



EU Policy Centre Digital Playbook

November 2024





Introduction to the EUPC



Introduction to the EUPC Digital Playbook



Technology Trends and the EU Digital Strategy



EU Digital Legislation and Key Sectors Overview



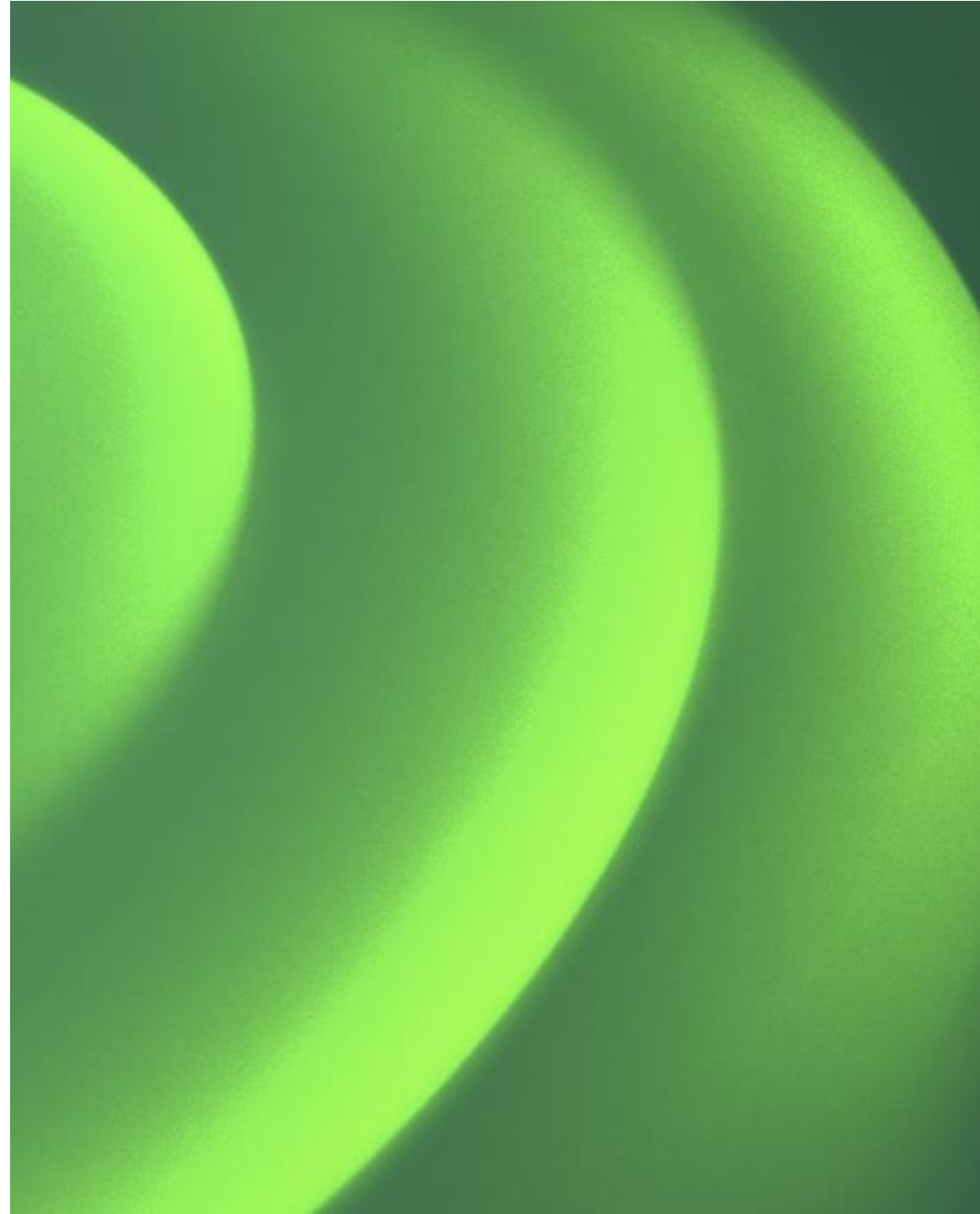
EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex





Introduction to the EUPC



Introduction to the EUPC Digital Playbook



Technology Trends and the EU Digital Strategy



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex

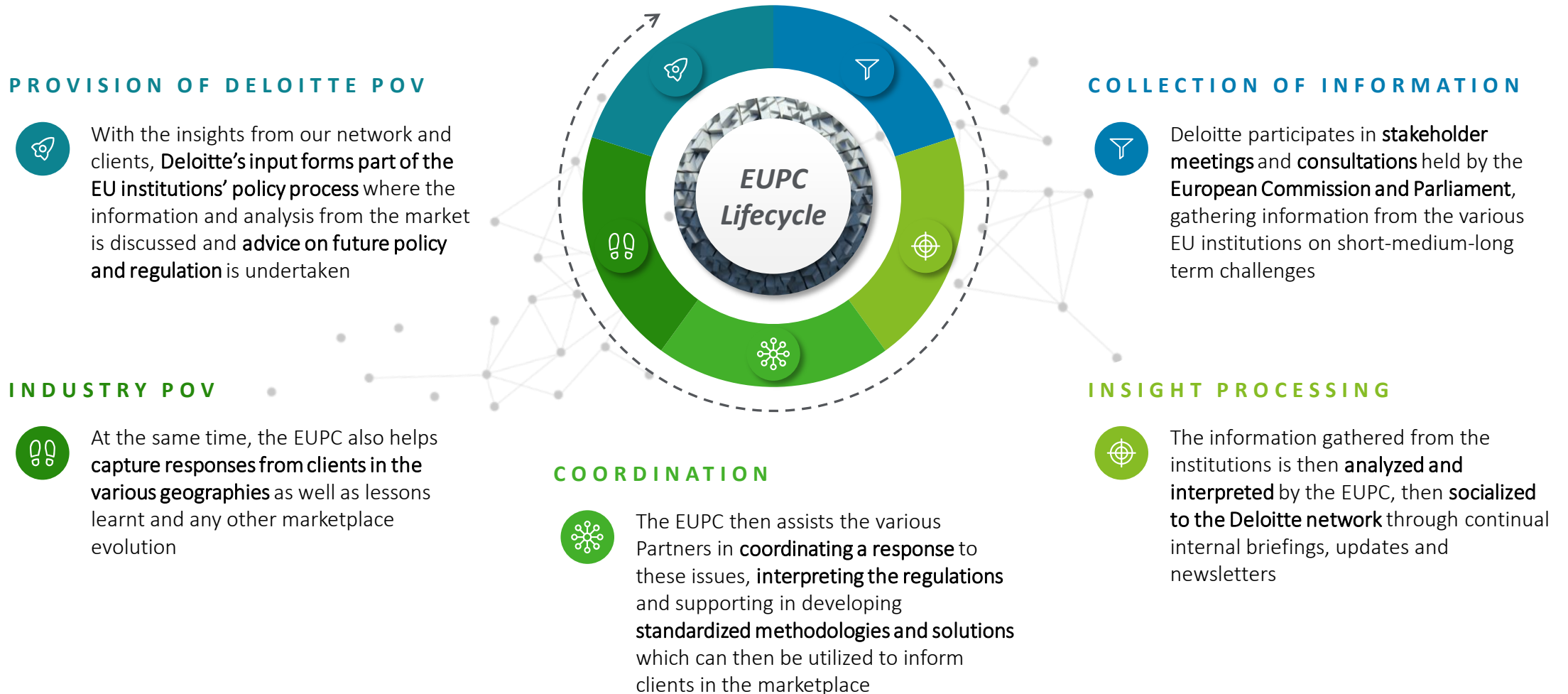
The EU Policy Centre (EUPC)

The EUPC makes Deloitte's insights and research on public policy issues and legislation available to key policy makers and to Deloitte's clients, building relationship between professionals, business leaders, and decision-makers



The EU Policy Centre lifecycle

Among its activities, the EUPC enables a constant flow of information between our network and the institutions, forging relationships and disseminating insights useful to us and our clients



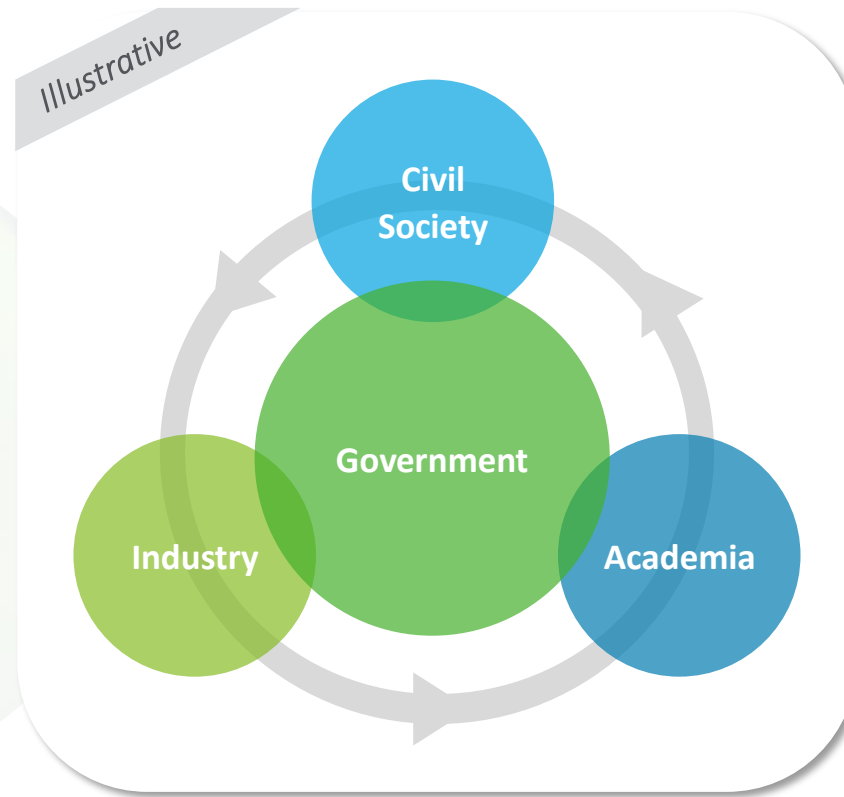
The EU Policy Centre ecosystem approach

To carry out its activities, the EUPC aims to adopt an ecosystem approach, leveraging relationships with different organizations to promote eminence and position Deloitte as a strategic advisor on key topics

EUPC Ecosystem Approach

Ecosystem based approach

Identification of **key organizations**, such as think-tanks, NGOs, universities and private technology companies in different geographic areas, and with which the EUPC can leverage **existing relationships**. Where these relationships do not yet exist, the EUPC takes steps to **create new ones** with the ultimate goal of **establishing a new ecosystem**



Promotion of eminence

Promotion of the EUPC's **eminence and reliability**, building on **Deloitte NSE's network** with the aim of achieving a **strategic advisor** position for EU policy. This is crucial, as **Cyber Diplomacy** is at the heart of the success of many EU initiatives and relies on the participation of external stakeholders



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



Technology Trends and the EU Digital Strategy



EU Digital Legislation and Key Sectors Overview



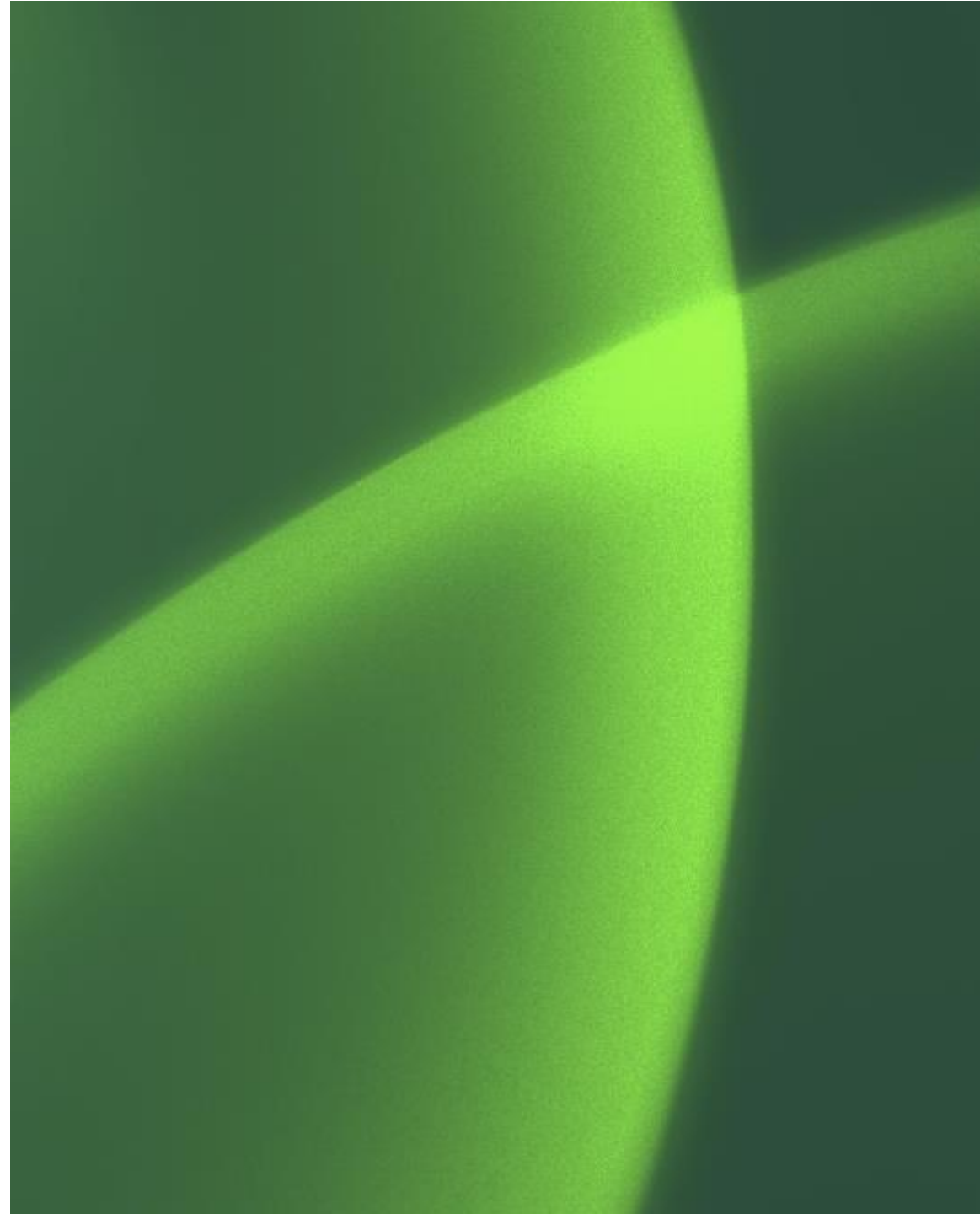
EU Digital Legislation Detail Cards



Key Sectors Use Cases



Annex



Sections of the EUPC Digital Playbook

In light of the increasing complexity of the EU digital and cyber legislative landscape, there is a compelling need to explore the new market opportunities opened by EU legislations and identify intersections and synergies among their requirements

Sections of the EUPC Digital Playbook

Technology Trends and EU Digital Strategy

From slide 10

EU Digital Legislation and Key Sectors overview

From slide 14

EU Digital Legislation Detail Cards

From slide 19

Key Sectors Use Cases

From slide 34

Overview of the technological trends transforming businesses and of the EU strategy guiding legislative advancements in the digital landscape

Overview of analyzed legislations, key sectors and use cases, and mapping of legislations' applicability to the key sectors

Deep-dive on the contents, targets, and regulatory stakeholders of each identified legislation, as well as intersections with other regulations

Deep-dive on use cases for each key sector to facilitate the understanding of the EU digital and cyber legislation's potential application

ILLUSTRATIVE

Emerging technology trends

Emerging technologies are redefining the business landscape by enhancing operational efficiency, driving innovation, and enabling new business models, thus unlocking opportunities to transform both practices and industries and gain competitive advantages. Their rapid adoption entails the need for robust regulations to harness benefits, mitigate risks, and enhance public trust.

EMERGING TECHNOLOGIES TRENDS...

COGNITIVE TECHNOLOGIES	DIGITAL REALITY	AMBIENT EXPERIENCES	AUTONOMOUS VEHICLES	QUANTUM COMPUTING	DISTRIBUTED LEDGER TECHNOLOGY	ROBOTICS
Involving general and specific AI, machine learning, deep learning, etc. to improve processing and data analysis.	Involving augmented reality (AR), virtual reality (VR), and mixed reality (MR) to create immersive experiences.	Involving sensors, smart devices, and data analytics to create seamless and personalized experiences.	Involving a mix of sensors, actuators, and control systems to enable vehicles to operate autonomously.	Involving quantum bits (qubits) and quantum algorithms to solve complex problems faster than classical computers.	Involving blockchain, smart contracts, and decentralized applications to create secure and transparent digital ecosystems.	Involving robots with artificial intelligence and sensors to perform tasks autonomously.

...AND THE NEED FOR IMMEDIATE ACTIONS

In order to benefit from the opportunities offered by emerging technologies, it is essential to promote and foster innovation, while ensuring that security risks, malpractices and misuses are minimized. Creating the EU's digital governance and legislative framework is a key enabler in this process.

ILLUSTRATIVE

An ever-changing EU cyber and digital regulatory landscape

Over the last 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.

Legislation	Key Sectors	Applicability
AI Act	AI	High
GDPR	Personal data	High
NIS2	Cybersecurity	High
DSA	Digital Services	High
DMA	Digital Markets	High
AI Act	AI	High
GDPR	Personal data	High
NIS2	Cybersecurity	High
DSA	Digital Services	High
DMA	Digital Markets	High

ILLUSTRATIVE

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.

Applicable to key sectors:

- Healthcare
- Energy
- Transport
- Manufacturing
- Public Services
- Financial
- Media
- Telecommunications
- Information Systems
- Cloud Services
- Software
- Hardware
- Services
- Products
- Infrastructure
- Supply Chains
- Public Services
- Financial
- Media
- Telecommunications
- Information Systems
- Cloud Services
- Software
- Hardware
- Services
- Products
- Infrastructure
- Supply Chains

Timeline:

2024: CRA adopted
2025: CRA enters into force
2026: CRA fully applicable

ILLUSTRATIVE

Energy & Resources – Use Case 1 (2/4)

Operator of oil production, refining and treatment facilities, storage and transmission

Regulatory framework:

- EU Cyber Resilience Act (CRA)
- EU NIS2 Directive
- EU AI Act
- EU GDPR
- EU DSA
- EU DMA
- EU AI Act
- EU GDPR
- EU DSA
- EU DMA

Key findings:

- High level of compliance with CRA and NIS2 Directive
- Low level of compliance with AI Act and GDPR
- Medium level of compliance with DSA and DMA

Preface to the first iteration of the EUPC Digital Playbook

Considering the broad scope of the EU cyber and digital legislation, the Playbook provides a snapshot of the current European legislative landscape and will be updated alongside regulatory changes

The EUPC Digital Playbook



Provides an overview of the **most impactful current EU digital and cyber legislation** and builds on foundational EU legislative initiatives from the past*



Outlines the **main requirements**** of EU digital and cyber legislation, exploring **intersections and synergies**



Aims to provide a **comprehensive overview** of the EU digital and cyber legislation, **without prejudice** to national and local requirements



Provides an overview of the regulations' impact on sectors even though **applicability and risks varies upon the strategies adopted** and the **services provided** at the **entity level**



Is **updated twice per year**, according to relevant developments in the EU cyber and digital legislative landscape

(*) 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



Technology Trends and the EU Digital Strategy



EU Digital Legislation and Key Sectors Overview



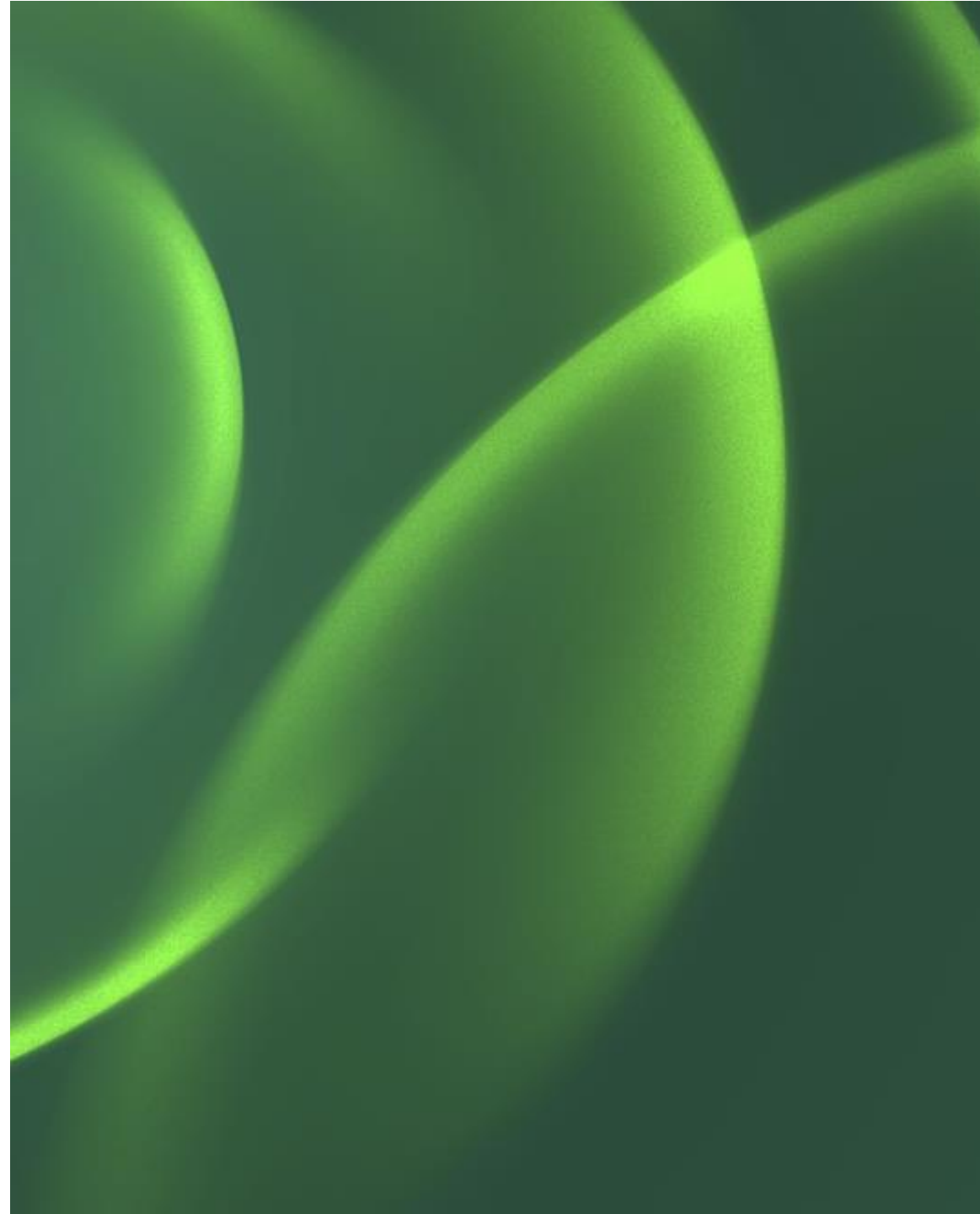
EU Digital Legislation Detail Cards



Key Sectors Use Cases



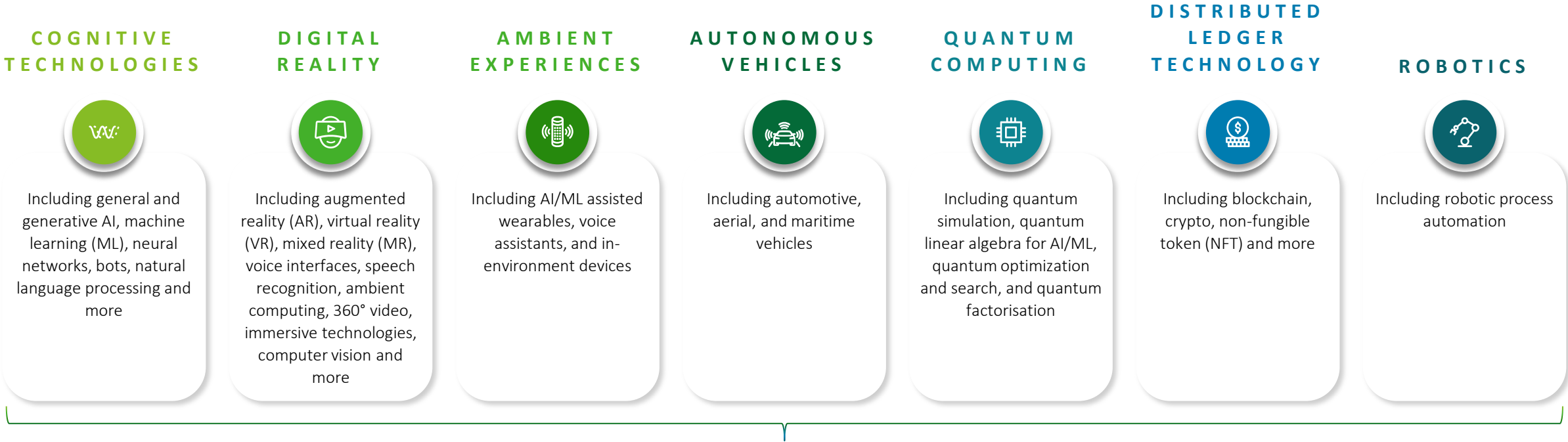
Annex



Emerging technology trends

Emerging technologies are revolutionising the business landscape by enhancing operational efficiency, driving innovation, and enabling new business models, thus unlocking opportunities to transform both practices and industries and gain competitive advantage. Their rapid adoption entails the need for robust regulations to harness benefits, mitigate risks and enhance public trust

EMERGING TECHNOLOGIES TRENDS...

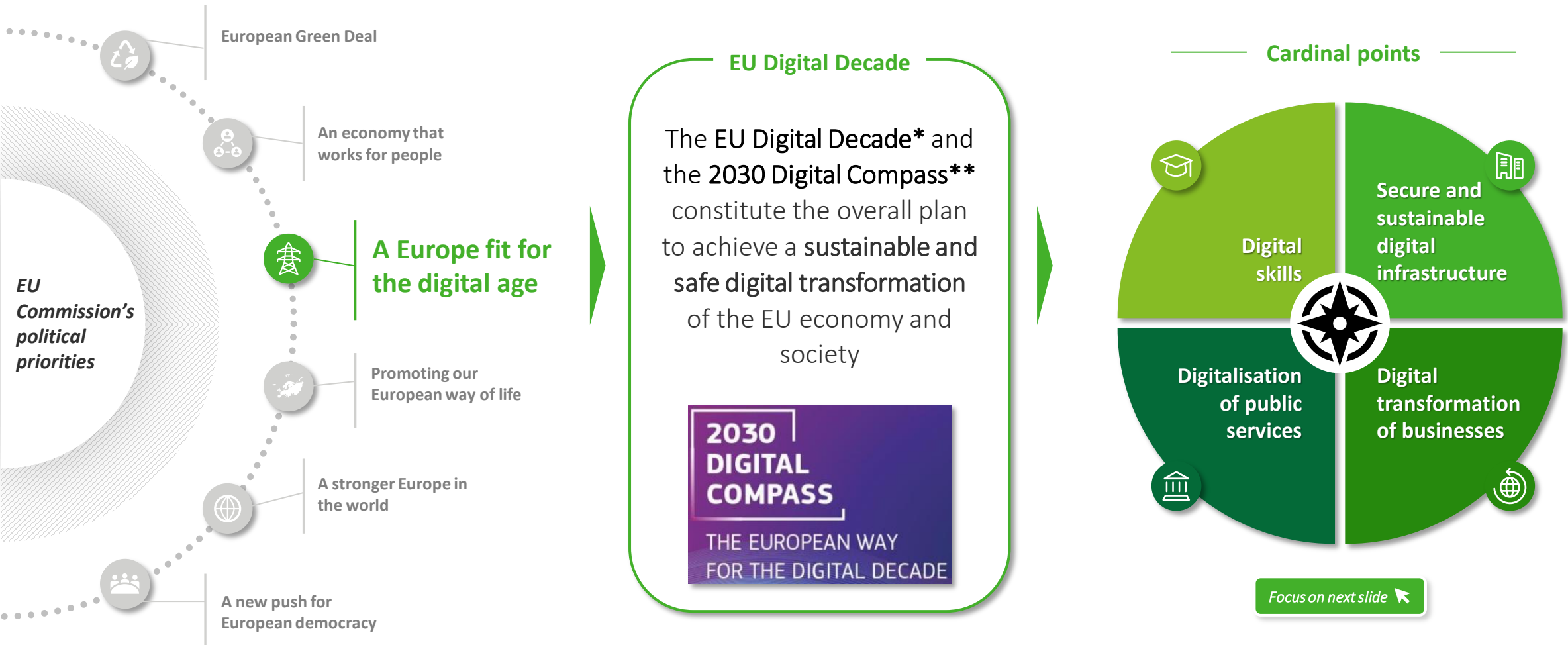


...AND THE NEED FOR IMMEDIATE ACTIONS

*In order to benefit from the opportunities unlocked by **emerging technologies**, it is crucial to promote and boost **investments** as well as develop a coherent **legislative framework** that supports those investments and encourages innovation. Currently, the EU is at the **forefront of regulatory and legislative efforts** in the field of emerging technologies and has developed a **EU Digital Strategy** to ensure a **sustainable and safe digital transformation** of the Union*

EU Digital Strategy and priorities

The EU Digital Strategy sets up a level playing field for the adoption of new technologies, with the aim to strengthen digital sovereignty, promote a healthy and competitive internal market, protect critical infrastructures and safeguard fundamental rights of EU citizens



Progress towards EU’s Digital Decade targets

On 2 July 2024, the EU Commission released the second report* on the State of the Digital Decade. This report summarizes the EU’s progress towards the Digital Decade objectives and targets, highlighting the constant need for collective policy measures and investments

DIGITAL SKILLS

Policy efforts and investment to boost digital literacy and skills across the population are still needed

Based on available data, **55,6% of the EU population** has basic digital skills with the target set at 80% by 2030. Furthermore, Member States should collectively **more than double the average increase of ICT specialists** to meet labour market targets set in the Digital Decade

DIGITALISATION OF PUBLIC SERVICES

Digitalisation of public services has progressed in terms of access to online public services, but should be further improved, especially with regards to cross-border features

The availability of eID schemes, digital public services, and access to e-Health records **is growing**, but **notable differences remain** between countries due to varying eID adoption. There are still significant **gaps** in delivering fully user-centric, accessible, and sovereign **digital public services**

SECURE AND SUSTAINABLE DIGITAL INFRASTRUCTURES

The EU is still far from achieving Digital Decade targets

According to available data, the targets related to **gigabit connection** and the deployment of **highly secure and sustainable edge nodes** are still far from being achieved. Progress still needs to be made also in terms of **5G** as data on coverage does not consider the **quality of service**, which largely remains basic.

The Chips Act has triggered investments in semiconductor manufacturing and the development of the first **quantum accelerated computer** is expected by 2025

DIGITAL TRANSFORMATION OF BUSINESSES

Digitalization of businesses (i.e., **SME digital identity, unicorns, and big data, cloud, and AI take-up**) is still insufficient and uneven across the EU

SMEs’ delay is particularly relevant with regards to the **uptake of AI**. On the other hand, data pertaining to the growth of **unicorns** is **in line with the targets** of the Digital Decade. The comparison with 2023 in terms of **Big Data** cannot be properly assessed, as the data indicator has changed and now includes the take-up of **data analytics technologies**

WHAT’S NEXT?

Apart from developing **resilient digital infrastructures** and encouraging the spread of **technical skills** and **ethical principles** to ensure **responsible use of emerging technologies**, the need for a **coherent regulatory framework** is pivotal for the **EU** to achieve the **Digital Decade targets**. The aims of a coherent and comprehensive regulatory framework are to promote **harmonization**, ensure high standards of digital products’ **safety and security**, foster **innovation**, protect **fundamental rights**, build **public trust**, unlock the full potential of the **single market**, and facilitate agile responses to **technological changes**



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



Technology Trends and the EU Digital Strategy



EU Digital Legislation and Key Sectors Overview



EU Digital Legislation Detail Cards



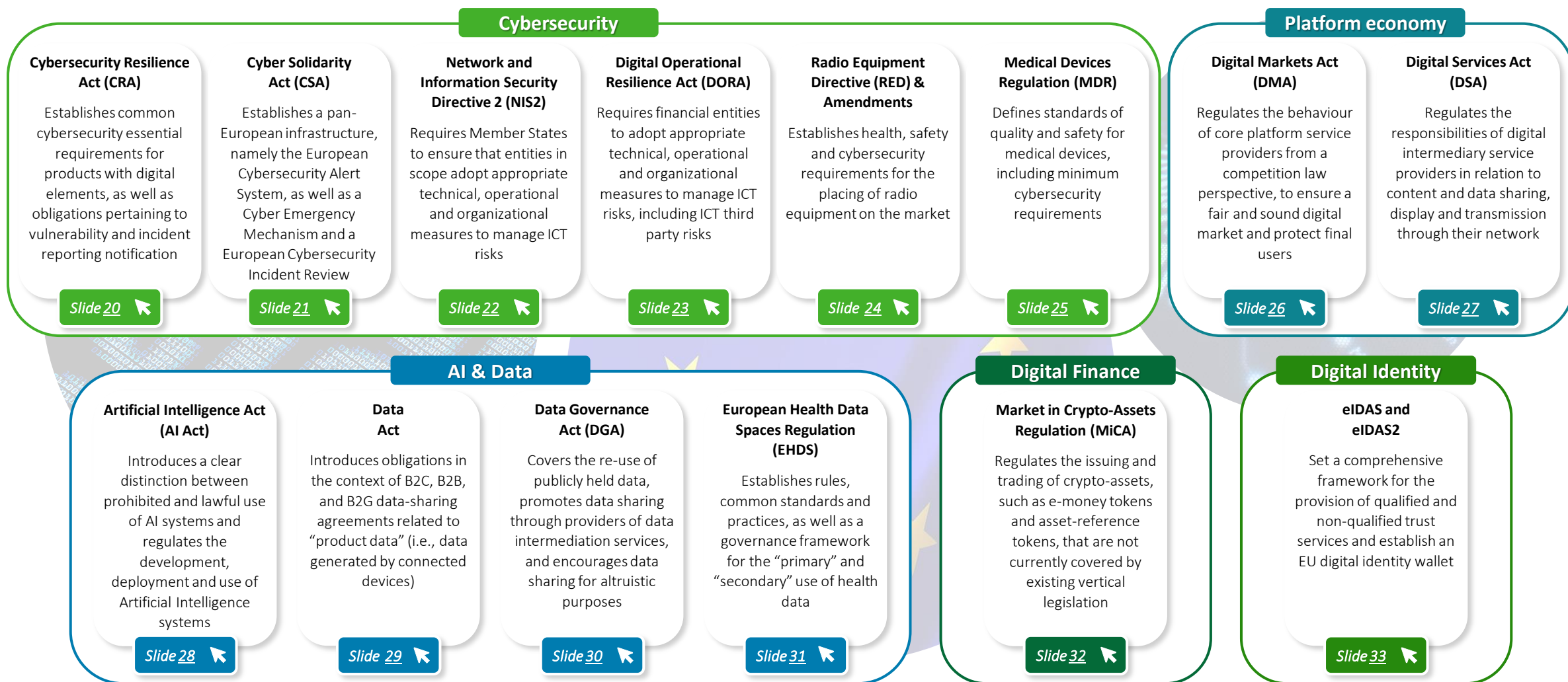
Key Sectors Use Cases



Annex

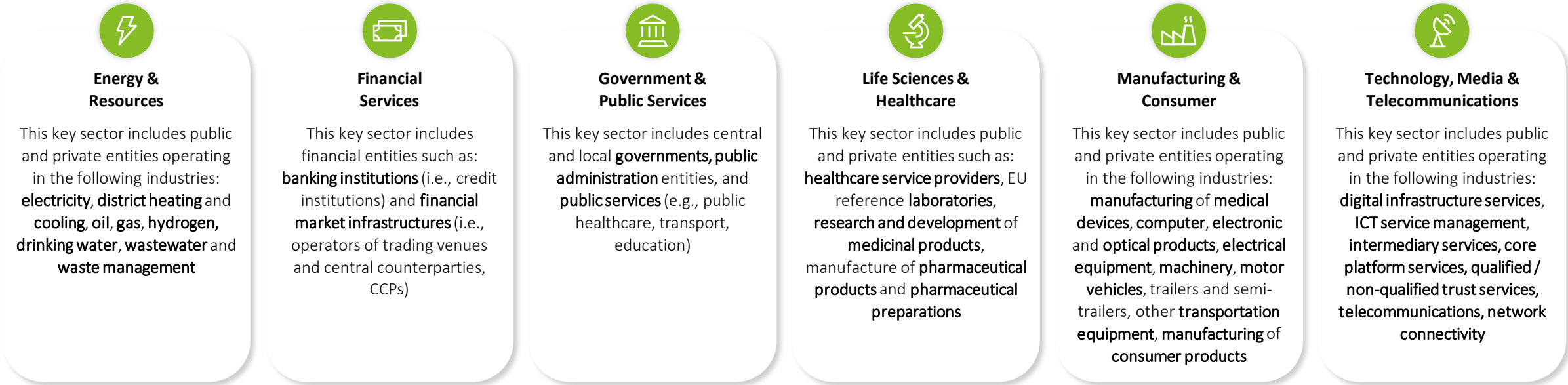
An ever-changing EU cyber and digital regulatory landscape

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



Key Sectors and Use Cases

To assess the impact of the EU digital and cyber legislation on public and private entities, the Playbook identifies six sectors*. For each sector, illustrative use cases have been developed to support readers understand potential applications of the identified EU legislation





























































































Use Cases – Entities subject to EU digital legislation



EU Digital legislation impact on key sectors

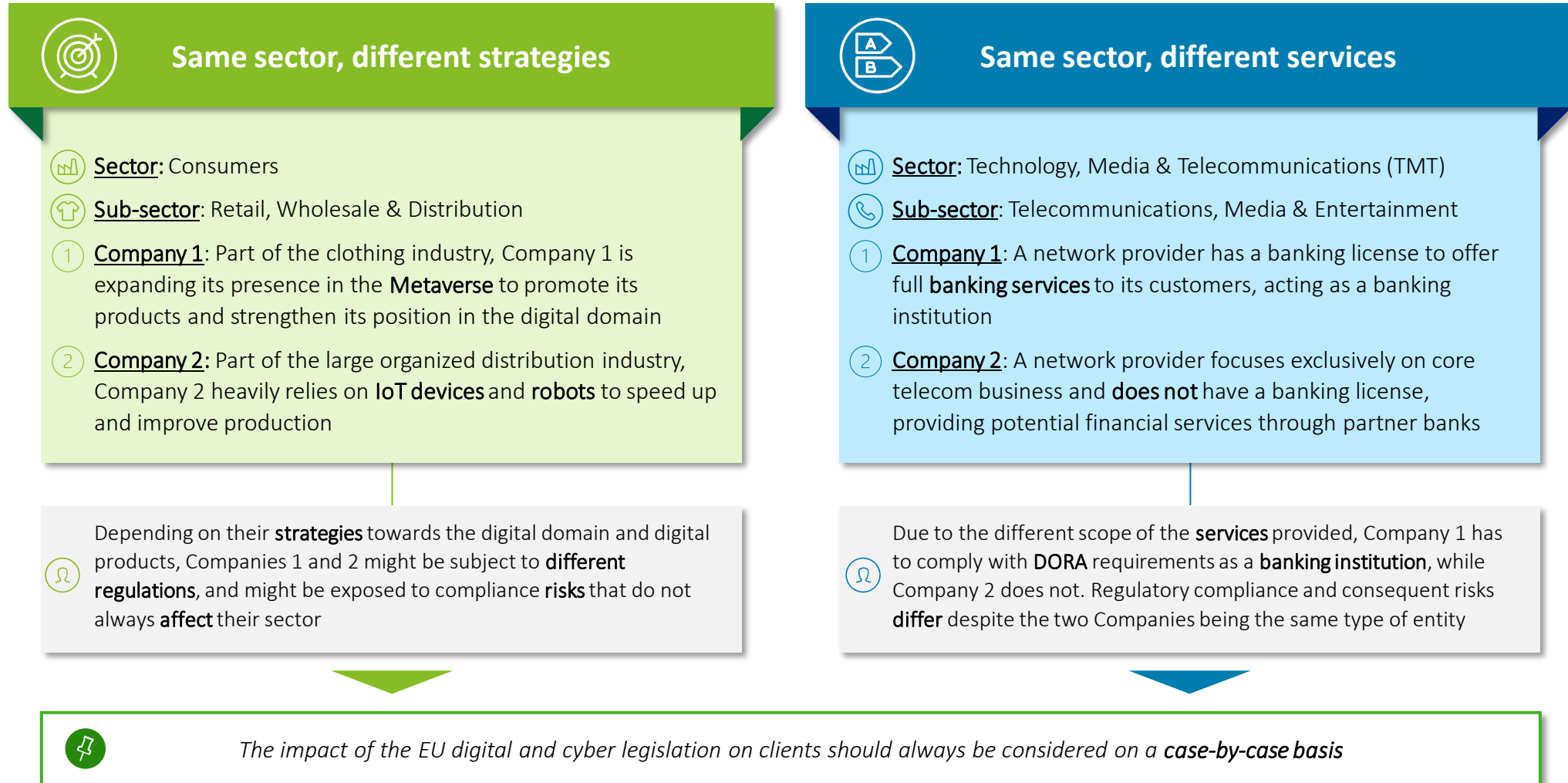
Below a high-level representation of the impact of the analyzed EU cyber and digital legislation against the identified sectors, acknowledging that the applicability of each legislation against entities depends on their specificities

	Cybersecurity						Platform economy		AI & Data				D. Finance	D. Identity
	CRA*	CSA	NIS2*	DORA	RED & Amendments*	MDR	DMA	DSA	AI Act*	Data Act*	DGA	EHDS	MiCA	eIDAS & eIDAS2
 Energy & Resources														
 Financial Services**														
 Government & Public Services														
 Life Sciences & Healthcare														
 Manufacturing & Consumer														
 Technology, Media & Telecommunications														

(*) Cross-sectoral legislation | (**) As per recital (28) of NIS2 Directive, the provisions of Regulation (EU) 2022/2554 (DORA) shall apply to the financial sector instead of the ones of NIS2 Directive

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





Introduction to the EUPC



Introduction to the EUPC Digital Playbook



Technology Trends and the EU Digital Strategy



EU Digital Legislation and Key Sectors Overview



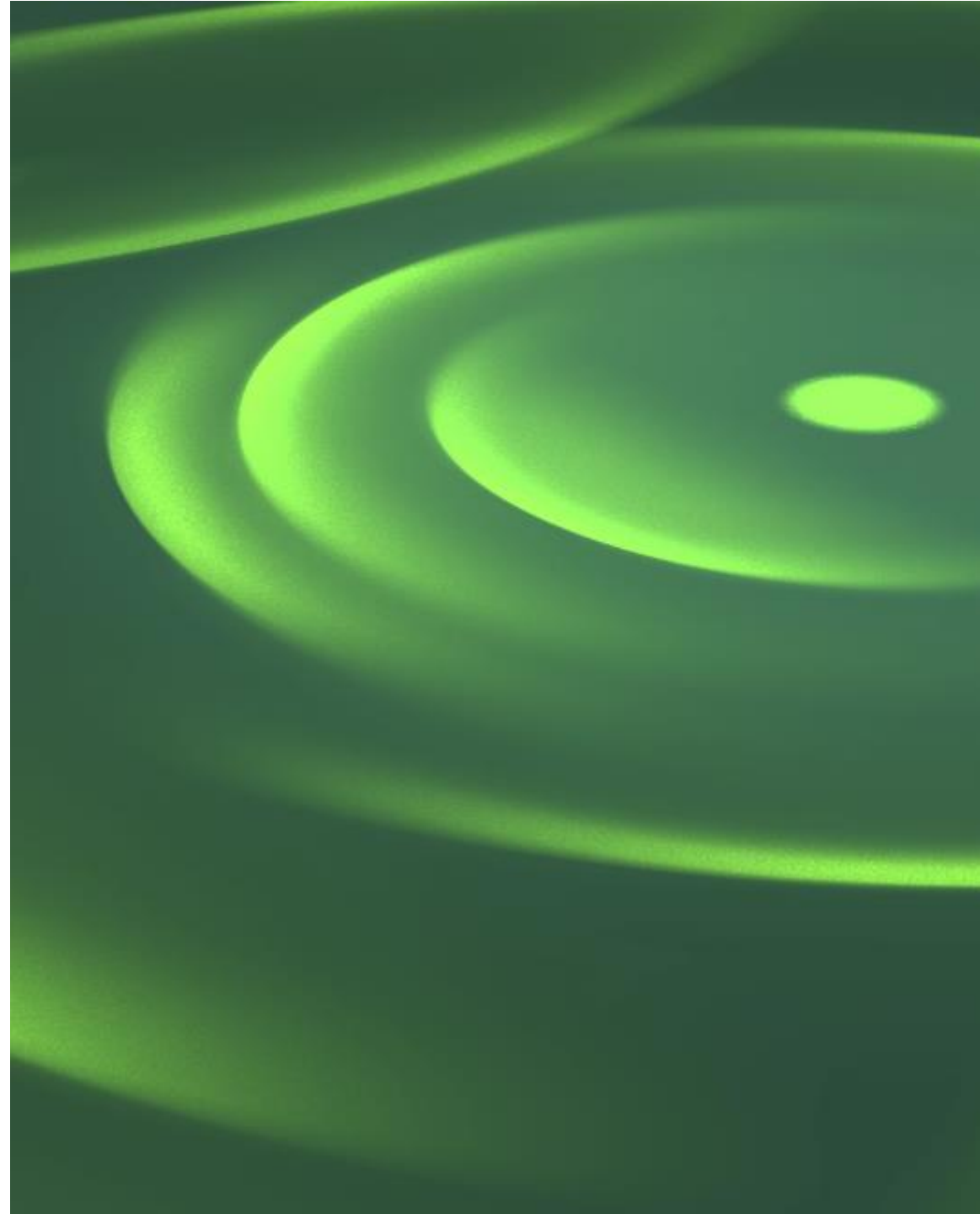
EU Digital Legislation Detail Cards



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 Organizations (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



Financial Services



Government & Public Services



Life Sciences & Healthcare



Manufacturing & Consumer



Technology, Media & Telecommunications

This Regulation applies to:

- Manufacturers (or entities that market under their name products with digital elements manufactured by others)
 - Authorized representatives of manufacturers
 - Importers
 - 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

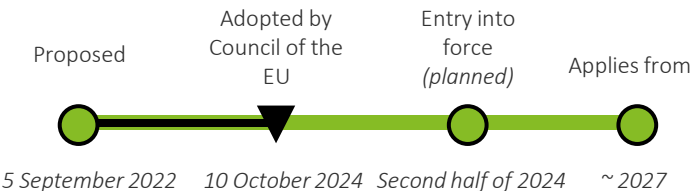
law:

- | | |
|--|--|
| <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"> NIS 2 RED and amendments Regulation (EU) 2017/745 Regulation (EU) 2017/746 Regulation (EU) 2019/2144 |
|--|--|

Regulatory Stakeholders:

- | | |
|---|--|
| <ul style="list-style-type: none"> National cybersecurity certification authorities Market surveillance authority European Standardization Organizations | <ul style="list-style-type: none"> ENISA EU Commission National CSIRT |
|---|--|

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, 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:

- The deployment of a pan-European infrastructure of **National Cyber Hubs (European Cybersecurity Alert System)** to build and enhance **common detection** and **situational awareness capabilities**
- The 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)
- The establishment of a **European Cybersecurity Incident Review Mechanism** to review and assess **specific significant** or **large-scale incidents**

Applicable key sectors*



Energy & Resources



Life Sciences & Healthcare



Financial Services



Manufacturing & Consumer



Government & Public Services



Technology, Media & Telecommunications

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)*
- *Trusted providers*

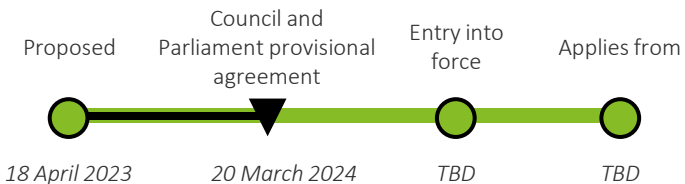
Intersection with other EU law:

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

Regulatory Stakeholders:







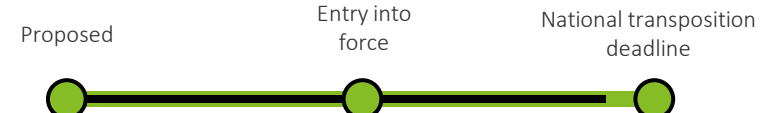



- *EU Commission*
- *CSIRTs/competent authority*
- *ENISA*
- *NIS Cooperation Group*

Timeline



Network and Information Security Directive 2 (NIS2)

In response to the growing threats posed by digitization and the resulting increase in cyber-attacks, the EU’s co-legislators have adopted new 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	Applicable key sectors	Intersection with other EU law: 2013/40/EU
<p>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.</p> <p>More specifically, to comply with NIS2 Member States:</p> <ul style="list-style-type: none"> • 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 detailed risk management frameworks, namely all appropriate and proportionate technical, operational and organizational measures to manage information and ICT risks, as well as 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 	<div> <div>  Energy & Resources </div> <div>  Financial Services </div> <div>  Government & Public Services </div> </div> <div> <div>  Life Sciences & Healthcare </div> <div>  Manufacturing & Consumer </div> <div>  Technology, Media & Telecommunications </div> </div> <p><u>This Directive applies to:</u></p> <ul style="list-style-type: none"> • Public or private entities operating in “Highly critical” (Annex I) or “Critical” (Annex II) sectors (e.g., energy, transportation, health) which qualify 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) 	<p><u>Intersection with other EU law:</u></p> <ul style="list-style-type: none"> • CRA • Cybersecurity Act • DORA • Directive 2022/2557/EU (CER) • Directives 2002/58/EC, 2011/93/EU and <p><u>Regulatory Stakeholders:</u></p> <ul style="list-style-type: none"> • CSIRTs • ENISA • EU Commission • National supervisory authorities • NIS Cooperation Group <div> <p><u>Timeline</u></p>  </div>
22 Deloitte EU Policy Centre Copyright © 2024 All rights reserved	Legend  Applicable  Partially applicable  Non-applicable	

Digital Operational Resilience Act (DORA)

DORA is the EU's largest digital operational resilience and cybersecurity initiative 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



Energy & Resources



Life Sciences & Healthcare



Financial Services



Manufacturing & Consumer



Government & Public Services



Technology, Media & Telecommunications

This Regulation applies to:

- | | |
|---|---|
| • <i>Credit and payment institutions</i> | • <i>management company</i> |
| • <i>account information service providers</i> | • <i>data communications service providers</i> |
| • <i>electronic money institutions</i> | • <i>Insurance, reinsurance companies and intermediaries</i> |
| • <i>investment enterprises</i> | • <i>occupational pension institutions</i> |
| • <i>service providers for cryptocurrencies</i> | • <i>credit rating agencies</i> |
| • <i>central securities depositories</i> | • <i>critical benchmark index administrators</i> |
| • <i>central counterparties</i> | • <i>crowdfunding service providers</i> |
| • <i>trading venues and trade repositories</i> | • <i>securitization data repositories third-party ICT service providers</i> |
| • <i>alternative investment fund managers</i> | |

Legend Applicable Partially applicable Non-applicable

Intersection with other EU

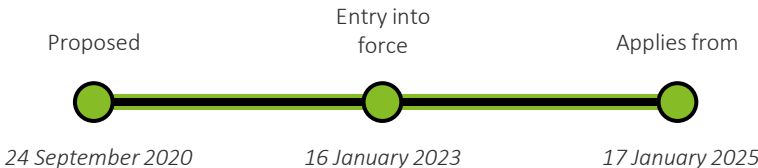
law:

- CRA
- NIS2

Regulatory Stakeholders:

- | | |
|---|------------------------|
| • <i>National supervisory authorities</i> | • <i>EIOPA</i> |
| • <i>ECB</i> | • <i>ESMA</i> |
| • <i>EBA</i> | • <i>EU Commission</i> |

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



Life Sciences & Healthcare



Financial Services



Manufacturing & Consumer



Government & Public Services



Technology, Media & Telecommunications

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

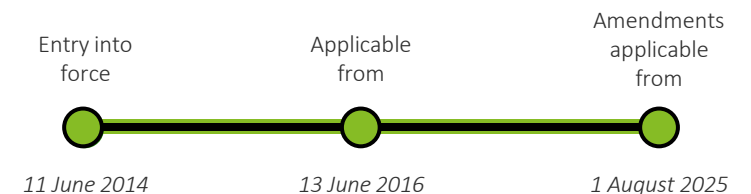
law:

- *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:

- Market surveillance authorities
- Notified bodies
- Spectrum authorities
- EU Commission
- Telecommunication Conformity Assessment

Timeline



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

The MDR aims to set high 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



Government & Public Services



Life Sciences & Healthcare



Manufacturing & Consumer



Technology, Media & Telecommunications

This Regulation applies to:

- Manufacturers of medical devices

Intersection with other EU

law:

- AI Act for horizontal AI regulation
- NIS2 and Cyber Resilience Act (for horizontal cybersecurity requirements)
- Machinery Directive (“Devices that are also machinery within the meaning of point (a) of the second paragraph of the Machinery Directive

shall, where a hazard relevant under that Directive exists, also meet the essential health and safety requirements set out in Annex I to that Directive to the extent to which those requirements are more specific than the general safety and performance requirements set out in Chapter II of Annex I to this Regulation.”)

Regulatory Stakeholders:

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

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 June 2024, the EU Commission designated as gatekeepers: **Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, and Booking**. In addition, **22 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

Applicable key sectors



Energy & Resources



Life Sciences & Healthcare



Financial Services



Manufacturing & Consumer



Government & Public Services



Technology, Media & Telecommunications

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:

- *EU 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

Applicable key sectors



Energy & Resources



Life Sciences & Healthcare



Financial Services



Manufacturing & Consumer



Government & Public Services



Technology, Media & Telecommunications

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:

The DSA should apply without prejudice to:

- 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:

- EU Commission
- European Board for Digital Services

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 systems, and iv) other basic AI systems. It then sets out different obligations depending on the subjective scope and type of AI system. With regard to **high-risk AI systems**, the AI Act requires:

- Adoption of a comprehensive **AI risk management framework**, including ex-ante testing of the system as well as post-market monitoring;
- Definition of appropriate **data governance practices** in case of development and training of the AI system;
- 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*



This Regulation applies to:

- *Providers*
- *Deployers*
- *Importers and distributors*
- *Users of AI systems falling within the scope of the Regulation*

AI Liability Directive

Proposed in September 2022, the AI Liability Directive (AILD) complements the AI Act by introducing a new liability regime that will ensure legal certainty, enhance consumer trust in AI, and assist consumers' liability claims for damage caused by AI-enabled products and services.

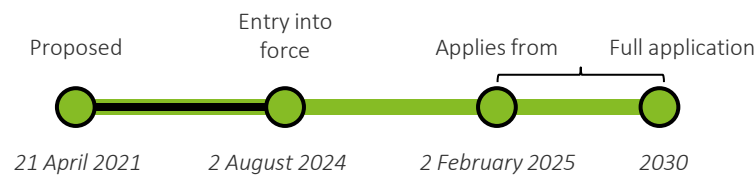
Intersection with other EU law:

- *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*
- *New Legislative Framework (NLF)*

Regulatory Stakeholders:

- *AI Office (within the EU 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*



Energy & Resources



Life Sciences & Healthcare



Financial Services



Manufacturing & Consumer



Government & Public Services



Technology, Media & Telecommunications

This Regulation applies to:

- Data holders*
- Data recipients*
- Users*

Financial Data Access Regulation

Proposed in June 2023, the Financial Data Access Regulation (FIDA) is a vertical legislation derived from the Data Act and the Data Governance Act which aims to establish rights and obligations to manage customer data sharing in the financial sector

Intersection with other EU

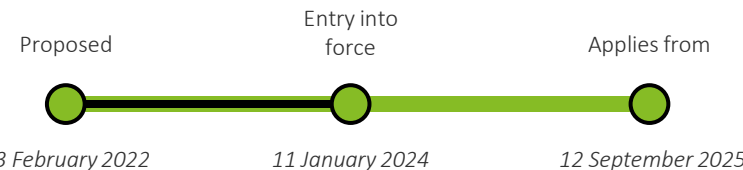
law:

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

Regulatory Stakeholders:

- Data Protection Supervisor*
- EDIB*
- EU Commission*

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



Life Sciences & Healthcare



Financial Services



Manufacturing & Consumer



Government & Public Services



Technology, Media & Telecommunications

This Regulation applies to:

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

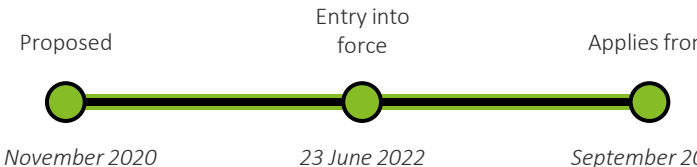
Intersection with other EU law:

- | | |
|---------------------------|-------------------------------|
| • Data Act | 2017/1132 |
| • Directive 2000/31/EC | • Directive (EU) 2019/790 |
| • Directive 2001/29/EC | • Directive (EU) 2019/1024 |
| • Directive 2004/48/EC | • DMA |
| • Directive 2007/2/EC | • GDPR |
| • Directive 2010/40/EU | • Regulation (EC) No 223/2009 |
| • Directive (EU) 2015/849 | • Regulation (EU) 2018/858 |
| • Directive (EU) 2016/943 | • Regulation (EU) 2018/1807 |
| • Directive (EU) | |

Regulatory Stakeholders:

- | | |
|----------------------------------|----------------------------------|
| • EU Commission | • National Competent Authorities |
| • European Data Innovation Board | |

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

Intersection with other EU

- law:
- AI Act
 - CRA
 - Data Act
 - Data Governance Act
 - Cross-border healthcare collaborations Directive (CBHC Directive)
 - GDPR
 - In Vitro Diagnostics Regulation
 - Medical Devices Regulation
 - NIS 2

Regulatory Stakeholders:

- Digital health authorities at the national level
- EU Commission
- European Health Data Space Board

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



This Regulation applies to:

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

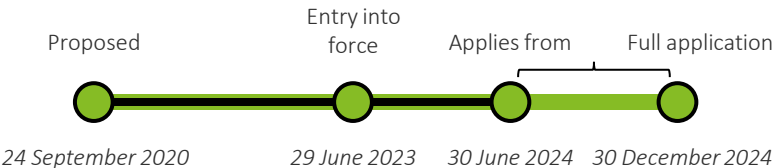
Intersection with other EU law:

- 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:

- National supervisory authorities
- ESMA (in cooperation with EBA, EIOPA and the ECB)
- EU Commission

Timeline



Regulation eIDAS and latest revision on EU digital identity framework

eIDAS, complemented by the proposed revision, sets out a comprehensive framework for the provision of qualified and non-qualified trust services, with the aim of creating a safe digital space and creating a digital wallet for EU citizens

Description

On 23 July 2014, the European Parliament and the Council of the European Union adopted the eIDAS Regulation, which establishes a clear **regulatory framework for electronic identification and trust services**. Among others, eIDAS lays down:

- A **list of trust services**, both qualified and non-qualified, including electronic signatures, seals, time stamps and authentication methods;
- Requirements for the **provision of trust services**, including, where applicable, the granting of a qualified status upon the service provider, as well as appropriate technical and organizational measures to manage security risks and ensure that the level of security is commensurate to the level of risk;
- The **obligation** of trust service providers **to notify supervisory bodies of any breach or loss that has a significant impact** on the service provided or on the personal data maintained;
- The obligation for qualified trust service providers to be **audited** at least every 24 months;
- The conditions under which Member States recognise **electronic identification means** falling under a notified electronic identification scheme of other Member States.

In order to meet the objective of making key public services available online by 2030, the EU Commission recently proposed a **revision of eIDAS** in 2021 to set the baseline for electronic attestation of attributes and an **EU digital identity wallet**

Applicable key sectors



This Regulation applies to:

- *Trust service providers*
- *Qualified trust service providers*

Intersection with other EU

law:

- GDPR

Regulatory Stakeholders:

- *National supervisory authorities*
- *National conformity assessment bodies*
- *ENISA*
- *EU Commission*

Timeline





Introduction to the EUPC



Introduction to the EUPC Digital Playbook



Technology Trends and the EU Digital Strategy



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

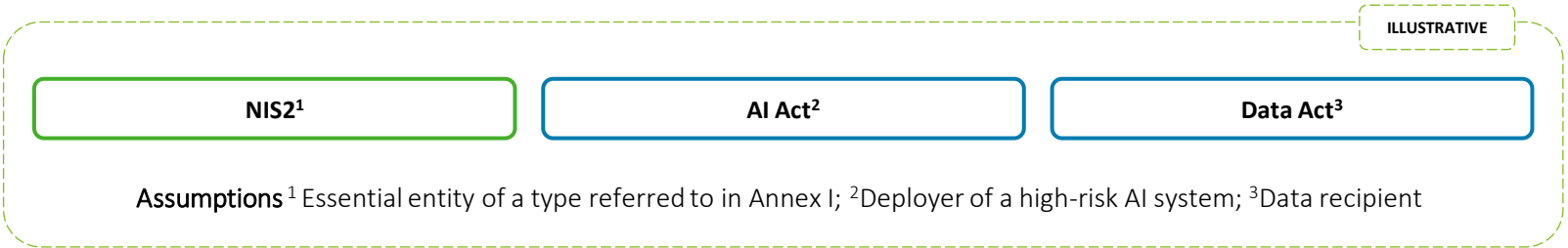
Categories used to cluster legislative requirements

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



Assumptions

Each legislation imposes specific requirements on companies 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 (1/4)

The Energy & Resources use case 1 provides an illustrative snapshot of how an Operator of oil production, refining and treatment facilities, storage and transmission 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



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

Entity



Operator of oil production, refining and treatment facilities, storage and transmission

Assumptions

Identification of an entity within the sector

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 Operator of oil production, refining and treatment facilities, storage and transmission, under the selected legislation, acts as:

NIS2

Essential entity

An entity referred to in Annex I “Sectors of High Criticality,” which exceeds the ceilings for medium-sized enterprises.

AI Act

Deployer of a high-risk AI system

Any individual, organization, government body, agency, or entity using an AI system under its control, unless the AI system is being used for personal, non-professional purposes.

Data Act

Data recipient

Any individual or organization acting for purposes related to their trade, business, craft, or profession, excluding the user of a connected product or service, to whom the data holder provides access to data. This may include a third party.

Energy & Resources – Use Case 1 (2/4)

Operator of oil production, refining and treatment facilities, storage and transmission

Obligations

	NIS2 ¹	AI Act ²	Data Act ³
Governance Measures	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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, e.g., ensure a sufficient level of AI literacy of staff✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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 and inform the provider or distributor and relevant market surveillance authority, and suspend the use of that system in case it poses any unacceptable risk	x Not covered

Regulatory intersection

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

The analyzed 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** introduces a general obligation to set a **clear and technology-agnostic risk governance framework**, while subject-specific legislation – such as the **AI Act** – introduces **vertical requirements**.

Therefore, **compliance** to high-risk AI systems **vertical requirements** **contributes** to the fulfillment of **NIS2 overall governance obligations**

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

As a horizontal legislation, **NIS2** 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. **AI systems** used by the entity, being tools, shall be included in the risk management framework, with their implementation and use being documented in adequate policies, as well within the entity's **overall third-party risk management process** (e.g., supply chain mapping, contract review).

Therefore, **compliance** to high-risk AI systems **vertical requirements** **contributes** to the fulfillment of **NIS2 overall ICT-related risk management obligations**

Energy & Resources – Use Case 1 (3/4)

Operator of oil production, refining and treatment facilities, storage and transmission

Obligations

	NIS2 ¹	AI Act ²	Data Act ³
Vulnerability Management	<ul style="list-style-type: none">✓ 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 Not covered	x Not covered
Incident Management	<ul style="list-style-type: none">✓ 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 to national CSIRT, or competent authority, any incident that has a significant impact on the provision of the operator's services	<ul style="list-style-type: none">✓ 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 Not covered

Regulatory intersection

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

The analyzed legislation requires entities 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.

With regard to **AI systems**, **deployers cannot directly test the infrastructure** of the AI system. It is likely that they will oversee the overall security of the AI system through their **overall third-party risk management framework** (e.g., reviewing supply chains and negotiating specific contractual clauses).

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

While NIS2 outlines measures for the notification of **ICT significant incidents** to national CSIRTs, or competent authorities, the AI Act outlines 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 fulfillment 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**.

Energy & Resources – Use Case 1 (4/4)

Operator of oil production, refining and treatment facilities, storage and transmission

Back to slide 16

Obligations

NIS2 ¹	AI Act ²	Data Act ³
<div>ICT Security Compliance & Certification</div> <ul style="list-style-type: none">✓ 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	<div></div> <ul style="list-style-type: none">x Not covered	<div></div> <ul style="list-style-type: none">x Not covered
<div>Data Governance & Management</div> <ul style="list-style-type: none">✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	<div></div> <ul style="list-style-type: none">✓ 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	<div></div> <ul style="list-style-type: none">✓ 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

Regulatory intersection

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

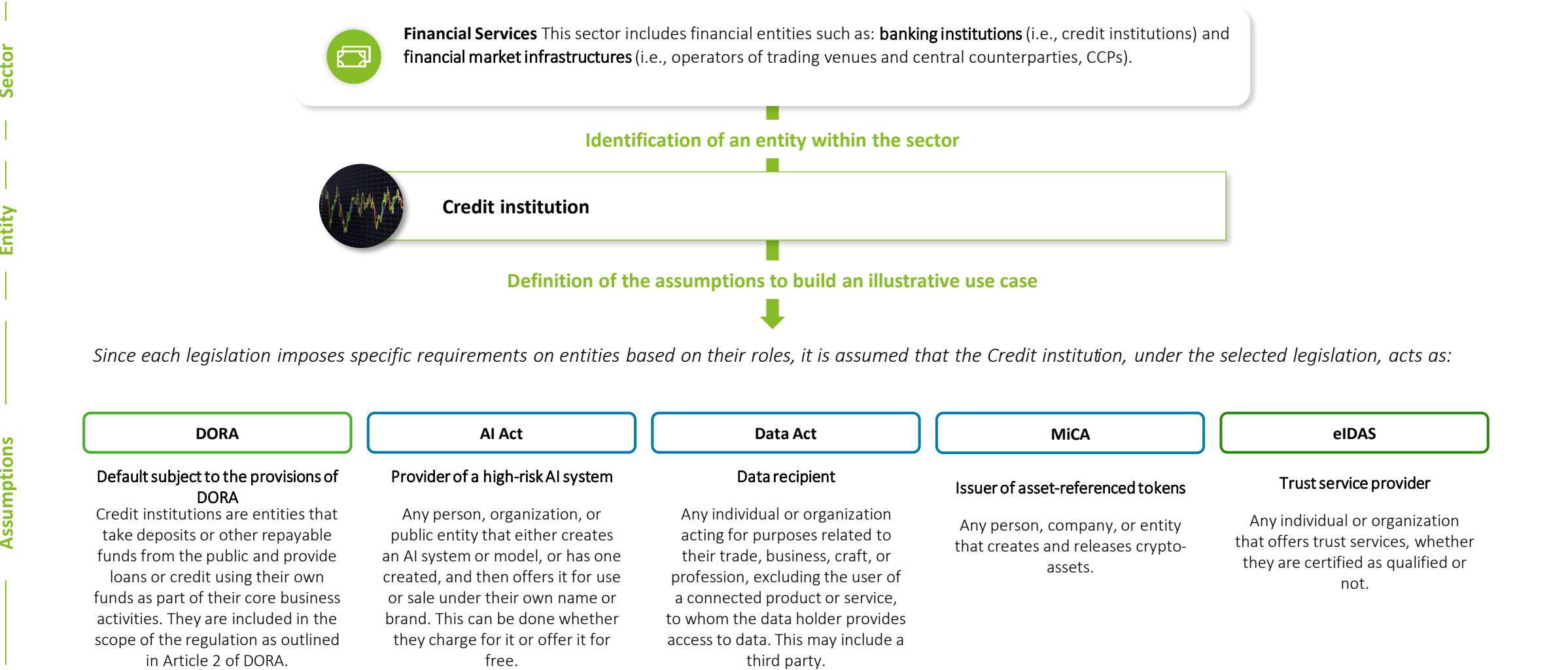
The analyzed legislation requires entities to **demonstrate compliance with ICT security requirements**.

NIS2 provides that Member States **may require** essential and important entities to use particular ICT products, ICT services and ICT processes, either developed by the entity or procured from third parties, that are **certified under European cybersecurity certification schemes** adopted pursuant to Article 49 of Regulation (EU) 2019/881. In the absence of appropriate European cybersecurity certification schemes, Member States shall require entities to comply with **relevant European and international standards** (e.g., upcoming AI standards defined by CEN/CENELEC). Entities shall **oversee the compliance with ICT security requirements by providers** as part of their third-party risk management obligations

The analyzed legislation, without prejudice to the overall compliance with **data protection obligations under the GDPR**, requires entities to comply with **additional subject-specific obligations** (e.g., ensuring 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)

Financial Services – Use Case 1 (1/4)

The Financial Services’ use case 1 provides an illustrative snapshot of how a Credit institution 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 1 (2/4)

Credit Institution

Back to slide 16

Obligations

Regulatory intersection

	DORA ¹	AI Act ²	Data Act ³	MiCA ⁴	eIDAS ⁵
Governance Measures	<ul style="list-style-type: none">Establish an internal governance and control framework that ensures an effective and prudent management of ICT riskThe management body shall define, approve, oversee and be responsible for all arrangements related to the ICT risk management frameworkA control function with appropriate level of independence shall be responsible for managing and overseeing ICT risk	<ul style="list-style-type: none">Put in place and document a quality management system, including an accountability framework detailing roles and responsibilities regarding high-risk AI systemsAssign human oversight to natural persons who have the necessary competence, training and authorityEnsure the staff has adequate AI literacyEnforce the conformity assessment procedure for high-risk AI systemsRegister AI systems and themselves in the EU and, if needed, national database	x <i>Not covered</i>	<ul style="list-style-type: none">Implement robust governance arrangements, including a clear organizational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which they are or might be exposed	<ul style="list-style-type: none">Take appropriate organizational measures to manage risks posed to the security of the trust services providedEmploy 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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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 possible risksPerform a fundamental rights impact assessment (FRIA) for high-risk AI systems before deploymentEstablish 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	x <i>Not covered</i>	<ul style="list-style-type: none">Implement internal control mechanisms and effective procedures for risk management, including effective control and safeguard arrangements for managing ICT systems as required by Regulation (EU) 2022/2554 (DORA)	<ul style="list-style-type: none">Take appropriate technical and organizational measures to manage risks posed to the security of the trust services providedUse trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by themComply with service-specific security requirements (e.g., ICT security for electronic signatures)

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

The analyzed 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**. Other subject-specific legislation introduce **vertical requirements**. Therefore, **compliance to vertical requirements contributes to the fulfillment of DORA overall governance obligations**.

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

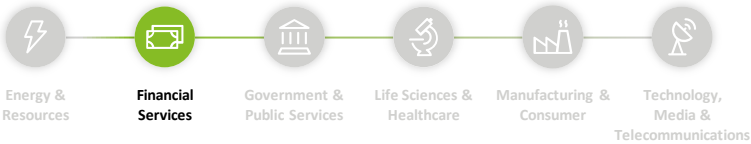
As the cornerstone legislation for financial entities, **DORA** introduces a broad obligation to set up a **comprehensive, documented and regularly updated risk management framework**, including strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks. Other **subject-specific risk management obligations** (e.g., under the **AI Act**, **MiCA** and **eIDAS**) constitute further specifications of the overall risk management obligation imposed by DORA.

Therefore, **compliance with requirements set out in the AI Act, MiCA, and eIDAS contribute to the fulfillment of DORA overall ICT-related risk management obligations**.

Financial Services – Use Case 1 (3/4)

Credit Institution

Back to slide 16



Obligations

Regulatory intersection

	DORA ¹	AI Act ²	Data Act ³	MiCA ⁴	eIDAS ⁵
Vulnerability Management	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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 Not covered	x Not covered	<ul style="list-style-type: none">✓ Perform a regular 2-year vulnerability assessment to maintain the certification of conformity for qualified electronic signature creation devices
Incident Management	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ Notify to market surveillance authorities 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	x Not covered	x Not covered	<ul style="list-style-type: none">✓ Take appropriate technical and organizational 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

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

The analyzed legislation requires entities 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.

With regard to **AI systems**, providers need to comply with strict monitoring obligations, both ante- and post-market. Other **subject-specific vulnerability management obligations** under **eIDAS** constitute further specifications of the overall vulnerability management obligation imposed by DORA.

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

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)

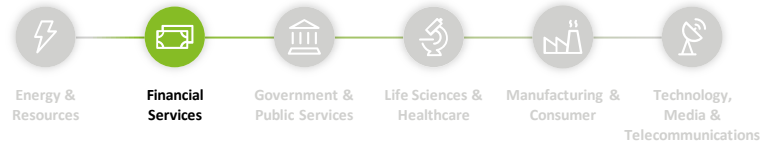
With regard to **incident reporting obligations under DORA**, Member States are expected to **provide single entry points** at national level.

The **AI Act** requires entities to notify **market surveillance authorities** of serious incidents. However, **it is likely that such authorities will coincide with the single-entry points** designated under NIS2. Under **eIDAS**, entities shall report incidents to competent supervisory authorities which will likely not coincide with single entry points designated under DORA.

Financial Services – Use Case 1 (4/4)

Credit Institution

Back to slide 16



Obligations

Regulatory intersection

	DORA ¹	AI Act ²	Data Act ³	MiCA ⁴	eIDAS ⁵
ICT Security Compliance & Certification	<ul style="list-style-type: none">✓ Adopt ICT systems, protocols, and tools that are appropriate, reliable, and technologically resilient	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">x Not covered	<ul style="list-style-type: none">x Not covered	<ul style="list-style-type: none">✓ 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
Data Governance & Management	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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)	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ Comply with fundamental data protection obligations under Union law	<ul style="list-style-type: none">✓ 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)

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

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

DORA provides that entities shall 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

The analyzed legislation, without prejudice to the overall compliance with **data protection obligations under the GDPR**, requires entities to comply with **additional subject-specific obligations** (e.g., ensuring that input data is relevant and sufficiently representative under the AI Act, refrain from using or sharing data for purposes that might damage the data holders or users under the Data Act, and taking appropriate measures against forgery and theft of data under eIDAS)

Financial Services – Use Case 2 (1/4)

The Financial Services’ use case 2 provides an illustrative snapshot of how an Insurance and reinsurance undertaking 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



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

Identification of an entity within the sector



Insurance and reinsurance undertaking

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 Insurance and reinsurance undertaking, under the selected legislation, acts as:

DORA

Default subject to the provisions of DORA

Insurance and reinsurance undertakings are entities authorized to provide direct insurance services (life or non-life) or reinsurance services. They are included in the scope of the regulation as outlined in Article 2 of DORA.

AI Act

Deployer of a high-risk AI system

Any individual, organization, government body, agency, or entity using an AI system under its control, unless the AI system is being used for personal, non-professional purposes.

Data Act

Data recipient

Any individual or organization acting for purposes related to their trade, business, craft, or profession, excluding the user of a connected product or service, to whom the data holder provides access to data. This may include a third party.

Financial Services – Use Case 2 (2/4)

Insurance and reinsurance undertaking

Back to slide 16

Obligations

Regulatory intersection

	DORA ¹	AI Act ²	Data Act ³
Governance Measures	<ul style="list-style-type: none">Establish an internal governance and control framework that ensures an effective and prudent management of ICT riskThe management body shall define, approve, oversee and be responsible for all arrangements related to the ICT risk management frameworkA control function with appropriate level of independence shall be responsible for managing and overseeing ICT risk	<ul style="list-style-type: none">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 systemEnsure the staff has adequate AI literacyAssign 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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for usePerform a fundamental rights impact assessment (FRIA) for high-risk AI systems before deploymentMonitor the operation of the high-risk AI system on the basis of the instructions for use and share relevant data with providers and inform the provider or distributor and relevant market surveillance authority, and suspend the use of that system in case it poses any unacceptable risk	x Not covered

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

The analyzed 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 the cornerstone of cyber resilience legislation for the financial sector, 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**. Other subject-specific legislation introduce **vertical requirements**. Therefore, **compliance to vertical requirements contributes to the fulfillment of DORA overall governance obligations**

The analyzed 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. Other **subject-specific risk management obligations** (e.g., under the AI Act and eIDAS) constitute further specifications of the overall risk management obligation imposed by DORA.

Therefore, **compliance with requirements set out in the AI Act and eIDAS contribute to the fulfillment of DORA overall ICT-related risk management obligations**.

Financial Services – Use Case 2 (3/4)

Insurance and reinsurance undertaking

Back to slide 16

Obligations

	DORA ¹	AI Act ²	Data Act ³
Vulnerability Management	<ul style="list-style-type: none">✓ 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 Not covered	x Not covered
Incident Management	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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 Not covered

Regulatory intersection

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

The analyzed legislation requires entities 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.

With regard to **AI systems**, **deployers cannot directly test the infrastructure** of the AI system. It is likely that they will oversee the overall security of the AI system through their **overall third-party risk management framework** (e.g. reviewing supply chains and negotiating specific contractual clauses).



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

DORA sets a general obligation to manage incidents throughout their lifecycle according to recognized standards and frameworks, covering analogous product-specific obligations (e.g., under the CRA) With regard to **incident reporting obligations under DORA**, Member States are 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 likely that such authorities will coincide with the single-entry points** designated under NIS2, in order to streamline reporting obligations.

Financial Services – Use Case 2 (4/4)

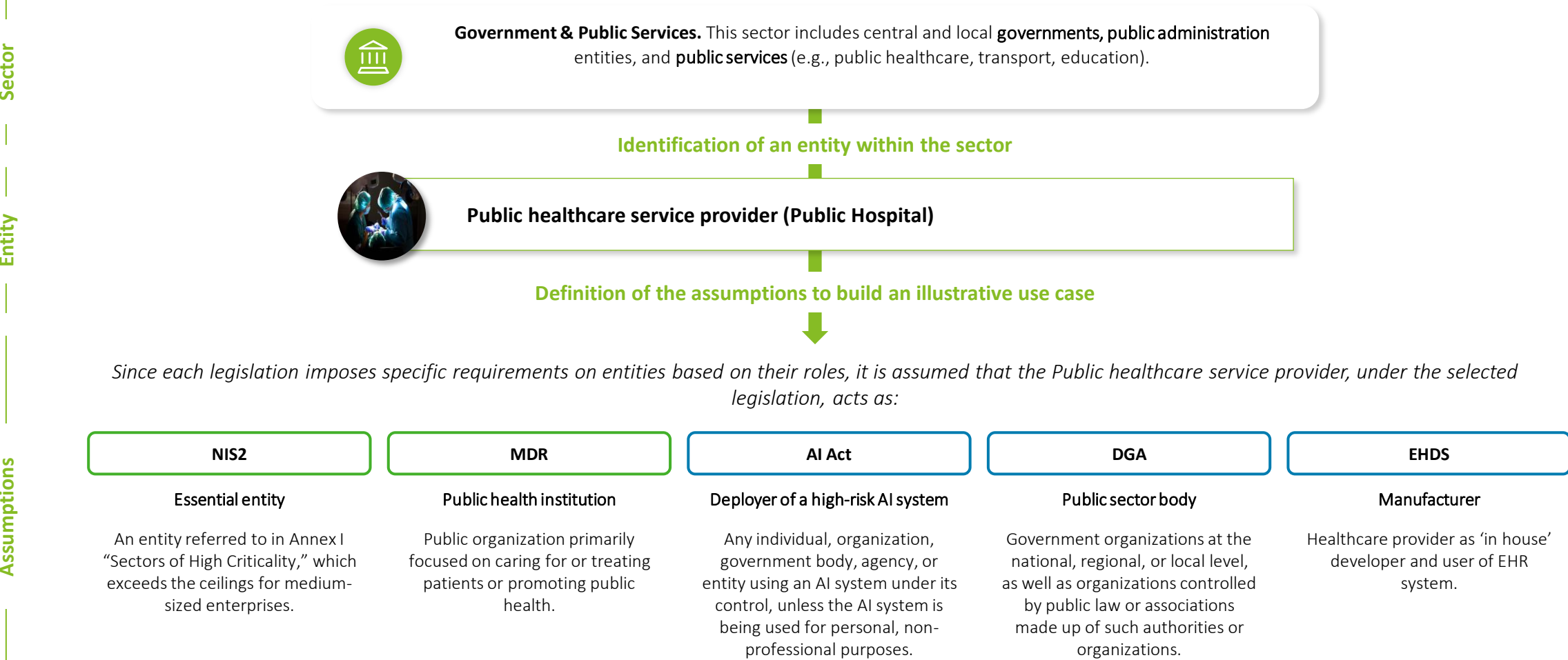
Insurance and reinsurance undertaking

Back to slide 16

Obligations				Regulatory intersection
	DORA ¹	AI Act ²	Data Act ³	How do the EU's cyber and digital laws intersect?
 ICT Security compliance & Certification	✓ Adopt ICT systems, protocols, and tools that are appropriate, reliable, and technologically resilient	x Not covered	x Not covered	<p>The analyzed legislation requires entities to demonstrate compliance with ICT security requirements.</p> <p>DORA provides that entities shall 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</p>
	✓ 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	<p>The analyzed legislation, without prejudice to the overall compliance with data protection obligations under the GDPR, requires entities to comply with additional subject-specific obligations (e.g., ensuring that input data is relevant and sufficiently representative under the AI Act, refrain from using or sharing data for purposes that might damage the data holders or users under the Data Act).</p>
 Data governance & management				

Government & Public Services – Use Case 1 (1/4)

The Government & Public Services’ use case 1 provides an illustrative snapshot of how a Public healthcare service 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



Government & Public Services – Use Case 1 (2/4)

Public healthcare service provider (Public Hospital)

Obligations

Regulatory intersection

	NIS2 ¹	MDR ²	AI Act ³	DGA ⁴	EHDS ⁵
Governance Measures	<ul style="list-style-type: none">✓ 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>	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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 and inform the provider or distributor and relevant market surveillance authority, and suspend the use of that system in case it poses any unacceptable risk	x <i>Not covered</i>	x <i>Not covered</i>

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

The analyzed 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** introduces a general obligation to set a **clear and technology-agnostic risk governance framework**, while subject-specific legislation – such as the AI Act – introduces **vertical requirements**.

Therefore, **compliance** to high-risk AI systems **vertical requirements** **contributes** to the fulfillment of **NIS2 overall governance obligations**

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

As a horizontal legislation, **NIS2** 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. **Medical devices** and **AI systems** used by the entity, being tools, shall be included in the risk management framework, with, respectively, their design and manufacture, as well as implementation and use being documented in adequate policies, as well within the entity's **overall third-party risk management process** (e.g., supply chain mapping, contract review). Therefore, **compliance** to medical devices and high-risk AI systems **vertical requirements** **contributes** to the fulfillment of **NIS2 overall ICT-related risk management obligations**

Government & Public Services – Use Case 1 (3/4)

Public healthcare service provider (Public Hospital)

[Back to slide 16](#)



Obligations

Regulatory intersection

	NIS ¹	MDR ²	AI Act ³	DGA ⁴	EHDS ⁵
Vulnerability Management	<ul style="list-style-type: none"> ✓ 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 Not covered	x Not covered	x Not covered	x Not covered
Incident Management	<ul style="list-style-type: none"> ✓ 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 to national CSIRT, or competent authority, any incident that has a significant impact on the provision of the operator's services 	x Not covered	<ul style="list-style-type: none"> ✓ 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 Not covered	<ul style="list-style-type: none"> ✓ Notify to market surveillance authorities 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

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

The analyzed legislation requires entities 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.

With regard to **AI systems**, **deployers cannot directly test the infrastructure** of the AI system. It is likely that they will oversee the overall security of the AI system through their **overall third-party risk management framework** (e.g. reviewing supply chains and negotiating specific contractual clauses)

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

While NIS2 outlines measures for the notification of **ICT significant incidents** to national CSIRTs, or competent authorities, the AI Act outlines measures for the notification of **serious incidents** to **market surveillance authorities**, and EHDS provides measures for the notification of incidents regarding **EHR systems** to **market surveillance authorities**.

The legislation aims to **simplify and streamline** reporting procedures by encouraging the establishment of national **single-entry points** for the fulfillment 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**

Government & Public Services – Use Case 1 (4/4)

Public healthcare service provider (Public Hospital)

Back to slide 16



Obligations

Regulatory intersection

	NIS2 ¹	MDR ²	AI Act ³	DGA ⁴	EHDS ⁵
ICT Security Compliance & Certification	<ul style="list-style-type: none"> ✓ 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	<ul style="list-style-type: none"> ✓ 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	<ul style="list-style-type: none"> ✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR 	x Not covered	<ul style="list-style-type: none"> ✓ 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 	<ul style="list-style-type: none"> ✓ Ensure that all the conditions for the re-use of data, for which the public sector body is competent, are satisfied, e.g., ensure that the protected nature of data is preserved ✓ Make publicly available the conditions for allowing the re-use of data and the procedure to request the re-use via the single information point 	<ul style="list-style-type: none"> ✓ 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

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

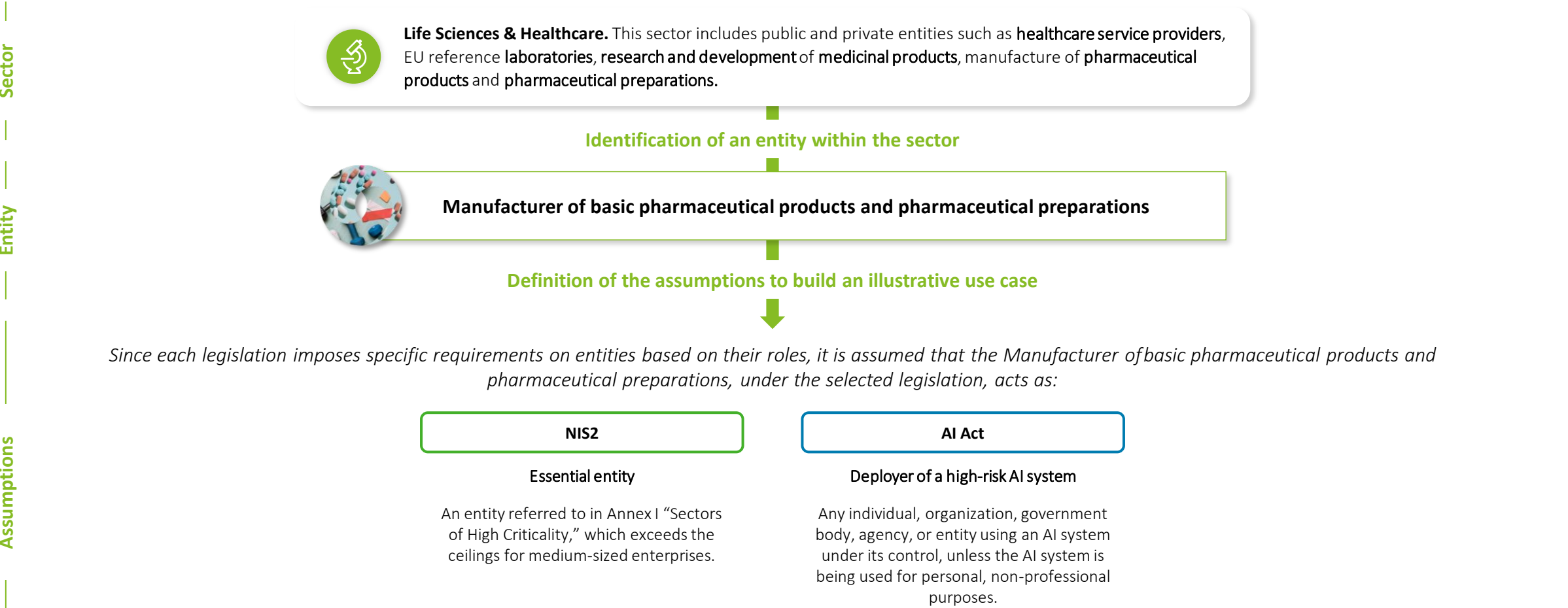
The analyzed legislation requires entities to **demonstrate compliance with ICT security requirements**.

NIS2 provides that Member States **may require** essential and important entities to use particular ICT products, ICT services and ICT processes, either developed by the entity or procured from third parties, that are **certified under European cybersecurity certification schemes** adopted pursuant to Article 49 of Regulation (EU) 2019/881. In the absence of appropriate European cybersecurity certification schemes, Member States shall require entities to comply with **relevant European and international standards** (e.g., upcoming AI standards defined by CEN/CENELEC and standardization of cybersecurity requirements under CRA)

The analyzed legislation, without prejudice to the overall compliance with **data protection obligations under the GDPR**, requires entities to comply with **additional subject-specific obligations** (e.g., ensuring that input data is relevant and sufficiently representative under the AI Act, making publicly available the conditions for allowing the re-use of data under the DGA, and ensuring compliance with interoperability, security and logging requirements under the EHDS)

Life Sciences & Healthcare – Use Case 1 (1/4)

The Life Sciences & Healthcare’s use case 1 provides an illustrative snapshot of how a Manufacturer of basic pharmaceutical products and pharmaceutical preparations 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



Life Sciences & Healthcare* – Use Case 1 (2/4)

Manufacturer of basic pharmaceutical products and pharmaceutical preparations

[Back to slide 16](#)



Obligations

NIS2¹

- ✓ 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**



Governance Measures



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

AI Act²

- ✓ 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 **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 and **inform the provider or distributor** and relevant **market surveillance authority**, and **suspend the use** of that system in case it poses any **unacceptable risk**

Regulatory intersection

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

The analyzed 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** introduces a general obligation to set a **clear and technology-agnostic risk governance framework**, while subject-specific legislation – such as the AI Act – introduces **vertical requirements**.

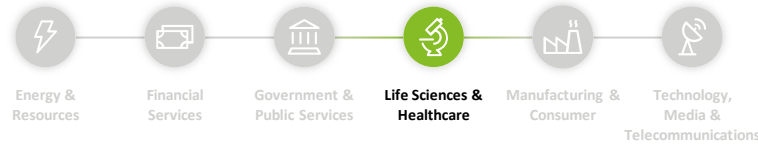
Therefore, **compliance** to high-risk AI systems **vertical requirements** **contributes** to the fulfillment of **NIS2 overall governance obligations**

As a horizontal legislation, **NIS2** 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. **AI systems** used by the entity, being tools, shall be included in the risk management framework, with their implementation and use being documented in adequate policies, as well within the entity's **overall third-party risk management process** (e.g., supply chain mapping, contract review)

Life Sciences & Healthcare – Use Case 1 (3/4)

Manufacturer of basic pharmaceutical products and pharmaceutical preparations

Back to slide 16



Obligations

NIS2 ¹	AI Act ²
<ul style="list-style-type: none">✓ 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	<p>x Not covered</p>
<ul style="list-style-type: none">✓ 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 to national CSIRT, or competent authority, any incident that has a significant impact on the provision of the operator's services	<ul style="list-style-type: none">✓ 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)



Vulnerability Management



Incident Management

Regulatory intersection

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

The analyzed legislation requires entities 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.

With regard to **AI systems**, **deployers cannot directly test the infrastructure** of the AI system. It is likely that they will oversee the overall security of the AI system through their **overall third-party risk management framework** (e.g. reviewing supply chains and negotiating specific contractual clauses)

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

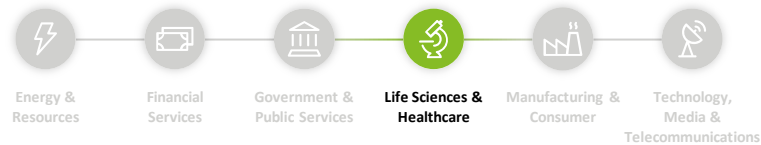
While NIS2 outlines measures for the notification of **ICT significant incidents** to national CSIRTs, or competent authorities, the AI Act outlines measures for the notification of **serious incidents** to **market surveillance authorities**.

The legislation aims to **simplify** and **streamline** reporting procedures by encouraging the establishment of national **single-entry points** for the fulfillment 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**

Life Sciences & Healthcare – Use Case 1 (4/4)

Manufacturer of basic pharmaceutical products and pharmaceutical preparations

Back to slide 16



Obligations

NIS2 ¹	AI Act ²
<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">x Not covered
<ul style="list-style-type: none">✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	<ul style="list-style-type: none">✓ 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

ICT Security Compliance & Certification

Data Governance & Management

Regulatory intersection

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

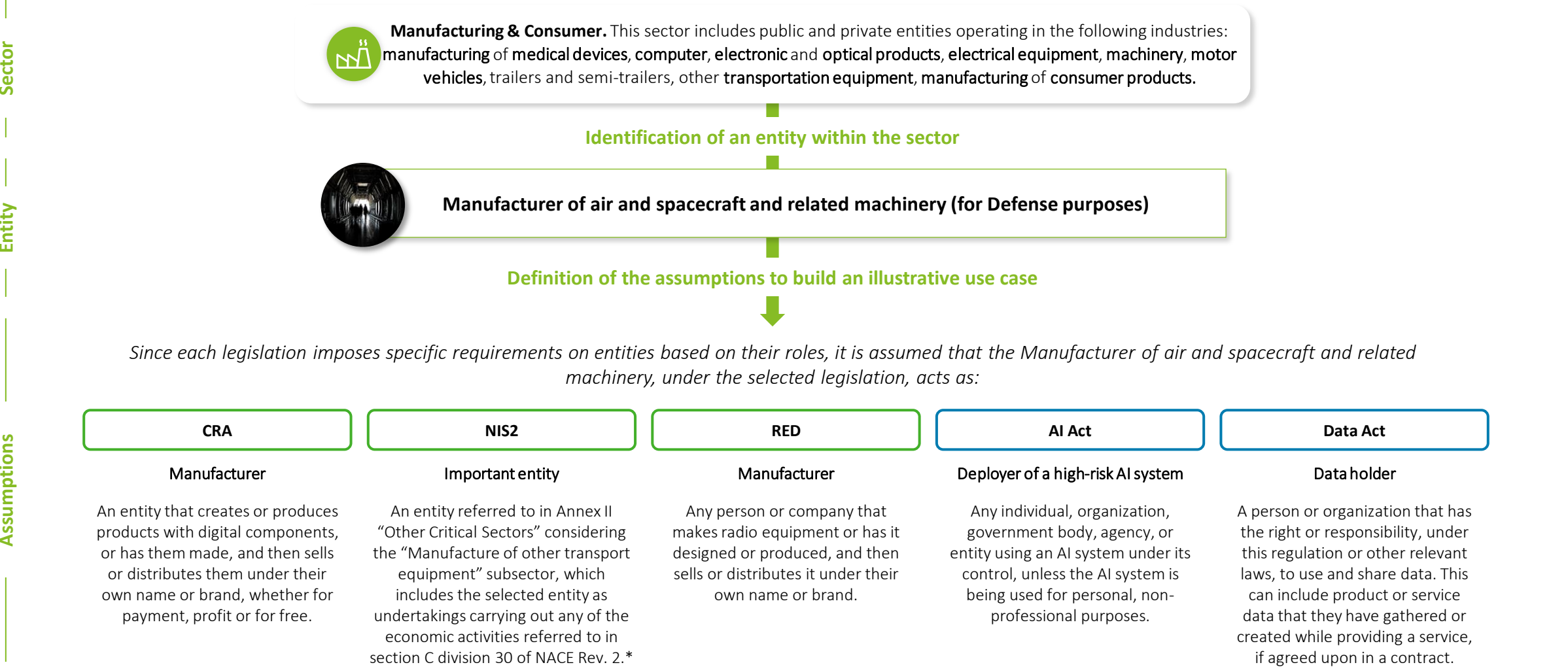
The analyzed legislation requires entities to **demonstrate compliance with ICT security requirements**.

NIS2 provides that Member States **may require** essential and important entities to use particular ICT products, ICT services and ICT processes, either developed by the entity or procured from third parties, that are **certified under European cybersecurity certification schemes** adopted pursuant to Article 49 of Regulation (EU) 2019/881. In the absence of appropriate European cybersecurity certification schemes, Member States shall require entities to comply with **relevant European and international standards** (e.g., upcoming AI standards defined by CEN/CENELEC)

The analyzed legislation, without prejudice to the overall compliance with **data protection obligations under the GDPR**, requires entities to comply with **additional subject-specific obligations** (e.g., ensuring that input data is relevant and sufficiently representative under the AI Act)

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

The Manufacturing & Consumer’s use case 1 provides an illustrative snapshot of how a Manufacturer of air and spacecraft and related machinery 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



Manufacturing & Consumer – Use Case 1 (2/4)

Manufacturer of air and spacecraft and related machinery (for Defense purposes)

Obligations				
CRA ¹	NIS2 ²	RED ³	AI Act ⁴	Data Act ⁵
<div>Governance Measures</div> <ul style="list-style-type: none">Establish and document a quality system that describes, inter alia, the organizational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling of a product with digital elements	<ul style="list-style-type: none">Establish appropriate and proportionate governance measures, i.e. accountability of management bodies for cybersecurity risk management measuresEstablish appropriate and proportionate organizational measures based on an all-hazards approach to manage cybersecurity related risks	<ul style="list-style-type: none">Implement a quality system which, inter alia, describes the quality objectives and the organizational structure, responsibilities and powers of the management with regard to design and product quality	<ul style="list-style-type: none">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 systemEnsure the staff has adequate AI literacyAssign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support	x Not covered
<div>Risk Management & Technical Standards</div> <ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Ensure that radio equipment complies with essential security requirements	<ul style="list-style-type: none">Take appropriate technical measures to ensure that the use of high-risk AI systems is in accordance with the instructions for usePerform a fundamental rights impact assessment (FRIA) for high-risk AI systems before deploymentMonitor 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	<ul style="list-style-type: none">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

Regulatory intersection

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

The analyzed 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** introduces a general obligation to set a **clear and technology-agnostic risk governance framework**, while subject-specific legislation – such as the CRA, RED and AI Act – introduces **vertical requirements**.

Therefore, **compliance** to, respectively, products with digital elements, radio equipment and high-risk AI systems **vertical requirements contributes** to the fulfillment of **NIS2 overall governance obligations**

The analyzed legislation requires entities to set up an **I-related risk management framework**.

As a horizontal legislation, **NIS2** 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. With specific regard to **essential requirements of products with digital elements**, the **Cyber Resilience Act** applies to radio equipment in scope of the RED Directive (and Delegated Regulation): hence, **CRA requirements align with those of RED**, depending on specific requirements.

Finally, **deployers** of high-risk AI systems shall take appropriate **technical measures**. Also, they shall **monitor the use** of such systems. If risks arise, they shall **notify** relevant stakeholders and **suspend** the use of the system.

Manufacturing & Consumer – Use Case 1 (3/4)

Manufacturer of air and spacecraft and related machinery (for Defense purposes)

Obligations						Regulatory intersection
	CRA ¹	NIS2 ²	RED ³	AI Act ⁴	Data Act ⁵	How do the EU's cyber and digital laws intersect?
Vulnerability Management	<ul style="list-style-type: none">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 policiesNotify 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	<ul style="list-style-type: none">Establish appropriate and proportionate technical and operational measures to manage vulnerabilities and report them to the national CSIRT an, where needed, to service recipientsTake into account vulnerabilities specific to direct suppliers and service providers and the overall quality of their products and cybersecurity practices	x Not covered	x Not covered	x Not covered	<p>The analyzed legislation requires entities 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.</p> <p>Obligations under the CRA are strictly complementary to the fulfillment of NIS2. Thus, compliance with the former contributes to the overall compliance of the latter.</p> <p>With regard to reporting obligations, Member States expected to provide single entry points at national level to alleviate administrative burden on entities</p>
Incident Management	<ul style="list-style-type: none">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 impactNotify 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	<ul style="list-style-type: none">Establish appropriate and proportionate technical and operational measures for incident handlingEstablish business continuity measures, such as backup management and disaster recovery, and crisis managementNotify to national CSIRT, or competent authority, any incident that has a significant impact on the provision of the operator's services	x Not covered	<ul style="list-style-type: none">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 incidentInform 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)	<ul style="list-style-type: none">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 (4/4)

Manufacturer of air and spacecraft and related machinery (for Defense purposes)

Obligations

	CRA ¹	NIS2 ²	RED ³	AI Act ⁴	Data Act ⁵
ICT Security Compliance & Certification	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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)	<p>x Not covered</p>	<p>x Not covered</p>
Data Governance & Management	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR	<ul style="list-style-type: none">✓ Radio equipment has to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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

Regulatory intersection

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

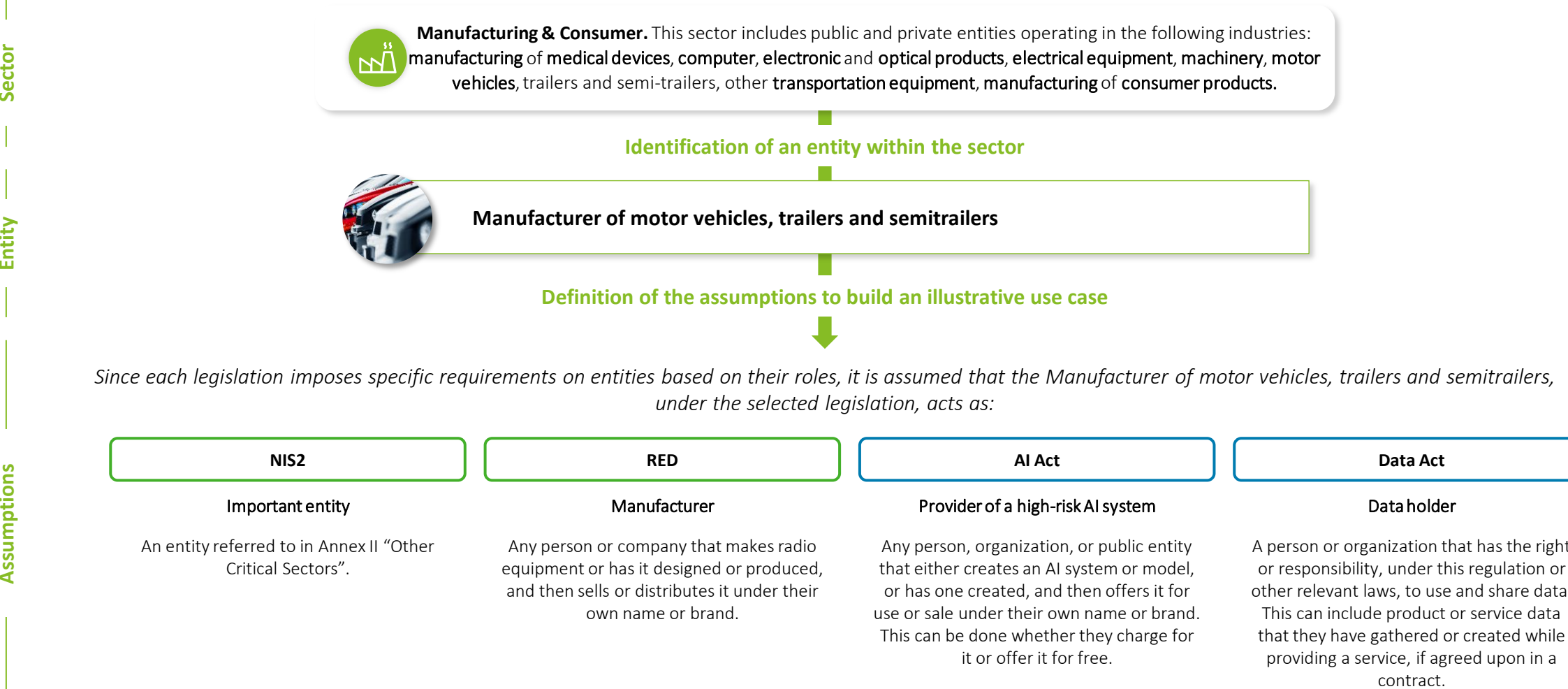
The analyzed legislation requires entities to **demonstrate compliance with ICT security requirements**.

NIS2 provides that Member States **may require** essential and important entities to use particular ICT products, ICT services and ICT processes, either developed by the entity or procured from third parties, that are **certified under European cybersecurity certification schemes** adopted under the **Cybersecurity Act**. In the absence of appropriate European cybersecurity certification schemes, Member States shall require entities to comply with **relevant European and international standards** (e.g., **upcoming AI standards** defined by CEN/CENELEC and **standardization of cybersecurity requirements under CRA**). Entities shall **oversee the compliance with ICT security requirements by providers** as part of their third-party risk management obligations

The analyzed legislation, without prejudice to the overall compliance with **data protection obligations under the GDPR**, requires entities to comply with **additional subject-specific obligations** (e.g., ensuring that **input data is relevant and sufficiently representative** under the **AI Act**, making data available under the Data Act)

Manufacturing & Consumer – Use Case 2 (1/4)

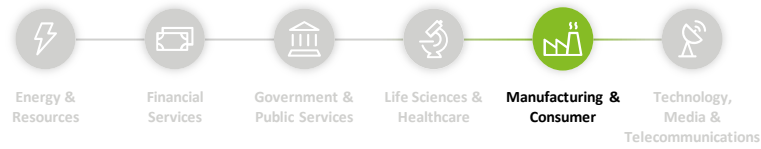
The Manufacturing & Consumer’s use case 2 provides an illustrative snapshot of how a Manufacturer of motor vehicles, trailers and semitrailers is impacted by the identified EU digital and cyber legislation and is based on a set of assumptions that may not account for all possible scenarios



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

Manufacturer of motor vehicles, trailers and semitrailers

Back to slide 16



Obligations

	NIS2 ¹	RED ²	AI Act ³	Data Act ⁴
Governance Measures	<ul style="list-style-type: none">Establish appropriate and proportionate governance measures, i.e. accountability of management bodies for cybersecurity risk management measuresEstablish appropriate and proportionate organizational measures based on an all-hazards approach to manage cybersecurity related risks	<ul style="list-style-type: none">Implement a quality system which, inter alia, describes the quality objectives and the organizational structure, responsibilities and powers of the management with regard to design and product quality	<ul style="list-style-type: none">Put in place and document a quality management system, including an accountability framework detailing roles and responsibilities regarding high-risk AI systemsAssign human oversight to natural persons who have the necessary competence, training and authorityEnsure the staff has adequate AI literacyEnforce the conformity assessment procedure for high-risk AI systemsRegister AI systems and themselves in the EU and, if needed, national database	x Not covered
Risk Management & Technical Standards	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Ensure that radio equipment complies with essential security requirements	<ul style="list-style-type: none">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 arisingPerform a fundamental rights impact assessment (FRIA) for high-risk AI systems before deploymentEstablish 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	<ul style="list-style-type: none"><u>May</u> 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

Regulatory intersection

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

The analyzed 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** introduces a general obligation to set a **clear and technology-agnostic risk governance framework**, while subject-specific legislation – such as RED and AI Act – introduces **vertical requirements**.

Therefore, **compliance** to, respectively, to radio equipment and high-risk AI systems **vertical requirements contributes** to the fulfillment of **NIS2 overall governance obligations**

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

As a horizontal legislation, **NIS2** 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.

With specific regard of high-risk AI systems, **providers** shall establish a **risk management system** throughout the entire lifecycle of a high-risk AI system and **monitor the use** of such systems.

Moreover, entities shall comply with **essential security requirements** envisaged by the RED Directive (and Delegated Regulation).

Manufacturing & Consumer – Use Case 2 (3/4)

Manufacturer of motor vehicles, trailers and semitrailers

Back to slide 16

Obligations

	NIS2 ¹	RED ²	AI Act ³	Data Act ⁴
Vulnerability Management	<ul style="list-style-type: none">✓ 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 Not covered	<ul style="list-style-type: none">✓ 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 Not covered
Incident Management	<ul style="list-style-type: none">✓ 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 to national CSIRT, or competent authority, any incident that has a significant impact on the provision of the operator's services	x Not covered	<ul style="list-style-type: none">✓ Notify to market surveillance authorities 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	<ul style="list-style-type: none">✓ 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

Regulatory intersection

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

The analyzed legislation requires entities 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.

With regard to **AI systems**, providers need to **comply with strict monitoring obligations**, both ante- and post-market. This contributes to the overall NIS2 compliance.

Finally, considering **reporting obligations**, Member States are expected to **provide single entry points** at national level to alleviate administrative burden on entities

The analyzed legislation requires entities to set up appropriate measures for **ICT incident management and reporting**. NIS2 sets a general obligation to **manage incidents throughout their lifecycle** according to recognized standards and frameworks, covering analogous product-specific obligations.

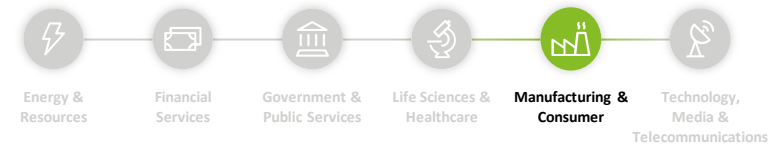
With regard to **incident reporting obligations under NIS2**, Member States are expected to **provide single entry points** at national level to alleviate administrative burden. The **AI Act** requires providers to notify **market surveillance authorities** of serious incidents. However, **it is likely that such authorities will coincide with the single-entry points** designated under NIS2, in order to streamline reporting obligations

Finally, in case of **major cybersecurity incidents**, entities shall **make data available to public sector bodies and Union bodies**.

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

Manufacturer of motor vehicles, trailers and semitrailers

Back to slide 16



Obligations

	NIS2 ¹	RED ²	AI Act ³	Data Act ⁴
ICT Security Compliance & Certification	<ul style="list-style-type: none"> ✓ 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 	<ul style="list-style-type: none"> ✓ 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) 	<ul style="list-style-type: none"> ✓ 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 Not covered
Data Governance & Management	<ul style="list-style-type: none"> ✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR 	<ul style="list-style-type: none"> ✓ Radio equipment has to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected 	<ul style="list-style-type: none"> ✓ 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) 	<ul style="list-style-type: none"> ✓ 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

Regulatory intersection

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

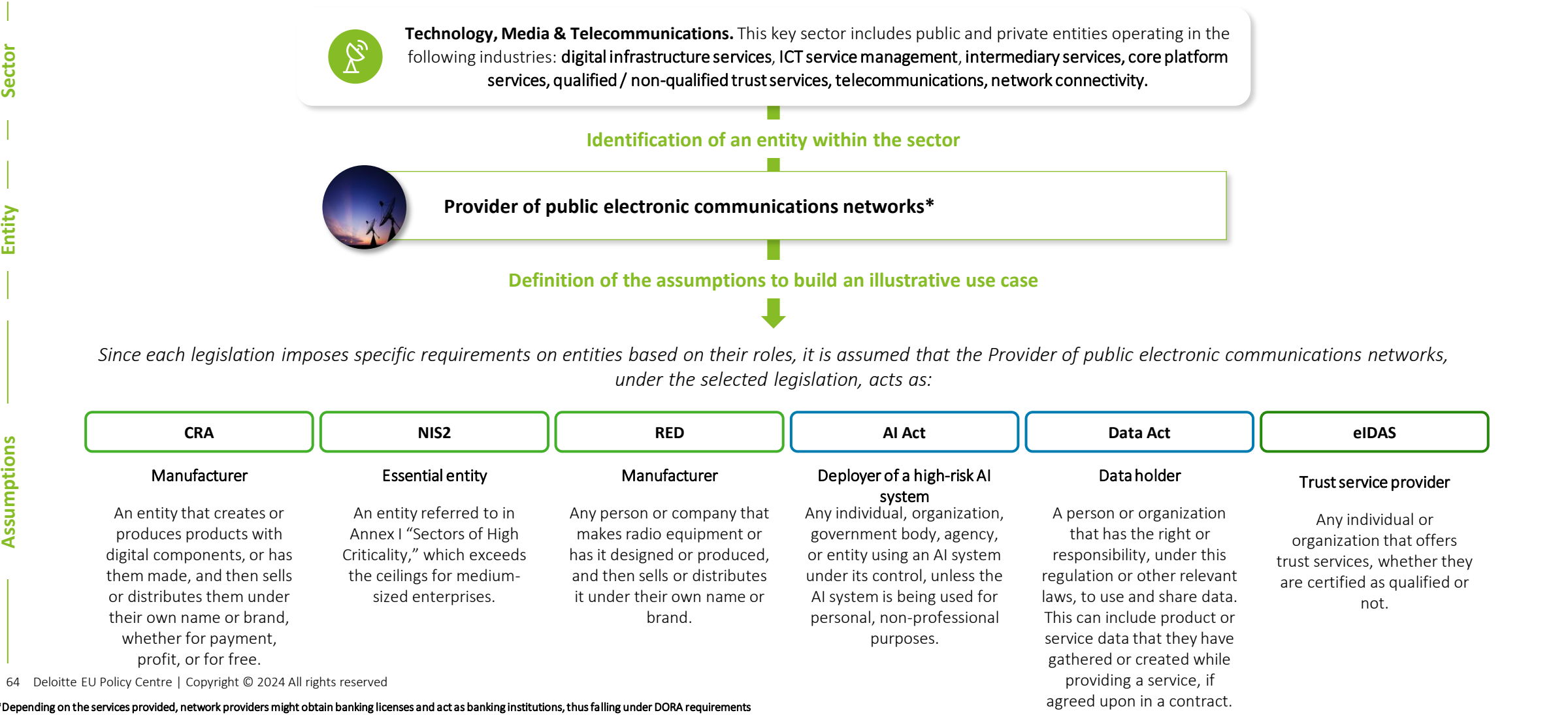
The analyzed legislation requires entities to **demonstrate compliance with security requirements**.

NIS2 provides that Member States **may require** essential and important entities to use particular IT/OT products, services and processes, either developed by the entity or procured from third parties, that are **certified under European cybersecurity certification schemes** adopted under the Cybersecurity Act. In the absence of appropriate European cybersecurity certification schemes, Member States shall require entities to comply with **relevant European and international standards** (e.g., **upcoming AI standards** defined by CEN/CENELEC). Entities shall **oversee the compliance with ICT security requirements by providers** as part of their third-party risk management obligations

The analyzed legislation, without prejudice to the overall compliance with **data protection obligations under the GDPR**, requires entities to comply with **additional subject-specific obligations** (e.g., ensuring that **input data is relevant and sufficiently representative** under the **AI Act**, making data available under the Data Act)

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

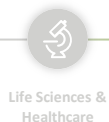
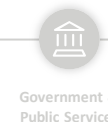
The Government & Public Services’ use case 1 provides an illustrative snapshot of how a Provider of public electronic communications networks is impacted by the identified EU digital and cyber legislation and is based on a set of assumptions that may not account for all possible scenarios



Technology, Media & Telecommunications – Use Case 1 (2/4)

Provider of public electronic communications networks

Back to slide 16



Obligations

Regulatory intersection

CRA¹

NIS2²

RED³

AI Act⁴

Data Act⁵

eIDAS⁶

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



Governance Measures

✓ Establish and document a **quality system** that describes, inter alia, the **organizational 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

✓ Implement a **quality system** which, inter alia, describes the **quality objectives** and the **organizational 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 Not covered

✓ Take appropriate **organizational 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**

The analyzed legislation requires entities to **review their internal governance systems** in view to establishing clear **roles and responsibilities** for overseeing and managing ICT-related risks. Being a horizontal legislation, NIS2 introduces a general obligation to set a **clear and technology-agnostic risk governance framework**, while subject-specific legislation – such as CRA, RED, AI Act, and eIDAS – introduces **vertical requirements** the compliance with which contributes to the overall fulfilment of governance obligations



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

✓ 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 **FRIA** for high-risk AI systems before deployment
✓ **Monitor the operation of the high-risk AI system** based on the instructions for use and share relevant data with providers and **inform the provider or distributor** and relevant **market surveillance authority**, and **suspend the use of that system** if it poses **unacceptable risk**

✓ **May** apply appropriate **technical protection measures**, including smart contracts and encryption, to prevent **unauthorised access to data**, including metadata, and to ensure compliance with data sharing obligations and with the agreed contractual terms for making data available

✓ Take appropriate **technical and organizational 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)

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

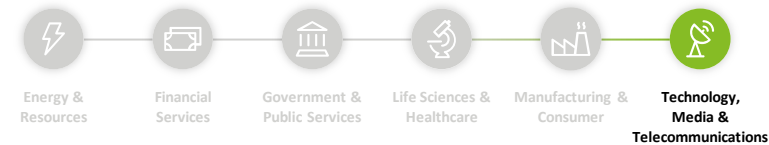
As a horizontal legislation, NIS2 introduces a broad obligation to set up a **comprehensive, documented and regularly updated risk management framework**, including strategies, policies, procedures, ICT protocols and tools to prevent, detect and manage ICT-related risks.

Other subject-specific **risk management obligations** (e.g., under the CRA, RED, AI Act, Data Act, and eIDAS) constitute further specifications of the overall risk management framework that entities need to implement. Hence, compliance with the latter contributes to the overall NIS2 compliance

Technology, Media & Telecommunications – Use Case 1 (3/4)

Provider of public electronic communications networks

Back to slide 16 ↗



Obligations

Regulatory intersection

CRA¹

NIS2²

RED³

AI Act⁴

Data Act⁵

eIDAS⁶

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



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 Not covered

x Not covered

x Not covered

- ✓ Perform a regular 2-year **vulnerability assessment** to maintain the **certification of conformity** for **qualified electronic signature creation devices**

The analyzed legislation requires entities 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.

With regard to **AI systems**, **deployers cannot directly test the infrastructure** of the AI system. It is likely that they will oversee the overall security of the AI system through their **overall third-party risk management framework** (e.g. reviewing supply chains and negotiating specific contractual clauses)



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** to **national CSIRT**, or **competent authority**, any **incident** that has a **significant impact** on the provision of the operator's services

x Not covered

- ✓ **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

- ✓ Take appropriate technical and **organizational 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

The analyzed legislation requires entities to set up appropriate measures for **ICT incident reporting and handling**. While NIS2 outlines measures for the notification of **ICT significant incidents** to national CSIRTs, or competent authorities, the **CRA** and **eIDAS** outline, respectively, measures for the notification of **severe incidents** to CSIRTs and breach of security or loss of integrity to supervisory authorities. Furthermore, reporting obligations set out in **eIDAS** have to be considered **complementary** to those outlined in **NIS2**. The legislation aims to **simplify and streamline** reporting procedures by encouraging the establishment of national **single-entry points** for the fulfillment 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**. Finally, in case of **major cybersecurity incidents**, entities shall **make data available to public sector bodies and Union bodies**.

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

Provider of public electronic communications networks

Obligations

	CRA ¹	NIS2 ²	RED ³	AI Act ⁴	Data Act ⁵	eIDAS ⁶
ICT Security Compliance & Certification	<ul style="list-style-type: none"> ✓ 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 	<ul style="list-style-type: none"> ✓ 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 	<ul style="list-style-type: none"> ✓ 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) ✓ Affix the CE marking 	x Not covered	x Not covered	<ul style="list-style-type: none"> ✓ 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
Data Governance & Management	<ul style="list-style-type: none"> ✓ 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 	<ul style="list-style-type: none"> ✓ Comply with fundamental data protection obligations, including the obligation to carry out a Data Protection Impact Assessment (DPIA), as per the GDPR 	<ul style="list-style-type: none"> ✓ Radio equipment must incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected 	<ul style="list-style-type: none"> ✓ 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 	<ul style="list-style-type: none"> ✓ 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 	<ul style="list-style-type: none"> ✓ 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)

Regulatory intersection

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

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

NIS2 provides that Member States **may require** essential and important entities to use particular ICT products, ICT services and ICT processes, either developed by the entity or procured from third parties, that are **certified under European cybersecurity certification schemes** adopted under the Cybersecurity Act. In the absence of appropriate European cybersecurity certification schemes, Member States shall require entities to comply with **relevant European and international standards** (e.g., **upcoming AI standards** defined by CEN/CENELEC and **standardization of cybersecurity requirements under CRA**). Entities shall **oversee the compliance with ICT security requirements by providers** as part of their third-party risk management obligations. Finally, **CRA requirements** are aligned to requirements of the **RED Delegated Regulation**

The analyzed legislation, without prejudice to the overall compliance with **data protection obligations under the GDPR**, requires entities to comply with **additional subject-specific obligations** (e.g., ensuring that input data is relevant and sufficiently representative under the AI Act, making data available under the Data Act, and taking appropriate measures against forgery and theft of data under eIDAS)



Introduction to the EUPC



Introduction to the EUPC Digital Playbook



Technology Trends and the EU Digital Strategy



EU Digital Legislation and Key Sectors Overview



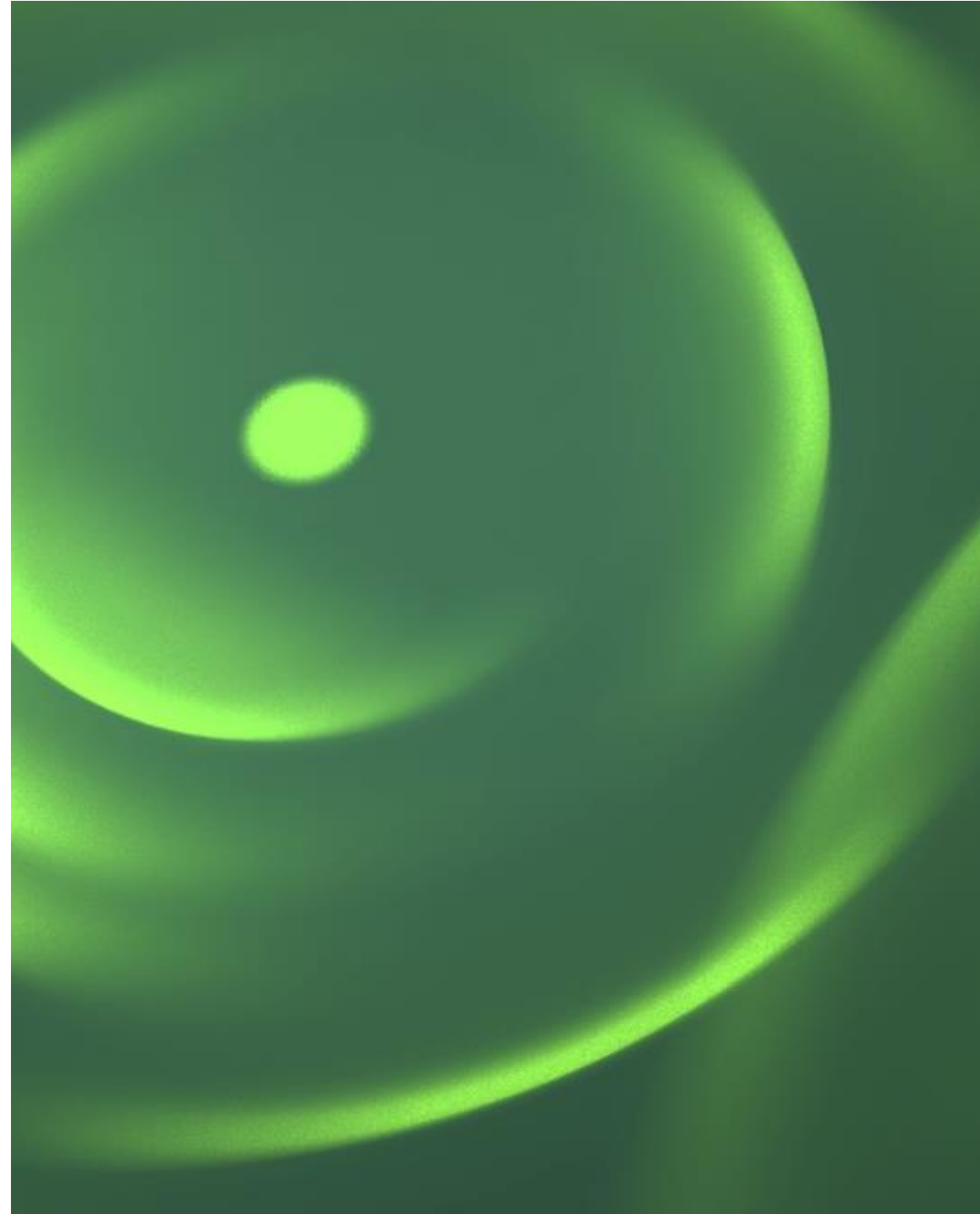
EU Digital Legislation Detail Cards



Key Sectors Use Cases

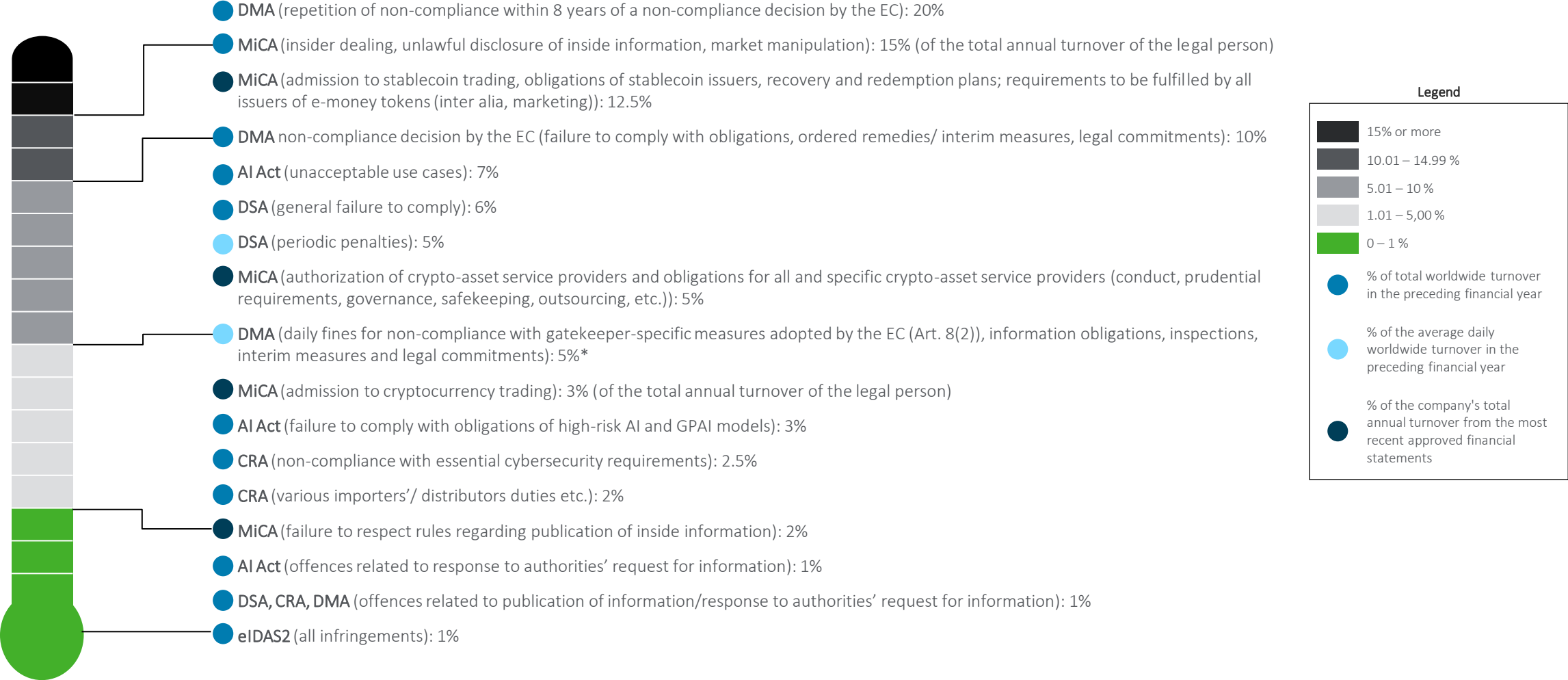


Annex



Annex A | Level of penalties (1/2)

Non-compliance with the identified digital regulations can lead to a wide range of penalties depending on the total worldwide turnover or the average daily global turnover of the entities subject to the obligations



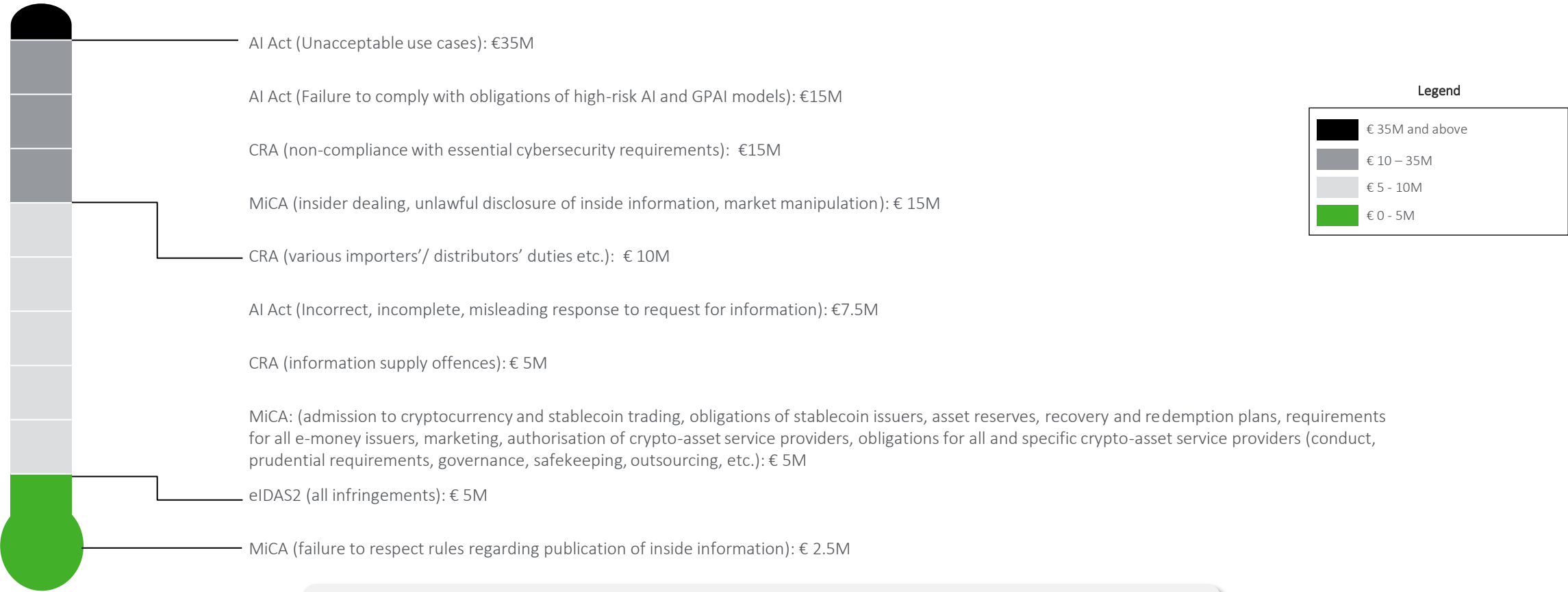
(*) Subject to a 5-year limitation period

(**) DSA only defines maximum penalties; Member States remain responsible for setting penalties. Hence, differences between Member States may arise

Annex A | Level of penalties (2/2)

Non-compliance with the identified digital regulations can lead to a wide range of penalties depending on the total worldwide turnover or the average daily global turnover of the entities subject to the obligations

Maximum penalties



*Note: when deciding between percentage of turnover or a fixed sum, in case of the AI Act, the principle of “whichever is greater” applies, unless the perpetrator is an SME (to which “whichever is lower” applies).
In case of the CRA and eIDAS2, the principle of “whichever is greater” applies.*

Annex B | References (1/2)

List of published legislation and proposals leveraged to develop the EU Policy Centre Playbook

— Legislation published on the EU Official Journal —

- Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0042>
- 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. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0053&qid=1712308517483>
- 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. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910>
- 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. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745>
- Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive. Available at: https://eur-lex.europa.eu/eli/reg_del/2022/30/oj
- 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). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&qid=1712309340916>
- 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). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925&qid=1712309021502>
- Directive (EU) 2022/2380 of the European Parliament and of the Council of 23 November 2022 amending Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.315.01.0030.01.ENG&toc=OJ%3AL%3A2022%3A315%3ATOC
- 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). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1712308948124>
- 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. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&qid=1712306799442>
- 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). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400903

Annex B | References (2/2)

List of published legislation and proposals leveraged to develop the EU Policy Centre Playbook

- 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 (NIS 2 Directive). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1712306799442>
- 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. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114&qid=1712307150661>
- 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. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1230&qid=1712308012293>
- Commission Delegated Regulation (EU) 2023/1717 of 27 June 2023 amending Directive 2014/53/EU of the European Parliament and of the Council as regards the technical specifications for the charging receptacle and charging communication protocol for all the categories or classes of radio equipment capable of being recharged by means of wired charging. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.223.01.0001.01.ENG
- 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). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1712309401277>
- 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) (Text with EEA relevance). Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- 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. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>
- Regulation of the European Parliament and of the Council 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). Available at: <https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/en/pdf>

Proposals

- Proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, and amending Regulation (EU) 2021/694. Available at: <https://www.consilium.europa.eu/media/69093/st16996-en23.pdf>
- Proposal for a Regulation on the European Health Data Space – Compromise text (March 2024). Available at: <https://www.consilium.europa.eu/media/70909/st07553-en24.pdf>

Annex C | 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 Policy Lead
egiglio@deloitte.it



Mosche Orth
Manager

moorth@deloitte.de



Wouter Lamers
Consultant

wlamers@deloitte.com

Support Team



Biagio Salerno
Director
bsalerno@deloitte.it



Alessia Sposini
Consultant
asposini@deloitte.it



Nicolò Benussi
Analyst
nibenussi@deloitte.it

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

Subject Matter Experts



Manel Carpio

Partner

Spain

macarpio@deloitte.es



Elisa de Hevia

Partner

Spain

edehevia@deloitte.es



Ljuba Kerschhofer-Wallner

Partner

Germany

lkerschhoferwallner@deloitte.de



Koen Magnus

Partner

Belgium

kmagnus@deloitte.com



Simone Pelkmans

Partner

Netherlands

spelkmans@deloitte.nl



Lorenzo Russo

Partner

Italy

lorusso@deloitte.it



Jan-Jan Lowijs

Director

Netherlands

jlowijs@deloitte.nl



Hanne Van Kerckhoven

Director

Belgium

hvankerckhoven@deloitte.com



Raf Geuns

Snr Manager

Belgium

rgeuns@deloitte.com



Henner Jose Truchsess

Snr. Manager

Spain

htruchsess@deloitte.es



Santiago Calvo Fantova

Manager

Spain

scalvofantova@deloitte.es