and the creation devices or remote electronic seal creation devices

Applicable key sectors



Energy & Resources



Manufacturing & Consumer



Financial Services



Technology, Media & Telecommunications



Life Sciences & Healthcare



Government & Public Services

This Regulation applies to:

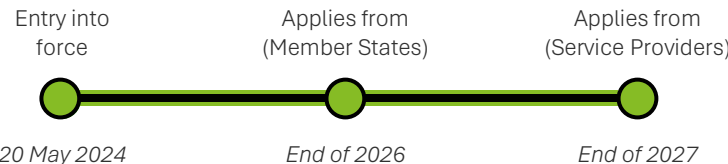
- *Trust service providers*
- *Qualified trust service providers*
- *Citizens*
- *Public authorities*

Intersection with other EU law:

- GDPR
- eIDAS

- Regulatory Stakeholders:**
- *National conformity assessment bodies*
 - *European Commission*
 - *ENISA*
 - *National supervisory authorities*

Timeline





Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex

Key sectors Use Cases: Categories and Assumptions

In order to enhance the understanding of the legislative requirements and highlight intersections, obligations targeting stakeholders across different sectors have been clustered into six categories for each use case and assumptions have been developed

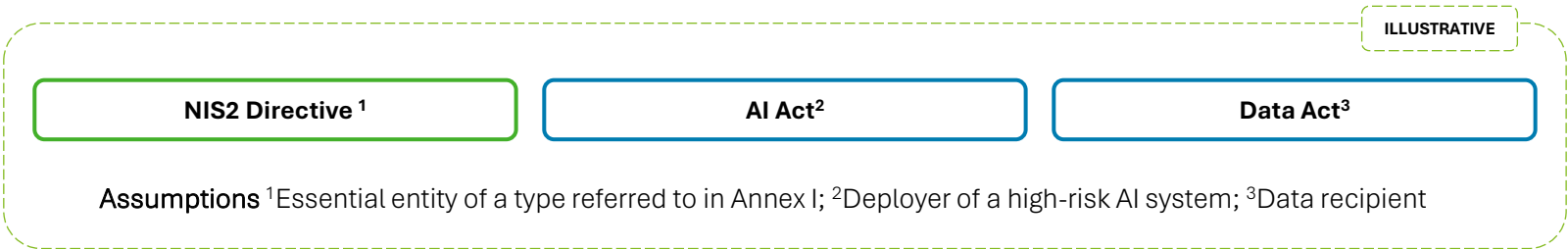
Categories used to cluster legislative requirements

The EU cyber and digital legislations requirements have been categorized into six categories to provide an overview and streamline enforcement actions



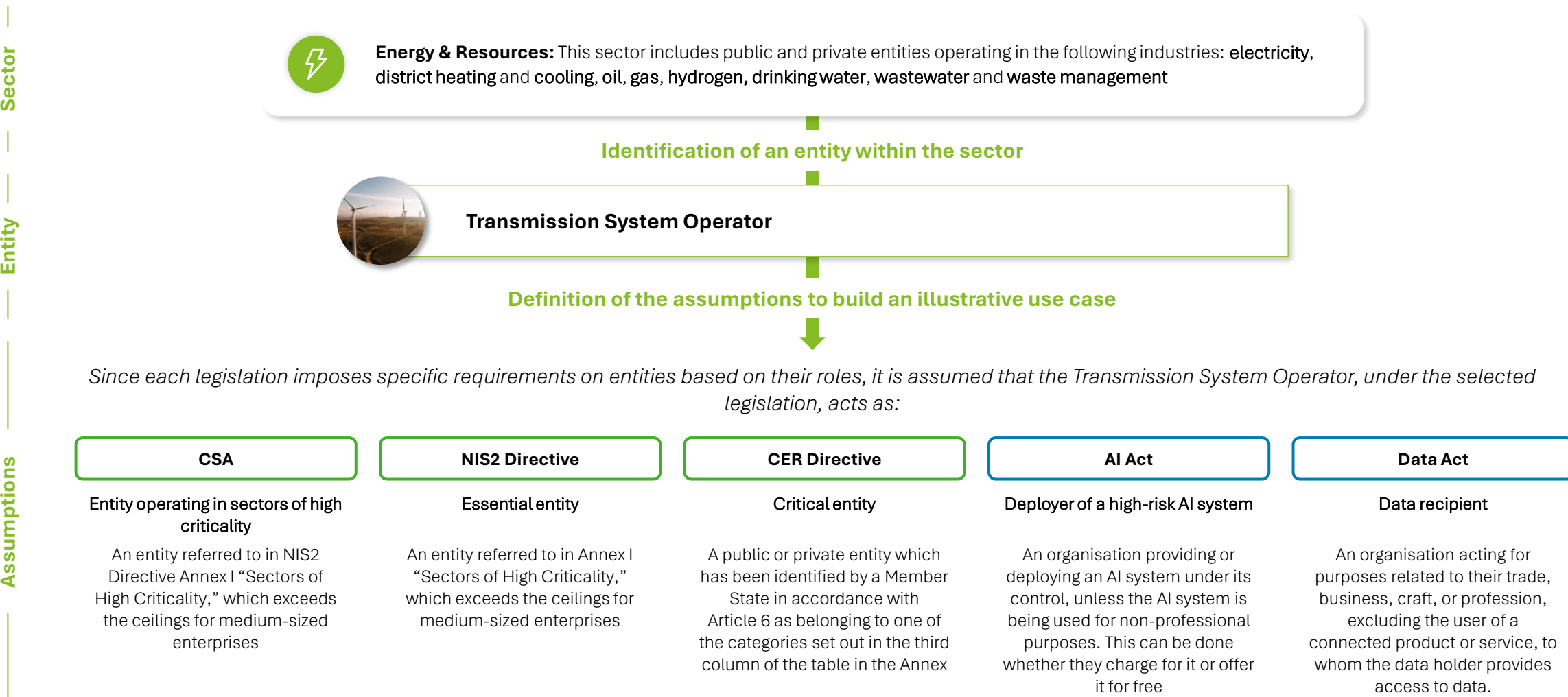
Assumptions

Each legislation imposes specific requirements on organisations according to different roles (e.g., manufacturer, importer, distributor). Thus, an assumption about the specific role has been made for each use case. Due to the complexity and variability of legal contexts, these use cases should not be seen as comprehensive or universally applicable:



Energy & Resources – Use Case (1/5)

The Energy & Resources use case provides an illustrative snapshot of how a Transmission System Operator is impacted by the identified EU digital and cyber legislation and is based on a set of assumptions that may not account for all possible scenarios



Energy & Resources – Use Case (2/5)

Transmission System Operator

Regulatory intersection: How do the EU's cyber and digital laws intersect?

 Governance Measures	 Risk Management & Technical Standards	 Vulnerability Management	 Incident Management	 ICT Security Compliance & Certification	 Data Governance & Management
The analysed legislation requires entities to review their internal security governance systems (e.g., cyber/IT security and physical security convergence based on an all-hazard approach), strengthen accountability of management bodies, and establish clear roles and responsibilities for overseeing and managing ICT-related risks. Being a horizontal legislation, NIS2 Directive introduces a general obligation to set a clear and technology-agnostic risk governance framework, while CER Directive addresses the physical and operational resilience, complementing NIS2 Directive provisions targeting the all-hazard approach. Subject-specific legislation, such as the AI Act, introduces vertical requirements covering the use of high-risk AI systems, which shall be managed with proper organisational controls. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive and CER Directive overall governance obligations.	The analysed legislation requires entities to set up an ICT-related risk management framework, as well as to assess and manage all natural and human-made risks, targeting an all-hazards approach. As a horizontal legislation, NIS2 Directive introduces a broad obligation to set up a comprehensive, documented and regularly updated risk management framework, including strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks; while CER Directive requires entities to complete a comprehensive risk assessment covering all relevant natural and human-made risks, complementing NIS2 Directive provisions. Under the AI Act, AI systems must be incorporated into the ICT risk management framework, documented in policies, and integrated into third-party risk management processes like supply chain mapping and contract review. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive and CER Directive overall risk management obligations.	The analysed legislation requires entities to establish structured processes for identifying, assessing and mitigating ICT vulnerabilities as part of their overall risk management framework. Being a horizontal legislation, NIS2 Directive introduces a general obligation to implement appropriate measures and processes to manage ICT system vulnerabilities, such as periodic vulnerability assessment and penetration testing, as well as to record and mitigate such vulnerabilities either directly or with the involvement of ICT providers. For AI systems, deployers may not directly test the system's but instead manage its security through third-party risk management. The CSA further complement the obligations set by NIS2 Directive, by introducing coordinated preparedness testing and vulnerability assessments, supported by the Cybersecurity Emergency Mechanism, which results shall be integrated into a remediation plan.	The analysed legislation requires entities to set up appropriate measures for ICT incident reporting and handling. As horizontal legislation, CSA require entities to support the EU Cybersecurity Reserve to assist in significant or large-scale cybersecurity incidents and NIS2 Directive outlines measures for the notification of ICT significant incidents to national CSIRTs, or competent authorities. Moreover, both NIS2 Directive and CER Directive require entities to establish appropriate technical, operational, and security measures to prevent, respond to, and recover from incidents. Subject-specific legislation, such as the AI Act, introduces vertical requirements covering measures for the notification of serious incidents to market surveillance authorities. The legislation aims to simplify and streamline reporting procedures by encouraging the establishment of national single-entry points for the fulfilment of reporting requirements. Currently, the AI Act falls outside such requirements and envisages notification procedures towards market surveillance authorities. However, such authorities are encouraged to correspond to single entry points.	The analysed legislation requires entities to demonstrate compliance with ICT security requirements. Being a horizontal legislation, NIS2 Directive introduces a general obligation for Member States to require essential and important entities to use ICT products, services, and processes certified under European cybersecurity certification schemes pursuant to Article 49 of Regulation (EU) 2019/881, or, in their absence, to comply with relevant European or international standards. Entities shall oversee the compliance with ICT security requirements by providers as part of their third-party risk management obligations.	The analysed legislation, without prejudice to the overall compliance with data protection obligations under the GDPR, as per NIS2 Directive, requires entities to comply with additional subject-specific obligations. These include ensuring input data is relevant and sufficiently representative under the AI Act, refraining from using or sharing data in ways that could harm data holders or users under the Data Act, and limiting information exchange to what is relevant and proportionate to protect sensitive data under the CER Directive.

Energy & Resources – Use Case (3/5)

Transmission System Operator

Obligations						
	CSA ¹	NIS2 Directive ²	CER Directive ³	AI Act ⁴	Data Act ⁵	
Governance Measures	x Not covered	✓ Establish appropriate and proportionate governance measures, i.e., accountability of management bodies for cybersecurity risk management measures ✓ Establish appropriate and proportionate organisational measures based on an all-hazards approach to manage cybersecurity related risks	✓ Adopt proportionate organisational measures i.e., appoint a liaison for communication with authorities ✓ Manage employee security by categorizing personnel with critical roles, enforcing access controls to premises, infrastructure, and sensitive data, conducting background checks, and setting training and qualification standards. ✓ Awareness of these measures is promoted among relevant staff through training, informational materials, and exercises	✓ Take appropriate organizational measures to ensure that the use of high-risk AI systems is in accordance with the instructions for the use of such system ✓ Ensure the staff has adequate AI literacy ✓ Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support	x Not covered	
Risk Management & Technical Standards	x Not covered	✓ Establish appropriate and proportionate technical and operational measures to manage cybersecurity related risks, e.g., adopt adequate policies, including business continuity and disaster recovery, third-party and supply chain security, ensure security in network and information systems acquisition, development and maintenance ✓ Adopt cyber hygiene practices and cybersecurity training, use of multi-factor authentication or continuous authentication solutions	✓ Complete a comprehensive risk assessment within nine months of notification and every four years thereafter, covering all relevant natural and human-made risks, including cross-sectoral and cross-border dependencies. Assessments should be based on the Member State risk assessment carried out by the National Competent Authority, and any other relevant source of information	✓ Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for use ✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers. If the use of the high-risk AI system presents a risk, the deployer shall inform the provider or distributor, the relevant market surveillance authority, and suspend the use of that system	x Not covered	

Energy & Resources – Use Case (4/5)

Transmission System Operator

Legend Cybersecurity AI & Data Platform Economy Digital Finance Digital Identity

Obligations

	CSA ¹	NIS2 Directive ²	CER Directive ³	AI Act ⁴	Data Act ⁵
Vulnerability Management	✓ Participate in vulnerability assessments, coordinated preparedness testing (e.g., penetration testing) supported by the Cybersecurity Emergency Mechanism ✓ Integrate the results of the coordinated preparedness testing into a remediation plan	✓ Establish appropriate and proportionate technical and operational measures to manage vulnerabilities and report them to the national CSIRT an, where needed, to service recipients ✓ Take into account vulnerabilities specific to direct suppliers and service providers and the overall quality of their products and cybersecurity practices	x <i>Not covered</i>	x <i>Not covered</i>	x <i>Not covered</i>
Incident Management	✓ Support from the EU Cybersecurity Reserve may be requested solely to assist in responding to, and initiating recovery from, significant cybersecurity incidents, large-scale cybersecurity incidents, or incidents of equivalent scale	✓ Establish appropriate and proportionate technical and operational measures for incident handling ✓ Establish business continuity measures, such as backup management and disaster recovery, and crisis management ✓ Notify the national CSIRT, or competent authority, of any incident that has a significant impact on the provision of the operator's services	✓ Adopt proportionate technical and security measures to prevent, respond to, and recover from incidents, including employee security and awareness ✓ Notify authorities of significant service disruptions within 24 hours and provide detailed reports within a month. Incidents affecting six or more Member States must be reported to the Commission. Reports should include all relevant details without increasing the entity's liability	✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers within their post-market monitoring activities, including data regarding any discovered serious incident ✓ Inform first the provider, and then the importer or distributor and the relevant market surveillance authorities in case of a serious incident as defined in Article 3(49)	x <i>Not covered</i>

Energy & Resources – Use Case (5/5)

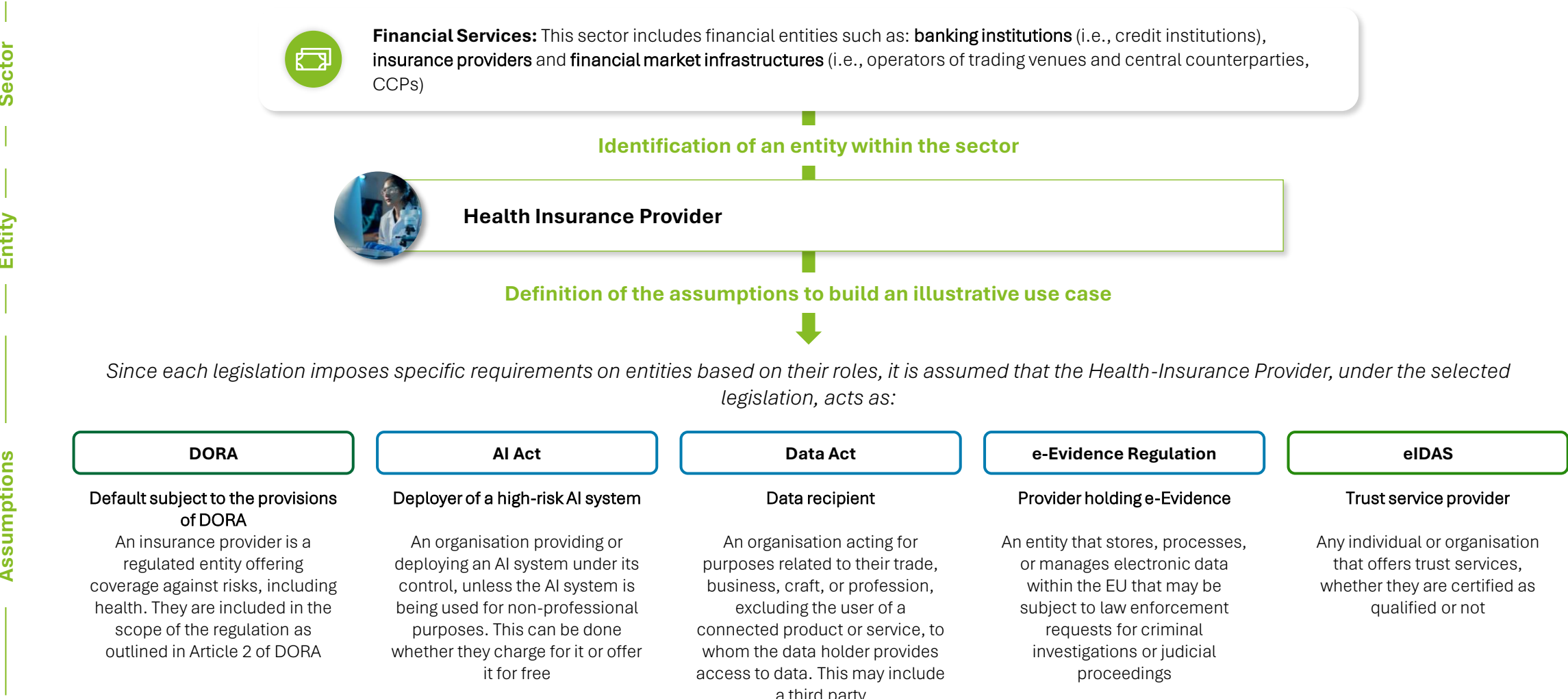
Transmission System Operator

Legend  Cybersecurity  AI & Data  Platform Economy  Digital Finance  Digital Identity

		Obligations				
		CSA ¹	NIS2 Directive ²	CER Directive ³	AI Act ⁴	Data Act ⁵
 ICT Security Compliance & Certification	x Not covered		✓ May be required to use IT/OT products, services and processes, developed by the operator or procured from third parties, that are certified under European cybersecurity certification schemes adopted under the Cybersecurity Act, in order to demonstrate compliance with cybersecurity risk management measures	x Not covered	x Not covered	x Not covered
	x Not covered		✓ Comply with fundamental data protection obligations , including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	✓ Request justified background checks for individuals in sensitive roles or with authorised access , complying with national and EU laws and limited to necessary security risk assessments. Checks verify identity and criminal records, usually completed within 10 working days ✓ Ensure that information exchange is limited, relevant, and proportionate, to protect sensitive data	✓ Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system, to the extent the deployer exercises control over the input data ✓ Keep the logs , to the extent that they are under the deployer's control, automatically generated by the high-risk AI system for a period appropriate to the intended purpose of the high-risk AI system	✓ Refrain from using the data obtained from data holders to develop a connected product that competes with the original connected product and avoid sharing the data with any third party for that purpose ✓ Refrain from using data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable the data holder ✓ Refrain from using data for the profiling , unless necessary to provide service requested by user; share data with other third parties or to a designated gatekeeper under the DSA

Financial Services – Use Case (1/5)

The Financial Services use case provides an illustrative snapshot of how a Health-Insurance Provider is impacted by the identified EU digital and cyber legislation and is based on a set of assumptions that may not account for all possible scenarios



Financial Services – Use Case (2/5)

Health Insurance Provider



Back to slide 25 ↗

Regulatory intersection: How do the EU's cyber and digital laws intersect?



Governance Measures

The analysed legislation requires entities to **review their internal security governance systems** (e.g., cyber/IT security and physical security convergence based on an all-hazard approach), strengthen **accountability of management bodies**, and establish clear **roles and responsibilities** for overseeing and managing ICT-related risks.

DORA introduces a general obligation to set a **clear and technology-agnostic risk governance framework**, including the obligation to establish a **sufficiently independent control function to manage and oversee ICT-related risks**.

Subject-specific legislation, such as the AI Act introduces **vertical requirements** covering the use of **high-risk AI systems**, which shall be managed with **proper organisational controls**. While **e-Evidence Regulation** requires the establishment of internal policies, as well as **roles and responsibilities** to manage **judicial orders**; and **eIDAS** requires entities to take **appropriate organisational measures** to manage **trust service security risks**. Therefore, **compliance** to subject-specific legislation **contributes** to the fulfilment of **DORA overall governance** obligations.



Risk Management & Technical Standards

The analysed legislation requires entities to set up an **ICT-related risk management framework**.

As the cornerstone legislation for financial entities, **DORA** introduces a broad obligation to set up a **comprehensive, documented and regularly updated risk management framework**, including strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks.

Under subject-specific legislation, such as the **AI Act**, **AI systems** must be incorporated into the ICT risk management framework, with their use documented in policies and integrated into the entity's third-party risk management process. Other **subject-specific risk management obligations** (e.g., **e-Evidence Regulation** and **eIDAS**) constitute further specifications of the overall risk management obligation imposed by DORA.

Therefore, **compliance** to subject-specific legislation **contributes** to the fulfilment of **DORA overall risk management** obligations.



Vulnerability Management

The analysed legislation requires entities to establish **structured processes** for **identifying, assessing and mitigating ICT vulnerabilities** as part of their overall risk management framework.

DORA introduces a general obligation to **periodically identify and assess cyber threats and ICT vulnerabilities**, execute appropriate **tests**, such as vulnerability assessments and end-to-end testing and penetration testing, as well as establish **crisis communication plans** to disclose vulnerabilities. For **AI systems**, deployers may not directly test the system's but instead manage its security through **third-party risk management**, including supply chain oversight and contractual safeguards.

Subject-specific legislation, such as the **e-Evidence Regulation** introduces **vertical requirements** covering the implementation of **safeguards** concerning **data** and the establishment of **reporting and escalation processes**. While **eIDAS** requires entities to perform **2-year vulnerability assessments**.



Incident Management

The analysed legislation requires entities to set up appropriate measures for **ICT incident reporting and handling**.

DORA sets a general obligation to **manage incidents throughout their lifecycle** according to recognized standards and frameworks. Hence, entities are expected to manage all incidents related to ICT systems and tools they manufacture or use (e.g., AI systems, software).

With regard to **incident reporting obligations under DORA**, Member States are expected to **provide single entry points** at national level. The **AI Act** requires entities to notify **market surveillance authorities** of serious incidents. However, **it is possible that such authorities will coincide with the single-entry points** designated under NIS2 Directive. Under **eIDAS**, entities shall report incidents to competent supervisory authorities which will likely not coincide with single entry points designated under DORA. Lastly, the **e-Evidence Regulation** constitutes further specifications of the overall incident management obligation imposed by DORA.



ICT Security Compliance & Certification

The analysed legislation requires entities to **demonstrate compliance with ICT security requirements**.

DORA introduces a general obligation to adopt ICT systems, protocols, and tools that are appropriate, reliable, and technologically resilient. The use of ICT systems, protocols or tools that are **certified under European cybersecurity certification schemes** adopted pursuant to Article 49 of Regulation (EU) 2019/881 or **relevant European and international standards** (e.g., upcoming AI standards defined by CEN/CENELEC), contributes to the overall compliance under DORA for the adoption of appropriate, reliable, and technologically resilient ICT systems, protocols or tools.

Subject-specific legislation, such as the **e-Evidence Regulation** introduces **vertical requirements** covering the implementation of secure ICT infrastructure, **eIDAS-compliant** communication, and the integration with approved IT systems. While **eIDAS** requires **biennial audits** and use of **cybersecurity certification schemes**. Therefore, **compliance** to subject-specific legislation **contributes** to the fulfilment of **DORA overall ICT security compliance and certification** obligations.



Data Governance & Management

The analysed legislation requires entities to adopt ICT systems, protocols, and tools with sufficient capacity to process necessary data while safeguarding its confidentiality, integrity, and availability under **DORA**. **obligations under the GDPR**, requires entities to comply with **additional subject-specific obligations** (e.g., ensure that input data is relevant and sufficiently representative under the **AI Act**), and refrain from using or sharing data for purposes that might damage the data holders or users under the **Data Act**.

Furthermore, ensuring access to and disclosure of only explicitly requested data, alongside measures against data forgery and theft under **eIDAS**.

Lastly, **e-Evidence Regulation** mandates limited data access, timely preservation and delivery, strict confidentiality, and thorough record-keeping for compliance and reporting.

Financial Services – Use Case (3/5)

Health Insurance Provider

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations

	DORA ¹	AI Act ²	Data Act ³	e-Evidence Regulation ⁴	eIDAS ⁵
 Governance Measures	✓ Establish an internal governance and control framework that ensures an effective and prudent management of ICT risk ✓ The management body shall define, approve, oversee and be responsible for all arrangements related to the ICT risk management framework ✓ A control function with appropriate level of independence shall be responsible for managing and overseeing ICT risk	✓ Take appropriate organizational measures to ensure that the use of high-risk AI systems is in accordance with the instructions for the use of such system ✓ Ensure the staff has adequate AI literacy ✓ Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support	x <i>Not covered</i>	✓ Take appropriate organizational measures to ensure that the use of high-risk AI systems is in accordance with the instructions for the use of such system ✓ Ensure the staff has adequate AI literacy ✓ Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support	✓ Take appropriate organisational measures to manage risks posed to the security of the trust services provided ✓ Employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules
 Risk Management & Technical Standards	✓ Implement a comprehensive and well-documented ICT risk management framework, including ICT third-party risk (i.e., strategies, policies, procedures, ICT protocols to duly and adequately protect all information assets and ICT assets) ✓ Draft and update a digital operational resilience strategy setting out how the framework shall be operationalized	✓ Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for use ✓ Perform a fundamental rights impact assessment (FRIA) for high-risk AI systems before deployment ✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers. If the use of the high-risk AI system presents a risk, the deployer shall inform the provider or distributor, the relevant market surveillance authority, and suspend the use of that system	x <i>Not covered</i>	✓ Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for use ✓ Perform a fundamental rights impact assessment (FRIA) for high-risk AI systems before deployment ✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers. If the use of the high-risk AI system presents a risk, the deployer shall inform the provider or distributor, the relevant market surveillance authority, and suspend the use of that system	✓ Take appropriate technical and organisational measures to manage risks posed to the security of the trust services provided ✓ Use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them ✓ Comply with service-specific security requirements (e.g., ICT security for electronic signatures)

Financial Services – Use Case (4/5)

Health Insurance Provider

Legend  Cybersecurity  AI & Data  Platform Economy  Digital Finance  Digital Identity

Obligations

	DORA ¹	AI Act ²	Data Act ³	e-Evidence Regulation ⁴	eIDAS ⁵
Vulnerability Management	✓ Identify and assess on a continuous basis cyber threats and ICT vulnerabilities relevant to ICT supported business functions ✓ Execute appropriate tests (e.g., vulnerability assessments, source code reviews, scenario-based and performance testing, end-to-end testing and penetration testing) ✓ Responsibly disclose vulnerabilities to clients and counterparts by establishing crisis communication plans	x <i>Not covered</i>	x <i>Not covered</i>	✓ Implement technical and organisational safeguards for data confidentiality, integrity, and availability ✓ Establish processes for reporting and escalating issues with order execution	✓ Perform a regular 2-year vulnerability assessment to maintain the certification of conformity for qualified electronic signature creation devices
Incident Management	✓ Adopt an ICT incident management process to detect, manage, and communicate ICT-related incidents ✓ Report major ICT-related incidents to competent authorities established in accordance with article 46	✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers within their post-market monitoring activities, including data regarding any discovered serious incident ✓ Inform first the provider, and then the importer or distributor and the relevant market surveillance authorities in case of a serious incident as defined in Article 3(49)	x <i>Not covered</i>	✓ Define procedures for incident response and documentation related to orders ✓ Keep records to support accountability and audits	✓ Take appropriate technical and organisational measures to prevent and minimize the impact of security incidents ✓ Notify supervisory authority or other relevant bodies within 24h of any breach of security or loss of integrity that has a significant impact on the trust service provided or on personal data ✓ Notify the legal or natural person to whom the service is provided

Financial Services – Use Case (5/5)

Health Insurance Provider

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations		DORA ¹	AI Act ²	Data Act ³	e-Evidence Regulation ⁴	eIDAS ⁵
ICT Security Compliance & Certification		✓ Adopt ICT systems, protocols, and tools that are appropriate, reliable, and technologically resilient	x <i>Not covered</i>	x <i>Not covered</i>	✓ Ensure ICT infrastructure meets cybersecurity standards as per implementing acts ✓ Use secure communication channels compliant with eIDAS ✓ Integrate with decentralised or approved secure IT systems for data exchange	✓ Carry out an audit by a conformity assessment body at least every 24 months and submit the resulting conformity assessment report to competent supervisory authorities ✓ Rely on cybersecurity certification schemes to demonstrate compliance of European Digital Identity Wallets
		✓ Adopt ICT systems, protocols and tools equipped with sufficient capacity to process data necessary for the performance of activities, as well as to safeguard the confidentiality, integrity and availability of data	✓ Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system, to the extent the deployer exercises control over the input data ✓ Keep the logs, to the extent that they are under the deployer's control, automatically generated by the high-risk AI system for a period appropriate to the intended purpose of the high-risk AI system	✓ Refrain from using the data requested from data holders to develop a connected product that competes with the connected product from which the data originate, and from sharing the data with a third party with that intent ✓ Refrain from using data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable the data holder ✓ Refrain from using data for the profiling, unless necessary to provide service requested by user; share data with other third parties or to a designated gatekeeper under the DSA	✓ Ensure access to and disclosure of only the data explicitly requested, adhering to principles of data minimisation and purpose limitation ✓ Promptly preserve requested data and produce them within stipulated deadlines to comply with legal requirements ✓ Maintain strict confidentiality of orders and data, with appropriate handling of privileged information; notify data subjects unless legally exempted ✓ Maintain comprehensive records and support monitoring and reporting obligations as mandated by the Regulation	✓ Use trustworthy systems to safeguard confidentiality, integrity, and availability of data ✓ Take appropriate measures against forgery and theft of data ✓ Comply with fundamental data obligations outlined in Regulation 2016/679 (GDPR)

Life Sciences & Healthcare – Use Case (1/5)

The Life Sciences & Healthcare use case provides an illustrative snapshot of how a manufacturer of medical imaging equipment is impacted by the identified EU digital and cyber legislation and is based on a set of assumptions that may not account for all possible scenarios

Sector

Entity

Assumptions



Life Sciences & Healthcare. This sector includes public and private entities such as **healthcare service providers**, EU reference **laboratories**, **research and development of medicinal products**, manufacture of **medical equipment**, **pharmaceutical products** and **pharmaceutical preparations**

Identification of an entity within the sector



Manufacturer of Medical Imaging Equipment

Definition of the assumptions to build an illustrative use case

Since each legislation imposes specific requirements on entities based on their roles, it is assumed that the manufacturer of medical imaging equipment, under the selected legislation, acts as:

MDR	NIS2 Directive	RED	AI Act	Data Act	EHDS
Manufacturer of medical devices Any natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured or fully refurbished, and markets that device under its name or trademark	Essential entity An entity referred to in Annex I “Sectors of High Criticality,” which exceeds the ceilings for medium-sized enterprises	Manufacturer Any person or company that makes radio equipment or has it designed or produced and then sells or distributes it under their own name or brand	Deployer of a high-risk AI system An organisation providing or deploying an AI system under its control, unless the AI system is being used for non-professional purposes. This can be done whether they charge for it or offer it for free	Data holder A person or organisation that has the right or responsibility, to use and share data. This can include product or service data that they have gathered or created while providing a service	Manufacturer of an EHR system Any natural or legal person who manufactures a product or has a product designed or manufactured and markets that product under its name or trademark (Regulation (EU) 2019/1020)

Life Sciences & Healthcare – Use Case (2/5)

Manufacturer of medical imaging equipment

Regulatory intersection: How do the EU's cyber and digital laws intersect?

Governance Measures	Risk Management & Technical Standards	Vulnerability Management	Incident Management	ICT Security Compliance & Certification	Data Governance & Management
The analysed legislation requires entities to review their internal security governance systems (e.g., cyber/IT security and physical security convergence based on an all-hazard approach), strengthen accountability of management bodies, and establish clear roles and responsibilities for overseeing and managing ICT-related risks. Being a horizontal legislation, NIS2 Directive introduces a general obligation to set a clear and technology-agnostic risk governance framework. Subject-specific legislation, such as the AI Act introduces vertical requirements covering the use of high-risk AI systems, which shall be managed with proper organisational controls to ensure they are used according to guidelines. While RED requires entities to implement a quality system as well as an organisational structure with regard to design and product quality. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive overall governance obligations.	As a horizontal legislation, NIS2 Directive introduces a broad obligation to set up a comprehensive, documented and regularly updated risk management framework, namely strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks. Under subject-specific legislation, such as the AI Act, AI systems must be incorporated into the ICT risk management framework, with their use documented in policies and integrated into the entity's third-party risk management process. Other subject-specific risk management obligations (e.g., MDR, that mandates to minimise hazards in device design with a focus on IT security, and RED, that enforces security standards for radio equipment) constitute further specifications of the overall risk management obligation imposed by NIS2. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive overall risk management obligations.	The analysed legislation requires entities to establish structured processes for identifying, assessing and mitigating ICT vulnerabilities as part of their overall risk management framework. Being a horizontal legislation, NIS2 Directive introduces a general obligation to implement appropriate measures and processes to manage ICT system vulnerabilities, such as periodic vulnerability assessment and penetration testing, as well as to record and mitigate such vulnerabilities either directly or with the involvement of ICT providers. For AI systems, deployers may not directly test the system's but instead manage its security through third-party risk management.	The analysed legislation requires entities to establish measures for ICT incident reporting and handling. As horizontal legislation, NIS2 Directive outlines measures for the notification of ICT significant incidents to national CSIRTs, or competent authorities, as well as appropriate technical, operational, and security measures to prevent, respond to, and recover from incidents. While the AI Act, introduces vertical requirements covering measures for the notification of serious incidents to market surveillance authorities. Both legislations aims to simplify and streamline reporting procedures by encouraging the establishment of national single-entry points for the fulfilment of reporting requirements. Moreover, the Data Act adds that, in emergencies or major cybersecurity incidents, data holders must provide relevant data to public authorities or Union bodies upon request. The EHDS Regulation further requires notification of EHR system incidents to market surveillance authorities, without prejudice to NIS2 Directive and GDPR breach obligations. Together, these instruments promote effective incident management, though alignment of reporting channels remains necessary.	The analysed legislation requires entities to demonstrate compliance with ICT security requirements. Being a horizontal legislation, NIS2 Directive introduces a general obligation for Member States to require essential and important entities to use ICT products, services, and processes certified under European cybersecurity certification schemes pursuant to Article 49 of Regulation (EU) 2019/881, or, in their absence, to comply with relevant European or international standards. Entities shall oversee the compliance with ICT security requirements by providers as part of their third-party risk management obligations. Subject-specific legislation, such as the RED and EHDS Regulation introduce vertical requirements that further extend these obligations by requiring conformity of with essential requirements and common specifications, supported by technical documentation.	The analysed legislation, without prejudice to the overall compliance with data protection obligations under the GDPR, as per NIS2 Directive, establishes additional sector-specific data obligations. Data governance is further enhanced under the Data Act. Data should be accessible to users securely, free of charge, in structured, machine-readable formats, and, if needed, in real-time. The AI Act requires deployers to ensure input data is relevant and representative for the high-risk AI system's intended purpose and to retain system-generated logs under their control for an appropriate period. Furthermore, the RED mandates safeguards in radio equipment to protect users' and subscribers' personal data and privacy. Lastly, the EHDS Regulation further requires EHR systems and interoperable products to meet essential requirements on interoperability, security, and logging, in line with GDPR principles. Collectively, these measures aim to promote trustworthy and interoperable data management across the Union.

Life Sciences & Healthcare – Use Case (3/5)

Manufacturer of medical imaging equipment

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

		Obligations					
		MDR ¹	NIS2 Directive ²	RED ³	AI Act ⁴	Data Act ⁵	EHDS ⁵
 Governance Measures		x <i>Not covered</i>	✓ Establish appropriate and proportionate governance measures, i.e. accountability of management bodies for cybersecurity risk management measures ✓ Establish appropriate and proportionate organisational measures based on an all-hazards approach to manage cybersecurity related risks	✓ Implement a quality system which, inter alia, describes the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design and product quality	✓ Take appropriate organizational measures to ensure that the use of high-risk AI systems is in accordance with the instructions for the use of such system ✓ Ensure the staff has adequate AI literacy ✓ Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support	x <i>Not covered</i>	x <i>Not covered</i>
	 Risk Management & Technical Standards	✓ Establish, implement, document and maintain a risk management system ✓ Design and manufacture medical devices to remove or reduce risks, including residual risks, associated with identified hazard ✓ Set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access	✓ Establish appropriate and proportionate technical and operational measures to manage cybersecurity related risks, e.g.: adopt adequate policies, including business continuity and disaster recovery, third-party and supply chain security; ensure security in network and information systems acquisition, development and maintenance ✓ Adopt basic cyber hygiene practices and cybersecurity training, use of multi-factor authentication or continuous authentication solutions	✓ Ensure that radio equipment complies with essential security requirements	✓ Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for use ✓ Perform a fundamental rights impact assessment (FRIA) for high-risk AI systems before deployment ✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers. If the use of the high-risk AI system presents a risk, the deployer shall inform the provider or distributor, the relevant market surveillance authority, and suspend the use of that system	✓ May apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorized access to data, including metadata, and to ensure compliance with data sharing obligations and with the agreed contractual terms for making data available	x <i>Not covered</i>

Life Sciences & Healthcare – Use Case (4/5)

Manufacturer of medical imaging equipment

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

		Obligations					
		MDR ¹	NIS2 Directive ²	RED ³	AI Act ⁴	Data Act ⁵	EHDS ⁵
 Vulnerability Management	x <i>Not covered</i>	✓ Establish appropriate and proportionate technical and operational measures to manage vulnerabilities and report them to the national CSIRT and, where needed, to service recipients ✓ Take into account vulnerabilities specific to direct suppliers and service providers and the overall quality of their products and cybersecurity practices	x <i>Not covered</i>	x <i>Not covered</i>	x <i>Not covered</i>	x <i>Not covered</i>	
	x <i>Not covered</i>	✓ Establish appropriate and proportionate technical and operational measures for incident handling ✓ Establish business continuity measures, such as backup management and disaster recovery, and crisis management ✓ Notify the national CSIRT, or competent authority, of any incident that has a significant impact on the provision of the operator's services	x <i>Not covered</i>	✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers within their post-market monitoring activities, including data regarding any discovered serious incident ✓ Inform first the provider, and then the importer or distributor and the relevant market surveillance authorities in case of a serious incident as defined in Article 3(49)	✓ In case of emergencies and major disasters, such as major cybersecurity incidents, data holders shall make data available to public sector bodies, the Commission, the European Central Bank or Union bodies upon their request	✓ Notify the market surveillance authorities of any incident involving an EHR system and the corrective action taken or envisaged by the manufacturer, without prejudice to incident notification requirements under NIS2 Directive ✓ Comply with data breach notifications under the GDPR	

Life Sciences & Healthcare – Use Case (5/5)

Manufacturer of medical imaging equipment

Legend Cybersecurity AI & Data Platform Economy Digital Finance Digital Identity

Obligations					
MDR ¹	NIS2 Directive ²	RED ³	AI Act ⁴	Data Act ⁵	EHDS ⁵
ICT Security Compliance & Certification x Not covered	May be required to use IT/OT products, services and processes, developed by the operator or procured from third parties, that are certified under European cybersecurity certification schemes adopted under the Cybersecurity Act, in order to demonstrate compliance with cybersecurity risk management measures	Ensure that radio equipment comply with essential requirements set out in Article 3, RED and Delegate Regulation 2022/30 Provide the Member States and the Commission with information on the compliance of intended combinations of radio equipment and software resulting from a conformity assessment in the form of a statement of compliance (EU declaration of conformity)	Not covered	Not covered	Ensure conformity of the harmonised components of EHR systems and EHR systems as such with the essential requirements and the common specifications Draw up technical documentation to demonstrate compliance Affix the CE marking
Data Governance & Management x Not covered	Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	Radio equipment has to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected	Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system, to the extent the deployer exercises control over the input data Keep the logs, to the extent that they are under the deployer's control, automatically generated by the high-risk AI system for a period appropriate to the intended purpose of the high-risk AI system	Make data available to users or to a party acting on user's behalf easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, if needed, continuously and in real-time Make data available to data recipients in a way that is fair, reasonable and non-discriminatory Make data available to public sector bodies and EU bodies on the basis of exceptional need	Ensure that the harmonised components of EHR systems and products claiming interoperability with EHR systems (i.e., AI systems) comply with the essential requirements for interoperability and for security and for logging Comply with data obligations outlined in the GDPR

Manufacturing & Consumer – Use Case 1 (1/5)

The Manufacturing & Consumer use case 1 provides an illustrative snapshot of how an automotive supplier, that produces and sells smart and/or data-driven aftermarket components, is impacted by the identified EU digital and cyber legislation and is based on a set of assumptions that may not account for all possible scenarios

Sector



Manufacturing & Consumer. This sector includes public and private entities operating in the following industries: manufacturing of medical devices, computer, electronic and optical products, electrical equipment, machinery, motor vehicles, trailers and semi-trailers, other transportation equipment, manufacturing of consumer products

Identification of an entity within the sector



Automotive supplier of smart and/or data-driven aftermarket components

Definition of the assumptions to build an illustrative use case

Since each legislation imposes specific requirements on entities based on their roles, it is assumed that the automotive supplier of smart and data-driven aftermarket components, under the selected legislation, acts as:

Assumptions

NIS2 Directive

Important entity

An entity referred to in Annex II “Other Critical Sectors”

RED

Manufacturer

An company that makes radio equipment or has it designed or produced, and then sells or distributes it under their own name or brand

CER Directive

Critical entity

An entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex

AI Act

Provider of a high-risk AI system

An organisation providing or deploying an AI system under its control, unless the AI system is being used for non-professional purposes. This can be done whether they charge for it or offer it for free

Data Act

Data holder

A person or organisation that has the right or responsibility, to use and share data. This can include product or service data that they have gathered or created while providing a service

Manufacturing & Consumer – Use Case 1 (2/5)

Automotive supplier of smart and/or data-driven aftermarket components

Regulatory intersection: How do the EU's cyber and digital laws intersect?

 Governance Measures	 Risk Management & Technical Standards	 Vulnerability Management	 Incident Management	 ICT Security Compliance & Certification	 Data Governance & Management
The analysed legislation requires entities to review their internal security governance systems (e.g., cyber/IT security and physical security convergence based on an all-hazard approach), strengthen accountability of management bodies, and establish clear roles and responsibilities for overseeing and managing ICT-related risks. Being a horizontal legislation, NIS2 Directive introduces a general obligation to set a clear and technology-agnostic risk governance framework, while CER Directive addresses the physical and operational resilience, complementing NIS2 Directive provisions targeting the all-hazard approach. Subject-specific legislation, such as the AI Act introduces vertical requirements covering the use of high-risk AI systems, which shall be managed with proper organisational controls to ensure they are used according to guidelines. While RED requires entities to implement a quality system as well as an organisational structure with regard to design and product quality. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive and CER Directive overall governance obligations.	The analysed legislation requires entities to set up an ICT-related risk management framework, as well as to assess and manage all natural and human-made risks, targeting an all-hazards approach. As a horizontal legislation, NIS2 Directive introduces a broad obligation to set up a comprehensive, documented and regularly updated risk management framework, namely strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks; while CER Directive requires entities to complete a comprehensive risk assessment covering all relevant natural and human-made risks, complementing NIS2 Directive provisions. Under subject-specific legislation, such as the AI Act, AI systems must be incorporated into the ICT risk management framework, with their use documented in policies and integrated into the entity's third-party risk management process. Other subject-specific risk management obligations (e.g., RED, that enforces security standards for radio equipment) constitute further specifications of the overall risk management obligation imposed by NIS2. While the Data Act promotes technical safeguards and access control.	The analysed legislation requires entities to establish structured processes for identifying, assessing and mitigating ICT vulnerabilities as part of their overall risk management framework. Being a horizontal legislation, NIS2 Directive introduces a general obligation to implement appropriate measures and processes to manage ICT system vulnerabilities, such as periodic vulnerability assessment and penetration testing, as well as to record and mitigate such vulnerabilities either directly or with the involvement of ICT providers. Subject-specific legislation, such as the AI Act, introduces vertical requirements for providers to comply with strict monitoring obligations, both ante- and post-market. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive overall governance obligations.	The analysed legislation requires entities to set up appropriate measures for ICT incident reporting and handling. As horizontal legislation, NIS2 Directive and CER outlines measures for the notification of ICT significant incidents to national CSIRTs, or competent authorities, as well as appropriate technical, operational, and security measures to prevent, respond to, and recover from incidents. Subject-specific legislation, such as the AI Act outlines measures for the notification of serious incidents to market surveillance authorities. Moreover, the Data Act adds that, in emergencies or major cybersecurity incidents, data holders must provide relevant data to public authorities or Union bodies upon request. The legislation aims to simplify and streamline reporting procedures by encouraging the establishment of national single-entry points for the fulfillment of reporting requirements.	The analysed legislation requires entities to demonstrate compliance with ICT security requirements. Being a horizontal legislation, NIS2 Directive introduces a general obligation for Member States to require essential and important entities to use ICT products, services, and processes certified under European cybersecurity certification schemes pursuant to Article 49 of Regulation (EU) 2019/881, or, in their absence, to comply with relevant European or international standards. Entities shall oversee the compliance with ICT security requirements by providers as part of their third-party risk management obligations. Subject-specific legislation, such as the RED introduces vertical requirements covering the compliance of radio equipment with essential requirements and the provision of EU declaration of conformity. While the AI Act requires entities to assess and demonstrate compliance with all requirements for high-risk AI systems.	The analysed legislation, without prejudice to the overall compliance with data protection obligations under the GDPR, as per NIS2 Directive, requires entities to comply with additional subject-specific obligations. Data governance is further enhanced under the Data Act. Data should be accessible to users securely, free of charge, in structured, machine-readable formats, and, if needed, in real-time. The AI Act requires deployers to ensure input data is relevant and representative for the high-risk AI system's intended purpose and to retain system-generated logs under their control for an appropriate period. Furthermore, the RED mandates safeguards in radio equipment to protect users' and subscribers' personal data and privacy. Lastly, CER Directive mandates justified background checks for sensitive personnel.

Manufacturing & Consumer – Use Case 1 (3/5)

Automotive supplier of smart and/or data-driven aftermarket components

Legend Cybersecurity AI & Data Platform Economy Digital Finance Digital Identity

Obligations					
	NIS2 Directive ¹	RED ²	CER Directive ³	AI Act ⁴	Data Act ⁵
 Governance Measures	✓ Establish appropriate and proportionate governance measures, i.e. accountability of management bodies for cybersecurity risk management measures ✓ Establish appropriate and proportionate organisational measures based on an all-hazards approach to manage cybersecurity related risks	✓ Implement a quality system which, inter alia, describes the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design and product quality	✓ Adopt proportionate organisational measures i.e., appoint a liaison for communication with authorities ✓ Manage employee security by categorizing personnel with critical roles, enforcing access controls to premises, infrastructure, and sensitive data, conducting background checks, and setting training and qualification standards. Awareness of these measures is promoted among relevant staff through training, informational materials, and exercises	✓ Put in place and document a quality management system, including an accountability framework detailing roles and responsibilities regarding high-risk AI systems ✓ Assign human oversight to natural persons who have the necessary competence, training and authority ✓ Ensure the staff has adequate AI literacy ✓ Enforce the conformity assessment procedure for high-risk AI systems ✓ Register AI systems and themselves in the EU and, if needed, national database	x <i>Not covered</i>
	 Risk Management & Technical Standards	✓ Establish appropriate and proportionate technical and operational measures to manage cybersecurity related risks, e.g., adopt adequate policies, including business continuity and disaster recovery, third-party and supply chain security, ensure security in network and information systems acquisition, development and maintenance ✓ Adopt basic cyber hygiene practices and cybersecurity training, use of multi-factor authentication or continuous authentication solutions	✓ Ensure that radio equipment complies with essential security requirements	✓ Complete a comprehensive risk assessment within nine months of notification and every four years thereafter, covering all relevant natural and human-made risks, including cross-sectoral and cross-border dependencies. Assessments should be based on the Member State risk assessment carried out by the National Competent Authority, and any other relevant source of information	✓ Establish, implement, document, and maintain a risk management system, namely continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, to evaluate risks possibly arising ✓ Establish and document a post-market monitoring system that collects, documents and analyses relevant data on the performance of high-risk AI systems throughout their lifetime, including possible risks

Manufacturing & Consumer – Use Case 1 (4/5)

Automotive supplier of smart and/or data-driven aftermarket components

Legend
 Cybersecurity
AI & Data
Platform Economy
Digital Finance
Digital Identity

Obligations					
	NIS2 Directive ¹	RED ²	CER Directive ³	AI Act ⁴	Data Act ⁵
Vulnerability Management	- Establish appropriate and proportionate technical and operational measures to manage vulnerabilities and report them to the national CSIRT an, where needed, to service recipients - Take into account vulnerabilities specific to direct suppliers and service providers and the overall quality of their products and cybersecurity practices	x <i>Not covered</i>	x <i>Not covered</i>	Implement measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set, or pre-trained components used in training, inputs designed to cause the AI model to make a mistake, confidentiality attacks or model flaws	x <i>Not covered</i>
Incident Management	- Establish appropriate and proportionate technical and operational measures for incident handling - Establish business continuity measures, such as backup management and disaster recovery, and crisis management - Notify the national CSIRT, or competent authority, of any incident that has a significant impact on the provision of the operator's services	x <i>Not covered</i>	- Adopt proportionate technical and security measures to prevent, respond to, and recover from incidents, including employee security and awareness - Notify authorities of significant service disruptions within 24 hours and provide detailed reports within a month. Incidents affecting six or more Member States must be reported to the Commission. Reports should include all relevant details without increasing the entity's liability	Notify the market surveillance authorities of the occurrence of serious incidents that directly or indirectly leads to the death of, or serious harm to, a person, a serious disruption of the management or operation of critical infrastructure, a violation of fundamental rights	In case of emergencies and major disasters, such as major cybersecurity incidents, data holders shall make data available to public sector bodies, the Commission, the European Central Bank or Union bodies upon their request

Manufacturing & Consumer – Use Case 1 (5/5)

Automotive supplier of smart and/or data-driven aftermarket components

Legend Cybersecurity AI & Data Platform Economy Digital Finance Digital Identity

Obligations					
NIS2 Directive ¹		RED ²	CER Directive ³	AI Act ⁴	Data Act ⁵
ICT Security Compliance & Certification	✓ May be required to use IT/OT products, services and processes, developed by the operator or procured from third parties, that are certified under European cybersecurity certification schemes adopted under the Cybersecurity Act, in order to demonstrate compliance with cybersecurity risk management measures	✓ Ensure that radio equipment comply with essential requirements set out in Article 3, RED and Delegate Regulation 2022/30 ✓ Provide the Member States and the Commission with information on the compliance of intended combinations of radio equipment and software resulting from a conformity assessment in the form of a statement of compliance (EU declaration of conformity)	x <i>Not covered</i>	✓ Perform a conformity assessment to demonstrate compliance with all requirements for high-risk AI systems, including cybersecurity requirements ✓ Draw up technical documentation to demonstrate compliance ✓ Affix the CE marking	x <i>Not covered</i>
	✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	✓ Radio equipment has to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected	✓ Request justified background checks for individuals in sensitive roles or with authorised access, complying with national and EU laws and limited to necessary security risk assessments. Checks verify identity and criminal records, usually completed within 10 working days ✓ Ensure that information exchange is limited, relevant, and proportionate, to protect sensitive data	✓ Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system ✓ Comply with obligation to carry out a data protection impact assessment as set out by Regulation 2016/679 (GDPR)	✓ Make data available to users or to a party acting on user's behalf easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, if needed, continuously and in real-time ✓ Make data available to data recipients in a way that is fair, reasonable and non-discriminatory ✓ Make data available to public sector bodies and EU bodies on the basis of exceptional need

Manufacturing & Consumer – Use Case 2 (1/5)

The Manufacturing & Consumer use case 2 provides an illustrative snapshot of how a manufacturer that produces and sells Augmented Reality (AR) and Virtual Reality (VR) Headsets, is impacted by the identified EU digital and cyber legislation and is based on a set of assumptions that may not account for all possible scenarios

Sector

Entity

Assumptions

Manufacturing & Consumer. This sector includes public and private entities operating in the following industries: manufacturing of medical devices, computer, electronic and optical products, electrical equipment, machinery, motor vehicles, trailers and semi-trailers, other transportation equipment, manufacturing of consumer products

Identification of an entity within the sector



Manufacturer of Augmented Reality (AR) and Virtual Reality (VR) Headsets

Definition of the assumptions to build an illustrative use case

Since each legislation imposes specific requirements on entities based on their roles, it is assumed that a Manufacturer of Augmented Reality (AR) and Virtual Reality (VR) Headsets, under the selected legislation, acts as:

CRA	NIS2 Directive	Machinery	RED	AI Act	Data Act
Manufacturer	Important entity	Manufacturer	Manufacturer	Deployer of a high-risk AI system	Data holder
An entity that creates or produces products with digital components, or has them made, and then sells or distributes them under their own name or brand, whether for payment, profit or for free	An entity referred to in Annex II “Other Critical Sectors”	An entity that designs, produces and provides with hardware products that qualify as machinery or partly completed machinery	Any person or company that makes radio equipment or has it designed or produced and then sells or distributes it under their own name or brand	An organisation providing or deploying an AI system under its control, unless the AI system is being used for non-professional purposes. This can be done whether they charge for it or offer it for free	A person or organisation that has the right or responsibility, to use and share data. This can include product or service data that they have gathered or created while providing a service

Manufacturing & Consumer – Use Case 2 (2/5)

Augmented Reality (AR) and Virtual Reality (VR) Headsets Manufacturer

Regulatory intersection: How do the EU's cyber and digital laws intersect?

 Governance Measures	 Risk Management & Technical Standards	 Vulnerability Management	 Incident Management	 ICT Security Compliance & Certification	 Data Governance & Management
The analysed legislation requires entities to review their internal security governance systems (e.g., cyber/IT security and physical security convergence based on an all-hazard approach), strengthen accountability of management bodies, and establish clear roles and responsibilities for overseeing and managing ICT-related risks. Being a horizontal legislation, NIS2 Directive introduces a general obligation to set a clear and technology-agnostic risk governance framework. Subject-specific legislation, such as the AI Act introduces vertical requirements covering the use of high-risk AI systems, which shall be managed with proper organisational controls to ensure they are used according to guidelines. While RED requires entities to implement a quality system as well as an organisational structure with regard to design and product quality, the CRA integrates requirements for vulnerability handling of products with digital elements. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive overall governance obligations.	The analysed legislation requires entities to set up an ICT-related risk management framework. As a horizontal legislation, NIS2 Directive introduces a broad obligation to set up a comprehensive, documented and regularly updated risk management framework, namely strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks. Under subject-specific legislation, such as the AI Act, AI systems must be incorporated into the ICT risk management framework, with their use documented in policies and integrated into the entity's third-party risk management process. Other subject-specific risk management obligations, with specific regard to essential requirements of products with digital elements, the CRA applies to radio equipment and machinery products in scope of the RED Directive (and Delegated Regulation) and Machinery Regulation. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive overall risk management obligations.	The analysed legislation requires entities to establish structured processes for identifying, assessing and mitigating ICT vulnerabilities as part of their overall risk management framework. Being a horizontal legislation, NIS2 Directive introduces a general obligation to implement appropriate measures and processes to manage ICT system vulnerabilities, such as periodic vulnerability assessment and penetration testing, as well as to record and mitigate such vulnerabilities either directly or with the involvement of ICT providers. Subject-specific legislation, such as the CRA, introduces vertical requirements covering reporting obligations, requiring Member States to provide single entry points at national level to alleviate administrative burden on entities. Obligations under the CRA are strictly complementary to the fulfilment of NIS2. Therefore, compliance with the former contributes to the overall compliance of the latter.	The analysed legislation requires entities to set up appropriate measures for ICT incident reporting and handling. As horizontal legislation, NIS2 Directive outlines measures for the notification of ICT significant incidents to national CSIRTs, or competent authorities, as well as appropriate technical, operational, and security measures to prevent, respond to, and recover from incidents. Regarding subject-specific legislation, the CRA cover product-specific obligations and notification duties, while AI Act outlines measures for the notification of serious incidents to market surveillance authorities. With regard to NIS2 and CRA, Member States expected to provide single entry points at national level to alleviate administrative burden. The AI Act requires entities to notify market surveillance authorities of serious incidents. However, it is to be considered that possibly such authorities will coincide with the single-entry points designated under NIS2, in order to streamline reporting obligations. Finally, the Data Act adds that, in emergencies or major cybersecurity incidents, data holders must provide relevant data to public authorities or Union bodies upon request.	The analysed legislation requires entities to demonstrate compliance with ICT security requirements. Being a horizontal legislation, NIS2 Directive introduces a general obligation for Member States to require essential and important entities to use ICT products, services, and processes certified under European cybersecurity certification schemes pursuant to Article 49 of Regulation (EU) 2019/881, or, in their absence, to comply with relevant European or international standards. Entities shall oversee the compliance with ICT security requirements by providers as part of their third-party risk management obligations. Subject-specific legislation, such as the RED introduces vertical requirements covering the compliance of radio equipment with essential requirements and the provision of EU declaration of conformity.	The analysed legislation, without prejudice to the overall compliance with data protection obligations under the GDPR, as per NIS2 Directive, requires entities to comply with additional subject-specific obligations. Data governance is further enhanced under the Data Act. Data should be accessible to users securely, free of charge, in structured, machine-readable formats, and, if needed, in real-time. The AI Act requires deployers to ensure input data is relevant and representative for the high-risk AI system's intended purpose and to retain system-generated logs under their control for an appropriate period. Furthermore, the RED mandates safeguards in radio equipment to protect users' and subscribers' personal data and privacy. Lastly, the CRA requires safeguarding data confidentiality, integrity, and availability, enabling users to securely and permanently delete their data and settings, and ensuring data portability.

Manufacturing & Consumer – Use Case 2 (3/5)

Augmented Reality (AR) and Virtual Reality (VR) Headsets Manufacturer

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations						
	CRA ¹	NIS2 Directive ²	Machinery ³	RED ⁴	AI Act ⁵	Data Act ⁵
 Governance Measures	✓ Establish and document a quality system that describes, inter alia, the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling of a product with digital elements	✓ Establish appropriate and proportionate governance measures, i.e. accountability of management bodies for cybersecurity risk management measures ✓ Establish appropriate and proportionate organizational measures based on an all-hazards approach to manage cybersecurity related risks	x <i>Not covered</i>	✓ Implement a quality system which, inter alia, describes the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design and product quality	✓ Take appropriate organizational measures to ensure that the use of high-risk AI systems is in accordance with the instructions for the use of such system ✓ Ensure the staff has adequate AI literacy ✓ Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support	x <i>Not covered</i>
	 Risk Management & Technical Standards	✓ Ensure that the product with digital elements has been designed, developed and produced in accordance with the essential cybersecurity requirements, of both products and processes, i.e. undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment during the product's lifecycle	✓ Establish appropriate and proportionate technical and operational measures to manage cybersecurity related risks, e.g., adopt adequate policies, including business continuity and disaster recovery, third-party and supply chain security, ensure security in network and information systems acquisition, development and maintenance ✓ Adopt basic cyber hygiene practices and cybersecurity training, use of multi-factor authentication or continuous authentication solutions	✓ Ensure machinery meets health and safety standards, complete conformity assessments, and keep documentation for 10 years ✓ Possess clear identification, contact details, and user instructions for the machinery ✓ Present immediate corrective action and notification to authorities for non-compliant products. Manufacturers must cooperate with authorities upon request	✓ Ensure that radio equipment complies with essential security requirements	✓ Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for use ✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers. If the use of the high-risk AI system presents a risk, the deployer shall inform the provider or distributor, the relevant market surveillance authority, and suspend the use of that system

Manufacturing & Consumer – Use Case 2 (4/5)

Augmented Reality (AR) and Virtual Reality (VR) Headsets Manufacturer

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations						
	CRA ¹	NIS2 Directive ²	Machinery ³	RED ⁴	AI Act ⁵	Data Act ⁵
Vulnerability Management	- Ensure that the product with digital elements has been designed, developed and produced in accordance with vulnerability handling requirements, i.e. establish appropriate vulnerability disclosure policies - Notify any actively exploited vulnerability contained in the product with digital elements to the national CSIRT designated as coordinator and to ENISA via the single reporting platform	- Establish appropriate and proportionate technical and operational measures to manage vulnerabilities and report them to the national CSIRT an, where needed, to service recipients - Take into account vulnerabilities specific to direct suppliers and service providers and the overall quality of their products and cybersecurity practices	x <i>Not covered</i>	x <i>Not covered</i>	x <i>Not covered</i>	x <i>Not covered</i>
Incident Management	- Ensure that the product with digital elements has been designed, developed and produced in accordance with essential cybersecurity requirements to prevent incidents and minimize their impact - Notify any severe incident having an impact on the security of the product with digital elements to the CSIRT designated as coordinator and to ENISA via the single reporting platform	- Establish appropriate and proportionate technical and operational measures for incident handling - Establish business continuity measures, such as backup management and disaster recovery, and crisis management - Notify the national CSIRT, or competent authority, of any incident that has a significant impact on the provision of the operator's services	x <i>Not covered</i>	x <i>Not covered</i>	- Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system, to the extent the deployer exercises control over the input data Keep the logs, to the extent that they are under the deployer's control, automatically generated by the high-risk AI system for a period appropriate to the intended purpose of the high-risk AI system	In case of emergencies and major disasters, such as major cybersecurity incidents, data holders shall make data available to public sector bodies, the Commission or Union bodies upon their request

Manufacturing & Consumer – Use Case 2 (5/5)

Augmented Reality (AR) and Virtual Reality (VR) Headsets Manufacturer

Legend Cybersecurity AI & Data Platform Economy Digital Finance Digital Identity

Obligations						
	CRA ¹	NIS2 Directive ²	Machinery ³	RED ⁴	AI Act ⁵	Data Act ⁵
ICT Security Compliance & Certification	✓ Perform a cybersecurity conformity assessment of products and processes to demonstrate compliance with essential cybersecurity requirements ✓ Draw up technical documentation to demonstrate compliance ✓ Affix the CE marking ✓ Identify “important” or “critical” products with digital elements that are subject to additional controls and conformity assessment procedures	✓ <i>May</i> be required to use IT/OT products, services and processes, developed by the operator or procured from third parties, that are certified under European cybersecurity certification schemes adopted under the Cybersecurity Act, in order to demonstrate compliance with cybersecurity risk management measures	x <i>Not covered</i>	✓ Ensure that radio equipment comply with essential requirements set out in Article 3, RED and Delegate Regulation 2022/30 ✓ Provide the Member States and the Commission with information on the compliance of intended combinations of radio equipment and software resulting from a conformity assessment in the form of a statement of compliance (EU declaration of conformity)	x <i>Not covered</i>	x <i>Not covered</i>
	✓ Safeguard the Confidentiality, Integrity and Availability (CIA) of processed data ✓ Ensure the possibility for users to securely and easily remove on a permanent basis all data and settings ✓ Ensure data portability	✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	x <i>Not covered</i>	✓ Radio equipment has to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected	✓ Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system, to the extent the deployer exercises control over the input data ✓ Keep the logs, to the extent that they are under the deployer’s control, automatically generated by the high-risk AI system for a period appropriate to the intended purpose of the high-risk AI system	✓ Make data available to users or to a party acting on user’s behalf easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, if needed, continuously and in real-time ✓ Make data available to data recipients in a way that is fair, reasonable and non-discriminatory ✓ Make data available to public sector bodies and EU bodies on the basis of exceptional need

Technology, Media & Telecommunications – Use Case 1 (1/5)

The Technology, Media & Telecommunications use case 1 provides an illustrative snapshot of how a cloud service provider is impacted by the identified EU digital and cybersecurity legislation and is based on a set of assumptions that may not account for all possible scenarios

Sector

Entity

Assumptions

Technology, Media & Telecommunications. This sector includes public and private entities operating in the following industries: **digital infrastructure services, ICT service management, intermediary services, core platform services, qualified / non-qualified trust services, telecommunications, network connectivity**

Identification of an entity within the sector



Cloud Computing Service Provider

Definition of the assumptions to build an illustrative use case



Since each legislation imposes specific requirements on entities based on their roles, it is assumed that the Cloud Computing Service Provider, under the selected legislation, acts as:

NIS2 Directive	Space Act	AI Act	Data Act	e-Evidence Regulation	DSA
Essential entity An entity referred to in Annex I “Sectors of High Criticality,” which exceeds the ceilings for medium-sized enterprises	Space Operator An entity that offers cloud-based services supporting space-related activities, infrastructure, or data within the European Union	Deployer of a high-risk AI system An organisation providing or deploying an AI system under its control, unless the AI system is being used for non-professional purposes. This can be done whether they charge for it or offer it for free	Data holder An organisation that has the right or responsibility, to use and share data. This can include product or service data that they have gathered or created while providing a service	Provider holding e-Evidence An entity that stores, processes, or manages electronic data within the European Union that may be subject to law enforcement requests for criminal investigations or judicial proceedings	Hosting Service Provider An entity designated Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) under DSA supervised by the Commission

Technology, Media & Telecommunications – Use Case 1 (2/5)

Cloud Computing Service Provider



Back to slide 25 ↗

Regulatory intersection: How do the EU's cyber and digital laws intersect?



Governance Measures

The analysed legislation requires entities to **review their internal security governance systems** (e.g., cyber/IT security and physical security convergence based on an all-hazard approach), strengthen **accountability of management bodies**, and establish clear **roles and responsibilities** for overseeing and managing ICT-related risks. Being a horizontal legislation, **NIS2 Directive** introduces a general obligation to set a **clear and technology-agnostic risk governance framework**.

Subject-specific legislation, such as the **AI Act** introduces vertical requirements covering the use of **high-risk AI systems**, which shall be managed with **proper organisational controls** to ensure they are used according to guidelines. While **e-Evidence Regulation** requires the establishment of internal policies, as well as **roles and responsibilities** to manage **judicial orders**; the **Space Act** mandates **cooperation with national bodies** and environmental reporting, respecting **national security**. Therefore, **compliance** to subject-specific legislation **contributes** to the fulfilment of **NIS2 Directive overall governance obligations**.



Risk Management & Technical Standards

The analysed legislation requires entities to set up an **ICT-related risk management framework**.

As a horizontal legislation, **NIS2 Directive** introduces a broad obligation to set up a **comprehensive, documented and regularly updated risk management framework**, including strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks. Under subject-specific legislation, such as the **AI Act**, **AI systems** must be incorporated into the ICT risk management framework, documented in policies, and integrated into third-party risk management processes like supply chain mapping and contract review.

Other **subject-specific risk management obligations** (e.g., under the **Space Act**, **e-Evidence Regulation** and **DSA**) complement the risk management obligations imposed by **NIS2 Directive**.

While the **Data Act** promotes technical safeguards for data integrity and access control in data sharing.

Therefore, **compliance** to subject-specific legislation **contributes** to the fulfilment of **NIS2 Directive overall risk management obligations**.



Vulnerability Management

The analysed legislation requires entities to establish **structured processes** for **identifying, assessing and mitigating ICT vulnerabilities** as part of their overall risk management framework.

Being a horizontal legislation, **NIS2 Directive** introduces a general obligation to implement **appropriate measures** and processes to **manage ICT system vulnerabilities**, such as **periodic vulnerability assessment and penetration testing**, as well as to **record and mitigate** such vulnerabilities either directly or with the involvement of ICT providers. For **AI systems**, deployers may not directly test the system's but instead manage its security through **third-party risk management**.

Subject-specific legislation, such as the **e-Evidence Regulation** and the **DSA** introduce **vertical requirements** covering the implementation of **security measures and safeguards**, and the establishment of **reporting and escalation processes**. While the **Space Act** requires entities to **monitor for anomalies, secure systems** and manage **supply chain risks**.



Incident Management

The analysed legislation requires entities to set up appropriate measures for **ICT incident reporting and handling**.

As horizontal legislation, **NIS2 Directive** outlines measures for the notification of **ICT significant incidents** to national CSIRTs, or competent authorities.

Subject-specific legislation, such as **Space Act**, **AI Act**, **Data Act**, **e-Evidence Regulation** and **DSA**, reinforce incident management by mandating **timely reporting**, **structured response procedures**, and **effective communication strategies**, emphasising accountability through documentation and cooperation with authorities.

Under **NIS2 Directive**, significant incidents are reported to **national CSIRTs** or **competent authorities**, while the **AI Act** mandates notification of serious AI-related incidents to **market surveillance authorities**.

Both legislations aims to **simplify and streamline reporting procedures** by encouraging the establishment of **national single-entry points** for the fulfilment of reporting requirements.



ICT Security Compliance & Certification

The analysed legislation requires entities to **demonstrate compliance with ICT security requirements**.

Being a horizontal legislation, **NIS2 Directive** introduces a general obligation for Member States to **require essential and important entities** to use ICT products, services, and processes certified under **European cybersecurity certification schemes** pursuant to Article 49 of Regulation (EU) 2019/881, or, in their absence, to comply with relevant European or international standards. Entities shall **oversee the compliance with ICT security requirements by providers** as part of their third-party risk management obligations.

Subject-specific legislation, such as the **e-Evidence Regulation** and the **DSA** sets **vertical requirements** for **secure ICT systems, compliant communication channels**, approved data exchange, and accountability through independent compliance audits. While the **Space Act** mandates certified **cryptographic products**, voluntary cyber threat information sharing, and adherence to space-specific cybersecurity rules that may override general **NIS2 Directive** provisions.



Data Governance & Management

The analysed legislation, without prejudice to the overall compliance with **data protection obligations under the GDPR**, as per **NIS2 Directive**, requires entities to comply with **additional subject-specific obligations**. The **Space Act** requires data for registration in the **Union Register of Space Objects** with e-certificates confirming compliance. Regarding **AI Act**, it requires deployers to ensure input data is relevant and representative for the high-risk AI system's intended purpose and to retain system-generated logs under their control for an appropriate period. **Data governance** is further enhanced under the **Data Act**. Data should be accessible to users securely, free of charge, in structured, machine-readable formats, and, if needed, in real-time.

Furthermore, the **e-Evidence Regulation** enforces **strict access controls**, data minimisation, timely preservation and disclosure, confidentiality, and record-keeping to **support accountability**.

Lastly, the **DSA** requires entities to provide **controlled access to data** for vetted researchers to **analyse systemic risks**.

Technology, Media & Telecommunications – Use Case 1 (3/5)

Cloud Computing Service Provider



Back to slide 25

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations

	NIS2 Directive ¹	Space Act ²	AI Act ³	Data Act ⁴	e-Evidence Regulation ⁵	DSA ⁵
 Governance Measures	✓ Establish appropriate and proportionate governance measures, i.e., accountability of management bodies for cybersecurity risk management measures ✓ Establish appropriate and proportionate organisational measures based on an all-hazards approach to manage cybersecurity related risks	✓ Cooperate with national authorities, the EU Agency for the Space Programme (EUSPA), and participate in the Union Space Resilience Network (EUSRN) ✓ Respect national security responsibilities of Member States. ✓ Calculation, verification, and reporting of environmental footprint with lifecycle data submitted to the EU database	✓ Take appropriate organizational measures to ensure that the use of high-risk AI systems is in accordance with the instructions for the use of such system ✓ Ensure the staff has adequate AI literacy ✓ Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support	x <i>Not covered</i>	✓ Establish internal policies ensuring compliance with judicial orders, recognising only competent judicial authorities can issue or validate orders ✓ Define clear roles for managing orders, with oversight by compliance/legal functions ensuring necessity, proportionality, and respect for rights ✓ Maintain confidentiality controls and timely notification procedures internally ✓ Coordinate communication with judicial authorities and designated representatives	✓ Define, oversee and be accountable for the implementation of the provider's governance arrangements that ensure the independence of the compliance function, including the division of responsibilities within the organisation, the prevention of conflicts of interest, and sound management of systemic risk
 Risk Management & Technical Standards	✓ Establish appropriate and proportionate technical and operational measures to manage cybersecurity related risks, e.g., adopt adequate policies, including business continuity and disaster recovery, third-party and supply chain security, ensure security in network and information systems acquisition, development and maintenance ✓ Adopt basic cyber hygiene practices and cybersecurity training, use of multi-factor authentication or continuous authentication solutions	✓ Implement comprehensive, proportionate risk management covering all lifecycle phases of space missions ✓ Maintain an information security management system aligned with relevant standards ✓ Conduct continuous risk assessments and apply technical compliance verified by qualified technical bodies ✓ Adhere to EU harmonised standards and common specifications for ground infrastructure	✓ Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for use ✓ Perform a fundamental rights impact assessment (FRIA) for high-risk AI systems before deployment ✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers. If the use of the high-risk AI system presents a risk, the deployer shall inform the provider or distributor, the relevant market surveillance authority, and suspend the use of that system	✓ <i>May</i> apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorized access to data, including metadata, and to ensure compliance with data sharing obligations and with the agreed contractual terms for making data available	✓ Assess and manage legal, operational, and reputational risks from handling electronic evidence requests ✓ Limit data access strictly to categories specified in orders ✓ Prepare for expedited handling of emergency orders. ✓ Ensure ICT systems support secure, interoperable communication	✓ Carry out risk assessments at least once every year thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified

Technology, Media & Telecommunications – Use Case 1 (4/5)

Cloud Computing Service Provider



[Back to slide 25](#)

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations

	NIS2 Directive ¹	Space Act ²	AI Act ³	Data Act ⁴	e-Evidence Regulation ⁵	DSA ⁵
Vulnerability Management	✓ Establish appropriate and proportionate technical and operational measures to manage vulnerabilities and report them to the national CSIRT an, where needed, to service recipients ✓ Take into account vulnerabilities specific to direct suppliers and service providers and the overall quality of their products and cybersecurity practices	✓ Continuously monitor and detect anomalies and incidents; regularly test detection systems ✓ Implement strong cryptography and key management for telemetry and telecommands. ✓ Manage supply chain risks with controls on software and hardware integrity. ✓ Ensure backup systems and redundancies to support rapid recovery. ✓ Conduct regular penetration testing and provide ongoing staff training	x <i>Not covered</i>	x <i>Not covered</i>	✓ Implement technical and organisational safeguards for data confidentiality, integrity, and availability ✓ Establish processes for reporting and escalating issues with order execution	✓ Implement appropriate technical and organisational security measures to protect service integrity. ✓ Report serious security incidents promptly to relevant authorities
Incident Management	✓ Establish appropriate and proportionate technical and operational measures for incident handling ✓ Establish business continuity measures, such as backup management and disaster recovery, and crisis management ✓ Notify the national CSIRT, or competent authority, of any incident that has a significant impact on the provision of the operator's services	✓ Prompt reporting of significant incidents to competent authorities and EUSPA, aligned with NIS2 and CER Directives ✓ Define Incident handling processes and business continuity plans for effective response and recovery ✓ Establish crisis communication strategies for internal and external stakeholders	✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers within their post-market monitoring activities, including data regarding any discovered serious incident ✓ Inform first the provider, and then the importer or distributor and the relevant market surveillance authorities in case of a serious incident as defined in Article 3(49)	✓ In case of emergencies and major disasters, such as major cybersecurity incidents, data holders shall make data available to public sector bodies, the Commission, the European Central Bank or Union bodies upon their request	✓ Define procedures for incident response and documentation related to orders ✓ Keep records to support accountability and audits	✓ Develop procedures for rapid detection, removal, and response to illegal content and incidents. ✓ Cooperate with authorities by providing necessary information for investigations

Technology, Media & Telecommunications – Use Case 1 (5/5)

Cloud Computing Service Provider



Back to slide 25 ↗

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations

	NIS2 Directive ¹	Space Act ²	AI Act ³	Data Act ⁴	e-Evidence Regulation ⁵	DSA ⁵
ICT Security Compliance & Certification	✓ May be required to use IT/OT products, services and processes, developed by the operator or procured from third parties, that are certified under European cybersecurity certification schemes adopted under the Cybersecurity Act, in order to demonstrate compliance with cybersecurity risk management measures	✓ Use of certified cryptographic products and voluntary cyber threat information sharing ✓ Compliance with tailored cybersecurity rules specific to space infrastructure, overriding general NIS2 Directive rules where applicable	x <i>Not covered</i>	x <i>Not covered</i>	✓ Ensure ICT infrastructure meets cybersecurity standards as per implementing acts ✓ Use secure communication channels compliant with eIDAS ✓ Integrate with decentralised or approved secure IT systems for data exchange	✓ Be accountable, through independent auditing, for their compliance with the obligations laid down by this Regulation and, where relevant, any complementary commitments undertaken pursuant to codes of conduct and crises protocols
Data Governance & Management	✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	✓ Provision of detailed data for registration in the Union Register of Space Objects (URSO) and obtaining e-certificates confirming compliance ✓ Ensure confidentiality and data protection in information exchanges ✓ Provision of detailed data for registration in the Union Register of Space Objects (URSO) and obtaining e-certificates confirming compliance	✓ Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system, to the extent the deployer exercises control over the input data ✓ Keep the logs, to the extent that they are under the deployer's control, automatically generated by the high-risk AI system for a period appropriate to the intended purpose of the high-risk AI system	✓ Make data available to users or to a party acting on user's behalf easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, if needed, continuously and in real-time ✓ Make data available to data recipients in a way that is fair, reasonable and non-discriminatory ✓ Make data available to public sector bodies and EU bodies on the basis of exceptional need	✓ Ensure access to and disclosure of only the data explicitly requested, adhering to principles of data minimisation and purpose limitation ✓ Promptly preserve requested data and produce them within stipulated deadlines to comply with legal requirements ✓ Maintain strict confidentiality of orders and data, with appropriate handling of privileged information; notify data subjects unless legally exempted ✓ Maintain comprehensive records and support monitoring and reporting obligations as mandated by the Regulation	✓ Provide controlled access to data for vetted researchers to analyse systemic risks

Technology, Media & Telecommunications – Use Case 2 (1/5)

The Technology, Media & Telecommunications use case 2 provides an illustrative snapshot of how an Operator of Ground-based Infrastructure supporting the provision of Space-based Services is impacted by the identified EU digital and cyber legislation and is based on a set of assumptions that may not account for all possible scenarios

Sector

Entity

Assumptions

 **Technology, Media & Telecommunications.** This key sector includes public and private entities operating in the following industries: **digital infrastructure services, ICT service management, intermediary services, core platform services, qualified / non-qualified trust services, telecommunications, network connectivity**

Identification of an entity within the sector



Operator of Ground-based Infrastructure supporting the provision of Space-based Services

Definition of the assumptions to build an illustrative use case

Since each legislation imposes specific requirements on entities based on their roles, it is assumed that an operator of ground-based infrastructure supporting the provision of space-based services, under the selected legislation, acts as:

NIS2 Directive	CER Directive	Space Act	AI Act	Data Act	e-Evidence Regulation
Essential entity	Critical entity	Space Operator	Deployer of a high-risk AI system	Data holder	Provider holding e-Evidence
An entity referred to in Annex I “Sectors of High Criticality,” which exceeds the ceilings for medium-sized enterprises	A public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex	A public or private entity that operates the space infrastructure, by carrying out the following space services: spacecraft operator, launch operator, launch site operator and ISOS provider	An organisation providing or deploying an AI system under its control, unless the AI system is being used for non-professional purposes. This can be done whether they charge for it or offer it for free	A person or organisation that has the right or responsibility, to use and share data. This can include product or service data that they have gathered or created while providing a service	An entity that stores, processes, or manages electronic data within the European Union that may be subject to law enforcement requests for criminal investigations or judicial proceedings

Technology, Media & Telecommunications – Use Case 2 (2/5)

Operator of Ground-based Infrastructure supporting the provision of Space-based Services

Regulatory intersection: How do the EU's cyber and digital laws intersect?

 Governance Measures	 Risk Management & Technical Standards	 Vulnerability Management	 Incident Management	 ICT Security Compliance & Certification	 Data Governance & Management
The analysed legislation requires entities to review their internal security governance systems (e.g., cyber/IT security and physical security convergence based on an all-hazard approach), strengthen accountability of management bodies, and establish clear roles and responsibilities for overseeing and managing ICT-related risks. Being a horizontal legislation, NIS2 Directive introduces a general obligation to set a clear and technology-agnostic risk governance framework; while CER Directive addresses the physical and operational resilience. Subject-specific legislation, such as the AI Act introduces vertical requirements covering the use of high-risk AI systems, which shall be managed with proper organisational controls. While e-Evidence Regulation requires the establishment of internal policies, as well as roles and responsibilities to manage judicial orders; the Space Act mandates cooperation with national bodies, environmental reporting and respecting national security. Therefore, compliance to subject-specific legislation contributes to the fulfilment of NIS2 Directive and CER Directive overall governance obligations.	The analysed legislation requires entities to set up an ICT-related risk management framework, as well as to assess and manage all natural and human-made risks, targeting an all-hazards approach. As a horizontal legislation, NIS2 Directive introduces a broad obligation to set up a comprehensive, documented and regularly updated risk management framework, including strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks; while CER Directive requires entities to complete a comprehensive risk assessment covering all relevant natural and human-made risks; therefore, complementing NIS2 Directive provisions. Under subject-specific legislation, such as the AI Act, AI systems must be incorporated into the ICT risk management framework, documented in policies, and integrated into third-party risk management processes. While the Data Act promotes technical safeguards for data integrity and access control in data sharing. The e-Evidence Regulation similarly focuses on risk management related to electronic evidence, data access restrictions, and secure communication.	The analysed legislation requires entities to establish structured processes for identifying, assessing and mitigating ICT vulnerabilities as part of their overall risk management framework. Being a horizontal legislation, NIS2 Directive introduces a general obligation to implement appropriate measures and processes to manage ICT system vulnerabilities, such as periodic vulnerability assessment and penetration testing, as well as to record and mitigate such vulnerabilities either directly or with the involvement of ICT providers. For AI systems, deployers may not directly test the system's but instead manage its security through third-party risk management. Subject-specific legislation, such as the e-Evidence Regulation introduces vertical requirements covering the implementation of safeguards concerning data and the establishment of reporting and escalation processes. While the Space Act requires entities to monitor for anomalies, secure systems and manage supply chain risks.	The analysed legislation requires entities to set up appropriate measures for ICT incident reporting and handling. As horizontal legislation, NIS2 Directive and CER Directive outline measures for the notification of ICT significant incidents to national CSIRTs, or competent authorities. Subject-specific legislation, such as Space Act, AI Act, Data Act, e-Evidence Regulation, reinforce incident management by mandating timely reporting, structured response procedures, and effective communication strategies, emphasising accountability through documentation and cooperation with authorities. Under NIS2 Directive, significant incidents are reported to national CSIRTs or competent authorities, while the AI Act mandates notification of serious AI-related incidents to market surveillance authorities. Both legislations aim to simplify and streamline reporting procedures by encouraging the establishment of national single-entry points for the fulfilment of reporting requirements.	The analysed legislation requires entities to demonstrate compliance with ICT security requirements. Being a horizontal legislation, NIS2 Directive introduces a general obligation for Member States to require essential and important entities to use ICT products, services, and processes certified under European cybersecurity certification schemes pursuant to Article 49 of Regulation (EU) 2019/881, or, in their absence, to comply with relevant European or international standards. Entities shall oversee the compliance with ICT security requirements by providers as part of their third-party risk management obligations. Subject-specific legislation, such as the e-Evidence Regulation introduces vertical requirements covering the implementation of secure ICT infrastructure, eIDAS-compliant communication, and the integration with approved IT systems. While the Space Act mandates certified cryptographic products, voluntary cyber threat information sharing, and adherence to space-specific cybersecurity rules that may override general NIS2 Directive provisions.	The analysed legislation, without prejudice to the overall compliance with data protection obligations under the GDPR, as per NIS2 Directive, requires entities to comply with additional subject-specific obligations. The Space Act requires detailed data for Union Register of Space Objects registration and e-certification, ensuring confidentiality. Data governance is further enhanced under the Data Act. Data should be accessible to users securely, free of charge, in structured, machine-readable formats, and, if needed, in real-time. The AI Act requires deployers to ensure input data is relevant and representative for the high-risk AI system's intended purpose and to retain system-generated logs under their control for an appropriate period. Furthermore, the e-Evidence Regulation enforces strict access controls, data minimisation, timely preservation and disclosure, confidentiality, and record-keeping to support accountability. Lastly, CER Directive mandates justified background checks for sensitive personnel.

Technology, Media & Telecommunications – Use Case 2 (3/5)

Operator of Ground-based Infrastructure supporting the provision of Space-based Services

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations

	NIS2 Directive ¹	CER Directive ²	Space Act ³	AI Act ⁴	Data Act ⁵	e-Evidence Regulation ⁶
Governance Measures	✓ Establish appropriate and proportionate governance measures, i.e., accountability of management bodies for cybersecurity risk management measures ✓ Establish appropriate and proportionate organisational measures based on an all-hazards approach to manage cybersecurity related risks	✓ Adopt proportionate organisational measures i.e., appoint a liaison for communication with authorities ✓ Manage employee security by categorizing personnel with critical roles, enforcing access controls to premises, infrastructure, and sensitive data, conducting background checks, and setting training and qualification standards. ✓ Awareness of these measures is promoted among relevant staff through training, informational materials, and exercises	✓ Cooperate with national authorities, the EU Agency for the Space Programme (EUSPA), and participate in the Union Space Resilience Network (EUSRN) ✓ Respect national security responsibilities of Member States. ✓ Calculation, verification, and reporting of environmental footprint with lifecycle data submitted to the EU database	✓ Take appropriate organizational measures to ensure that the use of high-risk AI systems is in accordance with the instructions for the use of such system ✓ Ensure the staff has adequate AI literacy ✓ Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support	x <i>Not covered</i>	✓ Establish internal policies ensuring compliance with judicial orders, recognising only competent judicial authorities can issue or validate orders ✓ Define clear roles for managing orders, with oversight by compliance/legal functions ensuring necessity, proportionality, and respect for rights ✓ Maintain confidentiality controls and timely notification procedures internally ✓ Coordinate communication with judicial authorities and designated representatives
Risk Management & Technical Standards	✓ Establish appropriate and proportionate technical and operational measures to manage cybersecurity related risks, e.g., adopt adequate policies, including business continuity and disaster recovery, third-party and supply chain security, ensure security in network and information systems acquisition, development and maintenance ✓ Adopt basic cyber hygiene practices and cybersecurity training, use of multi-factor authentication or continuous authentication solutions	✓ Complete a comprehensive risk assessment within nine months of notification and every four years thereafter, covering all relevant natural and human-made risks, including cross-sectoral and cross-border dependencies. Assessments should be based on the Member State risk assessment carried out by the National Competent Authority, and any other relevant source of information	✓ Implement comprehensive, proportionate risk management covering all lifecycle phases of space missions ✓ Maintain an information security management system aligned with relevant standards ✓ Conduct continuous risk assessments and apply technical compliance verified by qualified technical bodies ✓ Adhere to EU harmonised standards and common specifications for ground infrastructure	✓ Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for use ✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers. If the use of the high-risk AI system presents a risk, the deployer shall inform the provider or distributor, the relevant market surveillance authority, and suspend the use of that system	✓ May apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorized access to data, including metadata, and to ensure compliance with data sharing obligations and with the agreed contractual terms for making data available	✓ Assess and manage legal, operational, and reputational risks from handling electronic evidence requests ✓ Limit data access strictly to categories specified in orders ✓ Prepare for expedited handling of emergency orders. ✓ Ensure ICT systems support secure, interoperable communication

Technology, Media & Telecommunications – Use Case 2 (4/5)

Operator of Ground-based Infrastructure supporting the provision of Space-based Services

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations

	NIS2 Directive ¹	CER Directive ²	Space Act ³	AI Act ⁴	Data Act ⁵	e-Evidence Regulation ⁶
Vulnerability Management	✓ Establish appropriate and proportionate technical and operational measures to manage vulnerabilities and report them to the national CSIRT an, where needed, to service recipients ✓ Take into account vulnerabilities specific to direct suppliers and service providers and the overall quality of their products and cybersecurity practices	x <i>Not covered</i>	✓ Continuously monitor and detect anomalies and incidents; regularly test detection systems ✓ Implement strong cryptography and key management for telemetry and telecommands ✓ Manage supply chain risks with controls on software and hardware integrity ✓ Ensure backup systems and redundancies to support rapid recovery ✓ Conduct regular penetration testing and provide ongoing staff training	x <i>Not covered</i>	x <i>Not covered</i>	✓ Implement technical and organisational safeguards for data confidentiality, integrity, and availability ✓ Establish processes for reporting and escalating issues with order execution
Incident Management	✓ Establish appropriate and proportionate technical and operational measures for incident handling ✓ Establish business continuity measures, such as backup management and disaster recovery, and crisis management ✓ Notify the to national CSIRT, or competent authority, of any incident that has a significant impact on the provision of the operator's services	✓ Adopt proportionate technical and security measures to prevent, respond to, and recover from incidents, including employee security and awareness ✓ Notify authorities of significant service disruptions within 24 hours and provide detailed reports within a month. Incidents affecting six or more Member States must be reported to the Commission. Reports should include all relevant details without increasing the entity's liability	✓ Prompt reporting of significant incidents to competent authorities and EUSPA, aligned with NIS2 and CER Directives ✓ Define Incident handling processes and business continuity plans for effective response and recovery ✓ Establish crisis communication strategies for internal and external stakeholders	✓ Monitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers within their post-market monitoring activities, including data regarding any discovered serious incident ✓ Inform first the provider, and then the importer or distributor and the relevant market surveillance authorities in case of a serious incident as defined in Article 3(49)	✓ In case of emergencies and major disasters, such as major cybersecurity incidents, data holders shall make data available to public sector bodies, the Commission or Union bodies upon their request	✓ Define procedures for incident response and documentation related to orders ✓ Keep records to support accountability and audits

Technology, Media & Telecommunications – Use Case 2 (5/5)

Operator of Ground-based Infrastructure supporting the provision of Space-based Services

Legend ● Cybersecurity ● AI & Data ● Platform Economy ● Digital Finance ● Digital Identity

Obligations

	NIS2 Directive ¹	CER Directive ²	Space Act ³	AI Act ⁴	Data Act ⁵	e-Evidence Regulation ⁶
ICT Security Compliance & Certification	✓ May be required to use IT/OT products, services and processes, developed by the operator or procured from third parties, that are certified under European cybersecurity certification schemes adopted under the Cybersecurity Act, in order to demonstrate compliance with cybersecurity risk management measures	x <i>Not covered</i>	✓ Use of certified cryptographic products and voluntary cyber threat information sharing ✓ Compliance with tailored cybersecurity rules specific to space infrastructure, overriding general NIS2 Directive rules where applicable	x <i>Not covered</i>	x <i>Not covered</i>	✓ Ensure ICT infrastructure meets cybersecurity standards as per implementing acts ✓ Use secure communication channels compliant with eIDAS ✓ Integrate with decentralised or approved secure IT systems for data exchange
Data Governance & Management	✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	✓ Request justified background checks for individuals in sensitive roles or with authorised access, complying with national and EU laws and limited to necessary security risk assessments. Checks verify identity and criminal records, usually completed within 10 working days ✓ Ensure that information exchange is limited, relevant, and proportionate, to protect sensitive data	✓ Provision of detailed data for registration in the Union Register of Space Objects (URSO) and obtaining e-certificates confirming compliance ✓ Ensure confidentiality and data protection in information exchanges ✓ Provision of detailed data for registration in the Union Register of Space Objects (URSO) and obtaining e-certificates confirming compliance	✓ Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system, to the extent the deployer exercises control over the input data ✓ Keep the logs, to the extent that they are under the deployer's control, automatically generated by the high-risk AI system for a period appropriate to the intended purpose of the high-risk AI system	✓ Make data available to users or to a party acting on user's behalf easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, if needed, continuously and in real-time ✓ Make data available to data recipients in a way that is fair, reasonable and non-discriminatory ✓ Make data available to public sector bodies and EU bodies on the basis of exceptional need	✓ Ensure access to and disclosure of only the data explicitly requested, adhering to principles of data minimisation and purpose limitation ✓ Promptly preserve requested data and produce them within stipulated deadlines to comply with legal requirements ✓ Maintain strict confidentiality of orders and data, with appropriate handling of privileged information; notify data subjects unless legally exempted ✓ Maintain comprehensive records and support monitoring and reporting obligations as mandated by the Regulation



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



EU 2024-2029 Digital & Cyber Goals



Focus on EU Cyber Defence Innovation



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex

Annex A | References (1/3)

List of published legislation and proposals leveraged to develop the EUPC Digital Playbook

ID	Short Name	Full Name	Link
1	Cybersecurity Resilience Act (CRA)	Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)	https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
2	Cyber Solidarity Act (CSA)	Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)	https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng
3	Critical Entities Resilience Directive (CER)	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC	https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng
4	Network and Information Security Directive 2 (NIS2)	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1712306799442
5	Digital Operational Resilience Act (DORA)	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011	https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
6	Space Act	Proposal for a Regulation of the European Parliament and of the Council on the safety, resilience and sustainability of space activities in the Union	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0335
7	Machinery Regulation	Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC	https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng
8	Radio Equipment Directive (RED) & Amendments	Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC	https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng

Annex A | References (2/3)

List of published legislation and proposals leveraged to develop the EUPC Digital Playbook

ID	Short Name	Full Name	Link
9	Medical Devices Regulation (MDR)	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC	https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng
10	Artificial Intelligence Act (AI Act)	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)	https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
11	Data Act	Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)	https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
12	Data Governance Act (DGA)	Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)	https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng
13	Interoperable Europe Act	Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act).	https://eur-lex.europa.eu/eli/reg/2024/903/oj/eng
14	e-Evidence Regulation	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings	https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng
15	European Health Data Spaces Regulation (EHDS)	Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847	https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng
16	Digital Markets Act (DMA)	Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)	https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

Annex A | References (3/3)

List of published legislation and proposals leveraged to develop the EUPC Digital Playbook

ID	Short Name	Full Name	Link
17	Digital Services Act (DSA)	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)	https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
18	Market in Crypto-Assets Regulation (MiCA)	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937	https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng
19.1	eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng
19.2	European Digital Identity Regulation (EUDI)	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183

Annex B | EUPC Team, Support Team, and Subject Matter Experts (1/2)

EUPC Team



Pablo Zalba
Partner

Deloitte EUPC Managing Director
pzalba@deloitte.es



Edoardo Giglio
Partner

Deloitte EUPC Cyber & Defence Policy Lead
egiglio@deloitte.it



Mosche Orth
Senior Manager

EU Digital Policy
moorth@deloitte.de

Support Team



Biagio Salerno
Director

bsalerno@deloitte.it



Alessia Sposini
Consultant

asposini@deloitte.it



Chiara Ursino
Consultant

cursino@deloitte.it



Daniel Bottolini
Analyst

dbottolini@deloitte.it



Livio Campagna
Analyst

lcampagna@deloitte.it

Annex B | EUPC Team, Support Team, and Subject Matter Experts (2/2)

Subject Matter Experts



Manel Carpio

Partner

Spain

macarpio@deloitte.es



Ian Coppini

Partner

Malta

icoppini@deloitte.com.mt



Ljuba Kerschhofer-Wallner

Partner

Germany

lkerschhoferwallner@deloitte.de



Koen Magnus

Partner

Belgium

kmagnus@deloitte.com



Sebastiaan ter Wee

Partner

Netherlands

sterwee@deloitte.nl



Mathias Vierstraete

Partner

Belgium

mvierstraete@deloitte.com



Titus Aust

Senior Manager

Germany

taust@deloitte.de



Marlieke Bakker

Senior Manager

Netherlands

MaBakker@deloitte.nl



Vanessa Magtang

Senior Manager

Malta

vmagtang@deloitte.com.mt



Henner Jose Truchsess

Senior Manager

Spain

htruchsess@deloitte.es



Julie Van Com

Senior Manager

Belgium

jvancom@deloitte.com



Marja van der Sluis

Senior Consultant

Netherlands

mvandersluis@deloitte.nl



Michaël Dours

Consultant

Belgium

mdours@deloitte.com