EUROSMART
The Voice of the Digital Security Industry

EU Cybersecurity Regulatory Landscape

May 2024

About Eurosmart

Eurosmart is a European not for profit organisation dedicated to advancing the digital security industry through innovation, standardisation and certification, and advocacy. With a rich history spanning decades, Eurosmart serves as a trusted voice in the field, representing a diverse range of stakeholders including manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations and associations.

Committed to fostering a secure and trustworthy digital environment, Eurosmart engages in proactive initiatives to promote the adoption of robust security solutions and standards. By leveraging its expertise and extensive network, Eurosmart plays a pivotal role in shaping the future of cybersecurity and digital transformation across Europe and beyond.

Disclaimer

This document succinctly outlines a selection of key EU cybersecurity regulations and offers a concise summary of the primary provisions for each regulation, condensed into a single page. This publication is accompanied by a synoptic table illustrating the main developments for each regulation.

This publication is for informational purposes only and has been edited using publicly available information as of the date of publication. The interpretation and analysis do not necessarily represent the position or opinion of Eurosmart. Eurosmart bears no liability for the accuracy or validity of the information presented.

Copyright notice

Table of contents

Introduction

In the ever-evolving landscape of cybersecurity regulations, Europe stands as a pioneer in fostering compliance frameworks that facilitate the growth of a robust digital society. However, this journey towards regulatory excellence isn't without its complexities. As Europe strides forward in regulating various facets of digitalisation, a myriad of regulations emerges, each wielding its influence and impact. Navigating this regulatory maze requires vigilant monitoring, understanding, and discernment, even when the interrelations between regulations may not be immediately apparent.

Amidst this intricate regulatory ecosystem, the need for comprehensive mapping and understanding becomes paramount. Eurosmart has undertaken this task, and here are the results. This document aims to assist the digital industry ecosystem in easily navigating the various EU regulatory initiatives. It provides a set of overviews summarizing the most relevant regulations in the areas of Cybersecurity, Market Surveillance and Market Access, Data, Platforms and Competition, e-Commerce and Consumer Protection, Data Identity, and Digital Industrial Policy.

Recognising this imperative, our endeavour embarks on an exercise to distil the essence of these regulations, unravelling their key elements, enforcement mechanisms, implications, and current status. Moreover, we provide a timeline encapsulating the evolution of these regulations and offer insights into the underlying frameworks driving their formulation and implementation.

European legalese

Legislation

Legislation refers collectively to all laws and legal acts enacted by the European Union to govern various aspects of EU policies and activities. This encompasses all forms of EU legal acts, including regulations, directives, decisions, and related measures aimed at governing various aspects of EU policy and law.

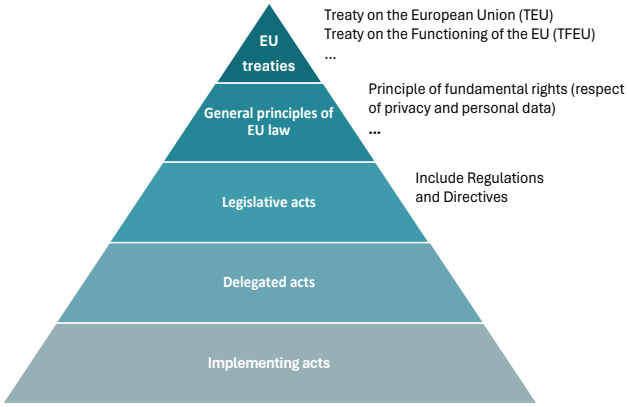

Figure 1. Hierarchy of sources of EU law

1. Legislative Acts

A legislative act in the EU refers to an act that is adopted through the legislative procedure laid down in the EU Treaties. These acts have the highest legal force and directly create EU law. They are binding on EU Member States and individuals within those states. Legislative acts can take various forms:

- Regulation: A Regulation is a binding legislative act of the European Union that applies directly and uniformly across all EU Member States without the need for national implementation. Regulations are immediately enforceable as law in all Member States upon entry into force.
- Directive: A Directive is a legislative act that sets out a goal that all EU Member States must achieve but leaves the choice of form and method to the individual states. Member States must transpose directives into national law within a specified timeframe.

2. Non-Legislative Acts

A non-legislative act in the EU refers to an act that is adopted through administrative or executive procedures, rather than through the legislative procedure defined in the EU Treaties. Non-legislative acts provide further details, implementation measures, or decisions based on the framework established by legislative acts. They do not create new EU law but are important for the implementation and enforcement of existing EU legislation. Non-legislative acts can include:

- Decision: A Decision is a legal act adopted by EU institutions (such as the European Commission or the Council of the EU) or by EU agencies. Decisions are binding in their entirety upon those to whom they are addressed. They are specific to particular cases, individuals, or entities and are used to address specific administrative situations or to implement EU law precisely.
- Delegated Act: A Delegated Act is a legal act adopted by the European Commission under powers delegated by the European Parliament and the Council. It supplements or amends non-essential parts of EU legislative acts (such as regulations or directives) and have a limited scope of application.
- Implementing Act: An Implementing Act is a legal act adopted by the European Commission to ensure uniform application of an EU legislative act (such as regulations or directives) across all EU Member States. It specifies how the provisions of the legislative act should be applied in practice.

	Delegated acts (Article 290 TFEU)	***Implementing acts (Article 291 TFEU)***
Legal nature	Act of general application only	Act of general or individual application
Purpose	To amend or supplement non-essential elements in the basic act	To ensure uniform conditions for implementing legally binding EU acts
Type of basic act	Legislative act only	Legislative or non-legislative act
Modification of basic act	Yes, if concerning non-essential elements	Excluded
Author of executive act	European Commission	European Commission or Council (in the common foreign and security policy and in exceptional situations)
General act governing procedure	Common Understanding on Delegated Acts (annexed to the Interinstitutional Agreement Better Law Making of 2016)	Comitology Regulation (2011)
European Parliament and Council's rights	Objection and/or revocation of delegation Parliament and Council generally have two months to formulate any objections. If they do not, the delegated act enters into force.	Scrutiny Parliament or the Council can object that the implementing act exceeds the implementing powers provided for in the basic act.
Member States' involvement	Member States' experts present in expert groups, with purely advisory role	Member States' experts sit on comitology committees (provided for by the Comitology Regulation) and may veto the proposed measure by qualified majority voting (QMV)

Table 1. Main differences between delegated acts and implementing acts.

Source: EPRS briefing on understanding delegated and implementing acts

3. Policy documents

- Communication: a Communication is a formal document issued by the European Commission to outline policy initiatives, provide guidance, or present information on specific topics. It serves as a means of communication between EU institutions, Member States, and stakeholders. Communications are not legally binding but reflect the Commission's position or proposed actions on specific issues.

Cybersecurity

This chapter deals with European legislation that has spearheaded efforts towards secure digitalisation. This set of regulations is driving norms for world-class solutions, cybersecurity standards, and the protection of essential services and critical infrastructures, as well as promoting the development and application of new technologies.

This array of legislation serves as the foundation upon which the EU's cybersecurity strategy is constructed, furnishing essential mechanisms and governance structures. The NIS Directive marks a significant milestone as the inaugural EU-wide legislation dedicated to cybersecurity, enacting legal measures aimed at elevating the overall cybersecurity posture within the EU. Complementing this, the Cybersecurity Act bolsters the resilience outlined in the NIS Directive by endowing ENISA – the European cybersecurity agency – with a permanent mandate and establishing the EU cybersecurity certification framework. More recently, the Digital Operational Resilience Act (DORA) has been enacted to delineate specific rules for enhancing the resilience of the banking sector.

The 2020 EU cybersecurity strategy, straighten the need to provide collective strategy to respond to major cyberattacks while promoting the EU's technological sovereignty to support such a collective resilience.

Beyond the establishment of a robust legal framework, the EU's cybersecurity approach encompasses investment tools such as the Digital Europe Programme and the Horizon Europe programme, supported by a network of national and EU governance structures provided by the national and European Cybersecurity Competence Centres.

For Eurosmart's members, comprehensive analysis, and updates on ongoing developments in EU cybersecurity-related legislations are readily accessible through the online EU issue tracker.

The Cybersecurity Act (CSA)

Regulation (EU) 2019/881on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification

Legacy:
- ✓ *New regulation on cybersecurity certification*
- ↺ *Repealing Regulation (EU) 526/2013 (ENISA's mandate)*

Requirements
- ✓ *Voluntary unless otherwise provided by other Union legal acts*

The Cybersecurity Act aims to bolster ENISA's organisational framework and replace outdated cybersecurity certification regulations. The proposal as a Regulation underscored the need for a unified approach to cybersecurity within the EU.

Key objectives of the CSA

The CSA aims to enhance cybersecurity coordination across Member States and EU institutions while fostering trust in critical infrastructures and consumer devices. It seeks to establish an EU Cybersecurity Agency and implement a comprehensive EU-wide certification framework to ensure trust in critical infrastructures and consumer devices.

Scope and coverage

The proposed CSA provides a permanent mandate to the EU Cybersecurity Agency (ENISA) to improve coordination and cooperation across the Union, as well as to prevent and to respond to cyber-attacks. Additionally, it aims to implement a robust certification framework to ensure the ICT products, processes, and services.

The CSA identifies three risk-based approach assurance levels with different types of assessments: Basic (can include self-assessment), Substantial (evaluation by a third-party), and High (including mandatory penetration testing). Essentially, each assurance level specifies the required resilience of a particular product, service, or process against cyberattacks with different sophistication and resources. For instance, achieving high assurance certification implies safeguarding against advanced attacks from attackers with significant skills and resources.

However, various EU regulations, including the NIS2 directive, the Artificial Intelligence Act, and the Cyber Resilience Act, task the European Commission with outlining CSA certification requirements under these regulations.

Mandatory certification will come in different forms. It might be required for accessing the EU market with certain products or services or within specific sectors, or through public procurement at national level. Alternatively, certification could serve as a basis for the "presumption of conformity" with cybersecurity requirements outlined in particular regulations.

Mandatory vs voluntary certification

The EU cybersecurity certification process is voluntary unless otherwise specified in other EU law. (cf. NIS 2 or CRA)

National cybersecurity certification schemes

The CSA establishes the supremacy of EU schemes over national schemes. Member States are obligated to implement EU certification schemes at the national level. This requirement ensures uniformity in cybersecurity standards and compliance across the EU, strengthening the overall cybersecurity framework.

Managed Security Services

In April 2023, a new proposal for a regulation was presented with the intention to amend the scope of the European cybersecurity certification framework to enable the adoption of European cybersecurity certification schemes for "managed security services". Managed security services are services consisting of carrying out or providing assistance for activities relating to their customers' cybersecurity risk management.

Timeline

- September 13th, 2017: Commission presents proposal for regulation for a Cybersecurity Act.
- June 27th, 2019: Regulation entered into force.
- April 18th, 2023: Commission presents proposal for Regulation on managed security services.
- January 31st, 2024: Commission adopts EUCC Implementing Regulation.

Cyber Solidarity Act

Proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

Legacy:	Requirements:
✓ *New regulation*	✓ *Voluntary framework*

The EU Cyber Solidarity Act is a legislative initiative aimed at strengthening the European Union's capacity to detect, prepare for, and respond to cybersecurity threats and incidents. It builds upon the objectives outlined in the EU Cyber Solidarity Initiative, focusing on enhancing common detection, situational awareness, and response capabilities across the EU. It is mainly supported by the Digital Europe Programme (DEP), providing funding for projects in crucial areas.

Key objectives of the European Union Cyber Solidarity Act

The Act seeks to achieve several key objectives, including strengthening common EU detection, situational awareness, and response capabilities, gradually building an EU-level cybersecurity reserve, and supporting the testing of critical entities to enhance their preparedness.

Scope and Coverage

The EU's Cyber Solidarity Act scope encompasses the establishment of the European Cyber Shield, a pan-European infrastructure comprised of Security Operations Centres (SOCs), to enhance detection and situational awareness. Additionally, it creates a Cyber Emergency Mechanism to support Member States in preparing for and responding to significant cybersecurity incidents. Furthermore, it establishes the European Cybersecurity Incident Review Mechanism to assess specific incidents.

Implementing Acts

The EU's Cyber Solidarity Act grants the Commission the authority to adopt implementing acts to specify operational and procedural details, including conditions for interoperability between cross-border SOCs and procedural arrangements for information sharing.

European Cybersecurity Reserve

The act mandates the creation of a European Cybersecurity Reserve, consisting of incident response services from trusted providers, selected based on specified criteria.

To support the establishment of the EU Cybersecurity Reserve, the Commission could consider requesting the preparation of a European cybersecurity certification scheme for managed security services in the areas covered by the Cyber Emergency Mechanism.

Timeline and next steps

- April 18th, 2023: Commission presents proposal for regulation for a European Union Cyber Solidarity Act.
- March 6th, 2024: Provisional agreement reached on the Cyber Solidarity Act.
- Date TBD: The text will undergo negotiations between the Council and the European Parliament, leading to its formal adoption, publication in the EU Official Journal, and entry into force 20 days after publication.

The Digital Operational Resilience Act (DORA)

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector

Legacy:	Requirements:
✓ *New regulation*	⚠ *Mandatory compliance*

In the dynamic realm of EU financial regulation, the Digital Operational Resilience Act (DORA) emerges as a cornerstone initiative, strategically designed to address the evolving landscape of ICT risks. Rooted in the imperative of fortifying digital resilience, DORA embodies a comprehensive framework aimed at safeguarding the EU financial sector against emerging threats.

Key objectives of DORA

DORA is designed to address the evolving landscape of ICT risks within the EU financial sector, aiming to enhance operational resilience by mandating rules for protection, detection, containment, recovery, and repair capabilities against ICT-related incidents. It seeks to ensure a high common level of digital operational resilience through uniform requirements applicable to financial entities, including ICT risk management, incident reporting, resilience testing, information sharing, and third-party risk management.

Scope and Coverage

DORA's scope mandates uniform requirements to ensure consistent digital operational resilience. Additionally, DORA acts as the central regulatory instrument, aiming to harmonise cybersecurity requirements for the financial sector, integrating with existing regulations such as PSD2 and MiFID2 to create a cohesive framework for cybersecurity resilience.

Delegated Acts

Recent developments include the adoption of delegated acts by the European Commission that aim to specify criteria for the classification of ICT-related incidents, materiality thresholds, contractual arrangements with ICT service providers, and harmonisation of ICT risk management tools, methods, processes, and policies.

Compliance and Regulatory technical standards

DORA highlights the responsibility of financial entities to evaluate critical third-party service providers, guided by technical advice from the European Supervisory Authorities (ESAs), to ensure adherence to regulatory standards. Additionally, DORA imposes financial entities to comply with prescribed standards for ICT risk management and operational resilience. Though specific requirements are yet to be finalised, DORA is set to enhance ICT risk management and operational resilience within the financial sector.

Timeline and next steps

- September 24th, 2020: Commission presents proposal for regulation for a Digital Operational Resilience Act Delegated Regulation.
- December 27th, 2022: Final text of DORA published in the Official Journal of the European Union as Regulation (EU) 2022/2554.
- January 16th, 2023: DORA entered into force.
- Expected by the end of 2024: DORA's Delegated regulations to be adopted by the Commission and to be published in the EU Official Journal.

NIS2 Directive

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)

Legacy:	**Requirements:**
✓ *Repealing Directive (EU) 2016/1148 (NIS 1 Directive)*	⚠ *Mandatory compliance to cybersecurity requirements* ⚠ *Mandatory EU cybersecurity certification schemes*

The NIS2 Directive stands as a pivotal legislative stride towards fortifying cybersecurity within the European Union. Member States must ensure that 'essential' and 'important' entities implement appropriate and proportionate technical, operational, and organisational measures to handle security risks related to network and information systems. These measures aim to prevent or mitigate the effects of incidents on recipients of their services and on other services, employing an all-hazards approach.

Key objectives of the NIS2 Directive

The NIS2 Directive sets out to enhance cybersecurity within the European Union by achieving a high common level of security. Its key objectives include ensuring essential and important entities adopt measures to manage cybersecurity risks effectively and minimise the impact of incidents on services.

These measures are based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents. At a minimum, these measures include:

- Risk analysis and information systems security policies;
- Incident handling;
- Business continuity;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers' security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure;
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- Basic cyber hygiene practices and cybersecurity training;
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- Human resources security, access control policies and asset management;
- The use of multi-factor authentication or continuous authentication solutions, secured communications, and secured emergency communication systems.

Moreover, essential, and important entities must report any significant incident without delay to the competent national authorities.

Scope and Coverage

The directive's scope covers a broad range of sectors and activities, encompassing medium-sized and large entities operating within them. The sectors are divided into two groups.

The sectors of high criticality:

- Energy (electricity, district heating and cooling, petroleum, natural gas, hydrogen);
- Transport (air, rail, water, road);
- Banking;
- Financial market infrastructure;
- Health (which no longer only includes hospitals but now also includes reference laboratories, medical devices or pharmaceutical preparation manufacturers and others);
- Drinking water;
- Water waste;
- Digital infrastructure;
- ICT service management;
- Public administration (central and regional);
- Space.

Other critical sectors:

- Postal and courier services;
- Waste management;
- Manufacture, production and distribution of chemicals;
- Production, processing, and distribution of food;
- Manufacturing (of medical devices and *in vitro* diagnostic medical devices; computer, electronic and optical products; electrical equipment; machinery and equipment n.e.c., motor vehicles, trailers, and semi-trailers; other transport equipment);
- Digital providers;
- Research.

Delegated Acts

Under the NIS2 Directive, important delegated acts define technical requirements for specific service providers and establish a voluntary peer review mechanism to enhance cybersecurity capabilities and alignment with sector-specific legislation (such as DORA, and GDPR). Notably, the directive emphasises equivalence with such legislation to ensure effectiveness.

Certification Obligations

After a consultation with stakeholders, the Commission is empowered to adopt delegated acts by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or to obtain a certificate under a European cybersecurity certification scheme to comply with the NIS2 obligations.

In addition, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes.

Timeline

- December 16th, 2020: Commission presents proposal for a NIS2 Directive.
- January 16th, 2023: NIS2 Directive entered into force.
- From October 18th, 2024: NIS1 Directive is repealed.
- October 2024: Delegated Acts to be published on mandatory cybersecurity certification.

Market Surveillance and Market Access

This chapter delves into a selection of legislations governing the placing of products on the European market. This framework encompasses both horizontal legislations, such as the Cyber Resilience Act (CRA) which apply broadly across various product categories, and vertical legislations, which may entail specific cybersecurity and/or safety requirements tailored to domains.

At the core of these regulations lies the New Legislative Framework (NLF), adopted in 2008. Initially developed to ensure product safety, the NLF comprises a comprehensive set of measures aimed at enhancing market surveillance and elevating the quality of conformity assessments. It also brings clarity to the employment of CE marking and establishes a toolkit of measures for application in product legislation. By specifying rules for accrediting conformity assessment bodies and bolstering market surveillance, the NLF aligns with product legislation (verticals), encompassing 25 distinct regulations.

Some recent cybersecurity measures, extend this framework to include digital goods and software, hitherto outside the scope of CE marking requirements.

The main driver for NLF is to adjust to the reality of digitalisation as most of the existing NLF legislation addressed safety in the absence of security. Nowadays, digital products go beyond the traditional hardware end devices, and software, and subcomponents are recognised as products. The relevance of security is stressed to make it a requirement, and the impact of security on safety and other areas like liability is brought to the forefront. In the process, existing regulations need to be updated, and new ones are created.

In efforts to modernise the approach further, initiatives like the revision of the product liability directive and forthcoming regulations on AI product liability aim to empower consumers to seek compensation in instances of defective products.

To demonstrate compliance with the 'essential requirements' outlined in such legislations, the European Commission may request the European Standardisation Organisations (ESOs) to develop specific harmonised standards. Additionally, ongoing efforts are being directed towards establishing future connections with the European Cybersecurity Certification Framework introduced by the Cybersecurity Act. These certification schemes hold the potential to grant a 'presumption of conformity', further streamlining the compliance process.

For Eurosmart's members, comprehensive analysis, and updates on ongoing developments of NLF-related legislations including the standardisation developments, are readily accessible through the online EU issue tracker.

Cyber Resilience Act (CRA)

Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements

Legacy:
- ✓ *New regulation*
- *Will repeal Commission Delegated Regulation (EU) 2022/30 (RED Delegated Act)*

Requirements:
- ⚠ *Mandatory demonstration of compliance to cybersecurity requirements*
- ⚠ *Mandatory EU cybersecurity certification schemes for certain digital products*

The European Cyber Resilience Act (CRA) defines horizontal requirements for the development of secure products with digital elements by ensuring that hardware and software products are placed on the European Union market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle. The regulation concerns the placing on the market of commercial hardware and software products, including both end-devices and their respective subcomponents.

The CRA aims to mitigate significant cybersecurity risks posed by digital products, which have increasingly become targets for cyberattacks affecting organisations and supply chains across borders.

Key objectives of the CRA

The Act mandates manufacturers to prioritise security throughout a product's lifecycle, including cybersecurity risk assessment, vulnerability handling processes, and cooperation with authorities. It aims to improve product security, facilitate compliance, enhance transparency, and enable secure usage of digital products.

Scope and coverage

Covering end-devices, software, and components (both hardware and software), the CRA ensures comprehensive cybersecurity measures across various product types for placing products on the EU market by setting out obligations for **manufacturers, distributors and importers making their product available on the European market.**

The CRA defines several types of product categories whose conformity with the CRA's horizontal requirement shall be ensured by relying on different conformity assessment procedures according to their criticality: self-assessment, third-party assessment and obtention of a cybersecurity certificate.

The text identifies "**core functionalities**" for "**critical products**" which may require to undergo a stricter conformity assessment procedure or a possible mandatory EU cybersecurity certificate.

Delegated and implementing Acts

The European Cyber Resilience Act (CRA) introduces significant delegated acts:

- Implementing Act on Technical Description of Categories and Products (entry into force + 12 months: October 2025): Specifies technical standards for Category 1, Category 2, and products in Annex IIIa, ensuring cybersecurity resilience through detailed criteria and definitions.
- Delegated Act for Conditions Delaying Notification of Vulnerabilities and Incidents (entry into force + 12 months: October 2025): Establishes conditions for delaying vulnerability and incident notifications, ensuring timely disclosure while considering risk factors and mitigation measures.
- Provision on Certification Assessment Bodies Notification (entry into force + 18 months: April 2026): Defines notification procedures for Certification Assessment Bodies (CABs), enhancing transparency in certification processes by requiring CABs to inform relevant stakeholders about their activities.
- Application of Article 11 on Reporting Obligation of Manufacturers (entry into force + 21 months: July 2026): Clarifies manufacturers' reporting obligations regarding cybersecurity incidents and vulnerabilities, specifying reporting

requirements, timelines, and authorities to notify for improved incident response and information sharing.
- Report on Effectiveness of the Single Platform (entry into force + 24 months: October 2026): Mandates a report assessing the Single Platform's effectiveness in promoting cross-border certification recognition, consistency in cybersecurity standards, and cooperation among Member States to strengthen EU cybersecurity.
- By delegated act (no schedule) the Commission may: Identify EU cybersecurity certificates that provide presumption of conformity against the CRA requirements. to obtain an EU cybersecurity certificate at level “high” or “substantial”

Timeline and next steps

- September 15th, 2022: Commission presents proposal for regulation for a Cyber Resilience Act.
- Expected by the end of 2024: Council’s approval is expected after the 2024 EU elections, with the Regulation expected to enter into force by the end of 2024.

Artificial Intelligence Act (AI Act)

Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence act)

Legacy:	Requirements:
✓ *New regulation*	⚠ *Mandatory demonstration of compliance to cybersecurity requirements* ⚠ *Mandatory EU cybersecurity certification schemes for certain digital products*

The AI Act, presented by the European Commission in April 2021 and ratified in February 2024, represents a legislative effort landmark aimed at regulating the proliferation of artificial intelligence (AI) systems within the European Union. At its core, the Act seeks to strike a delicate balance between promoting innovation and safeguarding fundamental rights by introducing a comprehensive regulatory framework.

Key objectives of the AI Act

With a primary focus on fostering responsible AI innovation, the AI Act aims to achieve several key objectives, such as establishing harmonised rules to govern the deployment and use of AI systems, ensuring transparency and accountability in AI decision-making processes, and mitigating potential risks associated with AI technologies. Furthermore, the Act aims to uphold EU values and fundamental rights by prohibiting harmful AI practices and promoting ethical AI development.

Scope, coverage, and classification of AI systems

Under the AI Act's framework lies a wide array of AI systems, each classified based on their associated risk levels. This classification facilitates the implementation of tailored regulations, with stringent obligations imposed on high-risk systems and more lenient requirements for low-risk counterparts. By adopting this risk-based approach, the AI Act aims to address the diverse challenges posed by AI technologies while fostering responsible innovation across various sectors.

- Unacceptable risks, such as social scoring systems and manipulative AI, are explicitly prohibited.
- High-risk AI systems: The majority of the framework focuses on high-risk AI systems, which are tightly regulated. Notably, verification of travel documents is excluded from high-risk AI systems.
- Limited-risks AI systems: AI systems posing limited risks, imposing lighter transparency requirements. Developers and deployers are obligated to ensure that end-users are informed when they interact with AI, such as in the case of chatbots and deepfakes.
- Minimal AI systems: AI applications with minimal risks remain unregulated. This category encompasses most AI applications available on the EU single market, such as AI-enabled video games and spam filters (as of 2021). However, this landscape is evolving with the advent of generative AI technologies.

Exclusion of Military, Defence or National Security purposes

The AI Act does not apply to systems placed on the market or put into service in the EU, the results are used exclusively for military, defence, or national security purposes.

General Purpose AI (GPAI):

- All providers of GPAI models are obligated to provide technical documentation, usage instructions, comply with the Copyright Directive, and publish the content of the training data employed.
- Models under free and open licenses are only required to follow the Copyright directive and publish the training data summary unless they present a systemic risk.
- Providers of General Purpose AI (GPAI) models, irrespective of their licensing status, must undertake model evaluations, adversarial testing, monitor and report serious incidents, and implement cybersecurity measures.

Remote biometric identification (RBI):

The AI Act defines remote biometric identification system as "an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database". The use of AI-enabled real-time RBI is only possible solely under circumstances where refraining from its use would result in significant harm and must account for affected persons' rights and freedoms.

Before deployment, police must complete a fundamental rights impact assessment and register the system in the EU database. In addition, an authorisation from a judicial authority or independent administrative authority is necessary.

Delegated Acts

To ensure the effective implementation and enforcement of the AI Act, provisions are made for delegated acts, granting the European Commission the authority to adopt specific measures for implementation. These delegated acts empower the Commission to address intricate aspects of regulation, such as certification processes for high-risk AI systems. This centralised approach aims to streamline regulatory procedures and ensure uniformity in enforcement practices across the EU Member States.

Certification Obligations

Central to the regulatory framework outlined in the AI Act are certification obligations imposed on high-risk AI systems. Through mandatory certification requirements, the AI Act aims to establish clear standards for assessing and mitigating the risks associated with AI technologies. In contrast, providers of low-risk AI systems are afforded the flexibility to voluntarily adhere to additional standards and codes of conduct, further enhancing accountability and transparency within the AI ecosystem.

Timeline and next steps

- April 21st, 2021: Commission presents proposal for an AI Act.
- March 13th, 2024: The European Parliament adopted the text as its first reading position on the proposed AI Act.
- Expected by mid of 2024: The AI Act to enter into force.

RED Delegated Act

Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f)

Legacy:	**Requirements:**
Supplementing Directive 2014/53/EU (Radio Equipment Directive)	*Mandatory demonstration of compliance to cybersecurity requirements*

The Radio Equipment Directive 2014/53/UE (RED), as one of the sectorial regulations of the New Legislative Framework, provides a regulatory framework for placing radio-equipped products on the EU market. It aims to foster the conditions for the placing on the market by defining essential criteria concerning safety, health, electromagnetic compatibility, and the optimal utilisation of radio spectrum resources.

Key objectives of RED Delegated Act

On 29 October 2021, the Commission adopted a Delegated Act (EU) 2022/30 activating already existing provisions of the RED for certain categories of radio equipment in terms of cybersecurity, personal data protection and privacy.

Standardisation request

On 23 August 2023, the Commission issued the standardisation request M/585 to the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) for drafting new harmonised standards in support of the article of the RED Directive providing cybersecurity, personal data protection and privacy essential requirements. These harmonised standards will serve as foundational pillars to ensure radio-equipped products compliance with the directive.

Timeline and next steps

- July 20th, 2023: Commission presents proposal for a RED Delegated Regulation (EU) 2022/30.
- October 29th, 2021: Commission adopted Delegated Act (EU) 2022/30 activating RED cybersecurity related essential requirements.
- August 23rd, 2023: Commission issued the Standardisation request M/585 to CEN and CENELEC.
- Expected by the third quarter of 2024: Application of the new essential requirements.

Product Liability Directive (revision)

Proposal for a Directive on liability for defective products COM/2022/495 final

Legacy:	Requirements:
Repealing Directive 85/375/EEC (Product liability directive)	*Mandatory compliance to safety-relevant cybersecurity requirements*

Since 1985, the Product Liability Directive (PLD) stands as a cornerstone of consumer protection within the European Union, providing a robust legal framework for addressing damages caused by defective products. The revision of the Product Liability Directive aims to ensure that the new regime for product liability rules is adapted to new types of products, to the benefit of both businesses and consumers. A major shift in this revision is the inclusion of software (SW) as a product, recognising the increasing prevalence of software-driven products in the market and the potential risks associated with them. Additionally, the proposal seeks to expand the scope of the directive to include the effects of security on safety systems, acknowledging the interconnectedness of digital systems and their impact on product safety. In fact, the proposal seeks to facilitate business assessments of the risks of marketing innovative products, while contemporarily allowing victims of product-caused damages to claim compensation for an increasing number of products.

Key objectives of the Revision of Product Liability Directive

The PLD aims to establish legal frameworks governing compensation for damages caused by defective products within the European Union. Its primary objectives include enhancing consumer access to compensation, ensuring liability for defective products, and adapting to advancements in technology.

Scope and Coverage

The PLD encompasses damages resulting from defective products, with proposed revisions extending coverage to include non-material losses such as psychological harm. Notably, the directive excludes open-source software from its application.

The revised text recognised the growing relevance and value of intangible assets such as the destruction or corruption of data, such as digital files deleted from a hard drive which could also be compensated.

In light of challenges faced by injured persons, especially in complex cases involving digital products, the text further aims to achieve a fair balance between industry and consumer interests by placing consumers on an equal footing with economic operators. Both would be required to disclose evidence with the burden of proof for victims alleviated in complex cases.

Timeline

- September 28th, 2022: Commission presents proposal for a Product Liability Directive.
- Dates TBD: 20 days post-publication in the Official Journal of the EU, PLD enters into force upon final adoption.

General Product Safety Regulation

Regulation (EU) 2023/988 on general product safety

Legacy:	Requirements:
Repealing Directive 2001/95/EC (General Product Safety)	*Mandatory compliance product's safety requirements*

The General Product Safety Regulation (GPSR) aims to enhance consumer protection within the EU by ensuring the safety of non-food consumer products. Replacing the former General Product Safety Directive (2001/95/EC).

Key objectives of the Product Safety Regulation

Key objectives include the guarantee of the safety of consumer products and the protection of consumers from risks, including those associated with new technologies and online sales channels. Enhancing the market surveillance and alignment of rules for harmonised and non-harmonised consumer products. And the effectiveness and speed with which product recalls are conducted when unsafe or hazardous products are identified in the market.

Scope and Coverage

The Regulation applies to all non-food consumer products sold on the EU single market and it extends safety requirements to cover new technologies and online sales platforms.

The GPSR explicitly states that products fall under its safety regulations when they are made accessible on the EU market, particularly through distance sales channels aimed at EU consumers. The text contains specific information requirements for offers in distance sales, which adds another compliance checkpoint before the product is supplied.

The GPSR extends its coverage to explicitly include products using emerging technologies. The term 'product' within the GPSR is now defined as "any item, whether standalone or interconnected with others (...)." Additionally, there are new criteria to evaluate a product's safety, including cybersecurity measures aimed at safeguarding it from external threats, as well as its adaptive, learning, and predictive capabilities.

The responsibilities of economic operators involved in the supply chain are updated to align with the standard obligations outlined in the 2008 New Legislative Framework. All economic operators are mandated to guarantee that only products meeting safety standards and conformity requirements are accessible within the EU. To fulfil this obligation, they should implement internal procedures, tailored to their role in the chain.

Delegated Acts

Delegated acts may be adopted to establish a more stringent system of traceability for products posing serious risks to health and safety.

Timeline and next steps

- June 30th, 2021: Commission presents proposal for a General Product Safety Regulation.
- June 12th, 2023: Regulation (EU) 2023/988 entered into force.

Accreditation and Market Surveillance

Regulation (EC) No 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products

Legacy:	Requirements:
Repealing Council Regulation (EEC) No 339/93	*No product requirement*

The Accreditation and Market Surveillance Regulation, established by Regulation (EC) No 765/2008, serves as a cornerstone in ensuring the conformity and safety of non-food products within the European Union. This regulation outlines common rules for accrediting bodies and establishes fundamental principles for CE marking—a vital indicator of adherence to EU legal standards.

Key objectives of Accreditation and Market Surveillance

The Accreditation and Market Surveillance Regulation aims to safeguard the public interest by creating a single European accreditation system covering both regulated and voluntary sectors. It sets out common rules for accrediting bodies to ensure non-food products in the EU conform to specific requirements.

Scope and Coverage

The regulation establishes a single European accreditation system covering both regulated and voluntary sectors. Each EU member state must appoint a single national accreditation body, ensuring it operates as a public authority activity and is not-for-profit. National accreditation bodies determine the competence of conformity assessment organisations, monitor their performance, and manage accreditation on a national level.

Accreditation of conformity assessment organisations

National accreditation bodies must ensure the competency of conformity assessment organisations and oversee the process of accreditation. CE marking can only be affixed to products that meet conformity standards.

Timeline and next steps

- February 14th, 2007: Commission presents proposal for an Accreditation and Market Surveillance Regulation.
- July 29th, 2008: Regulation (EC) No 765/2008 entered into force.

Data

In May 2018, the EU rolled out the General Data Protection Regulation (GDPR), supplanting the 1995 Data Protection Directive and modernising the approach to address the challenges of online usage. As a key component of the EU's soft power strategy, the GDPR is renowned for its stringent privacy and security provisions, positioning it as one of the world's most robust regulations in this domain, its interpretation leads to famous court cases. It establishes a unified framework for safeguarding personal data, encompassing requirements for its collection, storage, and management.

In February 2020, the European Commission unveiled the European Data Strategy, which extends beyond privacy assurances to emphasise the secure management of the data economy as a public infrastructure. The European Data Act sets out standardised rules to foster data sharing among service providers and data-handling firms, mandating the creation of industry-specific European data spaces.

Despite the enactment of the GDPR in 2018, additional policy measures are still in progress. The implementation of the European Data Act is slated for mid-2024. Progress regarding data spaces has been varied, with the most defined frameworks emerging in the financial sector. Moreover, the ePrivacy Regulation proposed by the Commission in 2017 has not been adopted. This text is intended to replace the ePrivacy Directive (Directive 2002/58/EC) and complement the General Data Protection Regulation (GDPR) by specifically addressing privacy concerns related to electronic communications.

For Eurosmart's members, comprehensive analysis, and updates on ongoing developments of Data-related legislations are readily accessible through the online EU issue tracker.

General Data Protection Regulation

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Legacy:	Requirements:
Repealing Directive 95/46/EC on personal data	*Personal data and data processing mandatory requirements* *Certification requirements*

The General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 seeks to protect individuals' rights regarding personal data processing within the EU, ensuring an unified approach to data protection, while addressing concerns regarding fragmented data protection practices, legal uncertainties, and risks associated with online activities. Additionally, the proposed regulation COM (2023) 348 aims to enhance GDPR enforcement by laying down additional procedural rules.

Key objectives of the GDPR

Key objectives in Regulation (EU) 2016/679 were the safeguarding of individuals' fundamental right to data protection and facilitating the free movement of personal data across EU Member States. The proposed regulation COM (2023) 348 has as its primary objectives enhancing efficiency and harmonisation in handling cross-border cases, addressing procedural disparities among Data Protection Authorities (DPAs).

Scope and Coverage

The Regulation (EU) 2016/679 introduced principles for lawful data processing, reinforced transparency, and specified rights such as access, rectification, erasure, and data portability for individuals. The proposed regulation COM (2023) 348 targets areas such as complaints, procedural rights, cooperation, and dispute resolution, seeking to standardise practices across Member States. It applies to complaints related to cross-border processing and focuses on harmonising administrative procedures among data protection authorities (DPAs) to improve cross-border case handling.

European Data Protection Board (EDPB)

EDPB is an EU body ensuring that the GDPR is applied consistently across the EU and work to ensure effective cooperation amongst DPAs. It's made up of the head of each DPA and of the European Data Protection Supervisor (EDPS).

EDPB's board issues guidelines on the interpretation of core concepts of the GDPR but also be called to rule by binding decisions on disputes regarding cross-border processing.

Delegated Acts

Provisions empowering the Commission to adopt delegated acts are outlined, enabling further regulatory adjustments as necessary, notably on specifications on data processing principles or technical standards for compliance.

Code of conducts and certifications mechanisms

The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller.

GDPR certification remains voluntary, it includes thorough assessment processes, issuance of compliance certificates, and periodic reviews to maintain certification.

Timeline and next steps

- January 25th, 2012: Commission presents proposal for a regulation updating the EU rules on the processing and exchange of personal data (Regulation (EU) 2016/679).
- May 24th, 2016: Regulation (EU) 2016/679 entered into force.
- July 4th, 2023: COM (2023) 348 Legislative proposal published laying down additional procedural rules relating to the GDPR enforcement.

Schrems I and Schrems II

Schrems I and II refer to two significant legal cases involving data privacy and the General Data Protection Regulation (GDPR) in the European Union:

Schrems I (2015):

- Background: Austrian privacy activist Max Schrems filed a complaint against Facebook in 2013, arguing that the company's data transfers from the EU to the United States didn't adequately protect EU citizens' data due to US surveillance practices.
- Outcome: The Court of Justice of the European Union (CJEU) invalidated the Safe Harbor Agreement, which previously allowed data transfers between the EU and the US. The court ruled that US surveillance programs didn't provide adequate protection for EU citizens' data.
- Impact: This decision had significant implications for transatlantic data transfers, leading to the renegotiation of data transfer agreements between the EU and the US.

Schrems II (2020):

- Background: Max Schrems challenged Facebook's data transfers to the US again, this time under the EU-US Privacy Shield framework, which had replaced Safe Harbor. He argued that US surveillance practices still didn't offer adequate protection for EU citizens' data.
- Outcome: The CJEU invalidated the EU-US Privacy Shield, stating that it didn't provide sufficient protection against US government surveillance for EU citizens' data. Additionally, the court clarified that the use of Standard Contractual Clauses (SCCs) for data transfers remains valid but requires assessment on a case-by-case basis to ensure the protection of personal data.
- Impact: The decision created uncertainty for businesses relying on the Privacy Shield for data transfers between the EU and the US. It emphasised the importance of thoroughly assessing data transfer mechanisms and ensuring compliance with GDPR requirements, particularly concerning data transfers to countries with surveillance programs that may compromise the protection of personal data.

The European Data Act

Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)

Legacy:	Requirements:
✓ *New regulation*	⚠ *Requirements on data* ⚠ *Conformance requirements defined by complementary regulation*

The European Data Act signifies a pivotal step towards fostering a dynamic and harmonised data ecosystem across the European Union. Aimed at enhancing data accessibility and utilisation while ensuring regulatory coherence, this legislation addresses a wide array of objectives spanning from data access facilitation and air data sharing to interoperability standardisation. With its broad applicability to manufacturers, service providers, users, and public sector entities within the EU, the European Data Act represents a comprehensive framework for navigating the complexities of modern data management.

The European Data Act lays out principles and guidelines that apply to all sectors. It does not modify existing data access obligations. However, any forthcoming legislation should align with its principles.

Key objectives of the European Data Act

Thanks to this regulation, connected products will have to be designed and manufactured in a way that empowers users (businesses or consumers) to easily and securely access, use and share the generated data.

The European Data Act objectives include facilitating data access, ensuring fair data sharing, and developing interoperability standards.

Scope and Coverage

The Act applies to manufacturers, service providers, users, data holders, public sector bodies, and data processing service providers within the EU. It encompasses various aspects of data management, including product data, related service data, and safeguards against unlawful data access.

Delegated Acts

Delegated acts play a crucial role in implementing certain aspects of the European Data Act, such as facilitating switching between data processing services and ensuring compliance with regulatory requirements regarding data sharing contracts and standards.

Compliance

The Act introduces essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces. Participants in data spaces that offer data or data services to other participants shall comply with these requirements, harmonised standards will support their correct implementation.

Timeline

- February 23rd, 2022: Commission presents proposal for a European Data Act.
- January 11th, 2024: European Data Act entered into force.

Platforms & Competition

In the digital age, consumers' attention is a vital and scarce resource, and all online Content and Service Providers (CSPs) are competing for it in various ways. The European market, representing approximately 451 million internet users in 2021, is a prime target for CSPs, many of which operate from outside the EU. These platforms aim to aggregate the consumers' attention by organising products, services, content, and other offers, facilitating the search process, and enabling better matches or allocations. Examples include search engines, booking platforms, social media platforms, ridesharing, and accommodation-sharing platforms, as well as shopping platforms.

Historically, European competition policy has been heavily influenced by Ordoliberal theory, which shaped German competition law. However, the limited efficacy of European competition law in addressing emerging power concentrations in digital markets has forced the legislator to develop a new regulatory approach. The European Commission has initiated a specific approach inspired by asymmetric regulation, as seen in telecommunications, rather than relying on pure competition law. This approach entails maximising the economic position of new entrants, by minimising the position of historical operators, thereby signalling the end of the grandfather clause (customer, patent, know-how).

At the core of this new approach is the Digital Markets Act, which aims to design open and fair digital markets. This paradigm shift in competition law entails a more proactive role for European antitrust authorities in monitoring and detecting the abuse of market power. This approach is complemented by data-related measures aimed at preventing vendor lock-in, such as the Data Act or the Data Governance Act.

Furthermore, other sector-specific initiatives contribute to this evolving European political approach, including the revised Payment Services Directive (PSD2) adopted in 2015. PSD2 plays a crucial role in regulating the payment services market within the EU, ensuring a level playing field for payment service providers, protecting consumers' rights, and fostering innovation and competition in the sector.

Digital Markets Act (DMA)

Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)

Legacy:	Requirements:
✓ *New regulation*	⚠ *Obligations for gatekeeper platforms*

The DMA is a pivotal part of the Digital Services Act package, designed to address the challenges posed by large online platforms, often referred to as "gatekeepers," such as Google, Amazon, and Meta.

Key objectives of DMA

The DMA aims to regulate "gatekeeper platforms" to ensure fair competition and protect user rights in the digital market. Effective from 2 May 2023, it addresses concerns regarding market dominance and data privacy. The DMA sets clear rules to ensure a level playing field and prevent the abuse of market dominance, while also creating a transparent and competitive digital environment within the European Union.

Scope and Coverage

Gatekeepers are designated based on criteria including significant market impact and importance of core platform services. The DMA covers various services such as online intermediation, social networking, and advertising.

The Digital Markets Act (DMA) sets out rules for gatekeeper platforms, outlining both actions they must take ("do's") and actions they are prohibited from taking ("don'ts"). Following are some key points:

Do's:

- Allow third-party interoperability in certain cases.
- Grant business users access to the data they generate on the platform.
- Provide advertisers with tools for independent verification of their ads.
- Permit business users to promote offers and make contracts outside the platform.

Don'ts:

- Show preferential treatment to the gatekeeper's own services over similar third-party services in rankings.
- Restrict consumers from linking to businesses outside the platform.
- Prevent users from uninstalling pre-installed software or apps.
- Track end users for targeted advertising without explicit consent.

Delegated Acts

The DMA empowers the European Commission to enact delegated acts, allowing refinement of identification methodologies for gatekeepers. Key obligations include establishing compliance functions and ensuring user consent for data processing.

On 6 September 2023, the European Commission designated 6 gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, and 22 related core platform services.

Standardisation

The implementation of some of the gatekeepers' obligations, such as those related to data access, data portability or interoperability could be facilitated by the use of technical standards. In this respect, the Commission may request European standardisation bodies to develop them

Timeline and next steps

- December 2020: Commission presents proposal for a Digital Markets Act.
- November 1st, 2022: Digital Markets Act entered into force.

E-commerce & Consumer

In complement to the EU platform policy, the EU legislator is actively working to dismantle online barriers, ensuring individuals can fully access all goods and services offered online by businesses in the EU. As the digital landscape continues to evolve, regulatory efforts are being intensified to address emerging challenges while safeguarding consumer interests and promoting fair competition.

The Digital Services Act, which came into force in 2022, represents one of the most significant efforts to update the legal framework for digital services in the EU. It includes provisions related to online platforms' responsibilities in moderating content, combating illegal goods or services, and ensuring transparency and accountability.

Furthermore, to facilitate access for online consumers, the EU has implemented new regulations aimed at eliminating unjustified geo-blocking practices. The 2018 Regulation on geo-blocking ensures that buyers of goods or services from another EU country are treated like local customers. The 2017 legislation on the portability of online content enables EU citizens to seamlessly utilise their online subscriptions for various media content while traveling within the EU, promoting cultural exchange and entertainment accessibility across borders.

The 2018 New Deal for Consumers reinforces online consumer rights, empowering authorities to swiftly address fraudulent websites or social media accounts. By enabling the removal of such platforms and facilitating the tracing of rogue online traders' identities through collaboration with internet service providers or banks, consumer protection measures are significantly strengthened.

In alignment with the New Deal for Consumers, the European Commission's amendment to the Consumer Rights Directive, initiated in 2019 and enacted in 2022, aligns and harmonises national consumer rules. For example, it enhances pre-purchase information disclosure requirements and clarifies consumers' rights to cancel online purchases, regardless of where they shop within the EU.

Digital Services Act (DSA)

Regulation (EU) 2022/2065 on a Single Market For Digital Services (Digital Services Act)

Legacy:	Requirements:
✓ *New regulation*	⚠ *Obligations for online platforms*
Amending Directive 2000/31/EC (eCommerce)	

The Digital Services Act (DSA) is a critical part of the Digital Services Act package proposed by the European Commission. This legislative package aims to comprehensively update the regulatory framework governing digital services within the European Union. Introduced in December 2020, the DSA is designed to address the evolving digital landscape and emerging societal challenges. It works in tandem with the Digital Markets Act (DMA), forming a comprehensive strategy to ensure a safer, more transparent, and accountable online environment for users across the EU.

Key objectives of the DSA

The DSA's primary objectives include creating a safer and more trusted online environment, combating the dissemination of illegal content and activities, and enhancing transparency and accountability in digital platforms.

Scope and Coverage

The DSA encompasses various types of digital services, including intermediary services, hosting services, online platform services, very large online platforms, and search engines (VLOPs and VLOSEs). The DSA enforces stricter rules on online platforms to enhance transparency and accountability.

Key provisions of the DSA include:

- Special obligations for online marketplaces to combat the sale of illegal products and services.
- Measures to counter illegal content online, with requirements for platforms to respond promptly while upholding fundamental rights.
- Protection of minors by prohibiting targeted advertising based on their personal data.
- Limits on advertising presentation and the use of sensitive personal data for targeted advertising.
- Prohibition of misleading interfaces and deceptive practices.

For VLOPs and VLOSEs, additional requirements include:

- Providing users with a recommendation system not based on profiling.
- Analysing systemic risks they create, such as the dissemination of illegal content and negative impacts on fundamental rights, electoral processes, gender-based violence, or mental health.

Delegated Acts

Important delegated acts under the DSA include the establishment of the European Centre for Algorithmic Transparency (ECAT) to assist in enforcement efforts and the launch of the DSA Transparency Database to enhance transparency in content moderation decisions.

Timeline and next steps

- December 2020: Commission presents proposal for a Digital Services Act.
- November 16th, 2022: Digital Services Act entered into force.

Digital identity

The European Commission proposed a new regulation on digital identity in 2021, updating existing regulation from 2014 (eIDAS 1 - Electronic Identification, Authentication and Trust Services). This proposal aims to facilitate cross-border electronic interactions within the EU and emphasises the importance of reliable digital identities for accessing increasingly digital services. At the core of the proposal lies the creation of an EU digital identity wallet, the European digital identity can be used for a wide range of purposes, from public services like obtaining birth certificates to private transactions like opening bank accounts or renting cars. The COVID-19 pandemic accelerated the need for secure remote identification, highlighting the importance of remote identity verification services and specific attributes linked to digital identities. Overall, the proposal aligns with the EU's digital transformation objectives, aiming to deploy a user-controlled trusted identity on a large scale by 2030.

The ongoing revision of the driving license directive proposes the introduction of digital driving licenses that could be supported by the EU's digital identity wallets.

Beyond the new European digital identity framework, the eID approach will directly impact the European Travel Information and Authorisation System (ETIAS). EU countries' general immigration policies are likely to undergo significant changes with the integration of the eID system, simplifying identification and verification procedures. This development could lead to more efficient handling of visa applications and border controls, enhancing security while making travel more convenient.

Moreover, adopted in 2023, the digitalisation of Schengen visa rules will modernise, simplify, and harmonise the visa procedures through digitalisation. This will benefit both the third-country nationals applying for a Schengen visa and the EU Member States processing these requests by streamlining visa applications and reducing costs for applicants and issuing authorities. These new rules will also mitigate risks associated with physical visa stickers.

For Eurosmart's members, comprehensive analysis, and updates on ongoing developments of Digital identity related topics are readily accessible through the online EU issue tracker.

The European Digital Identity Regulation (eIDAS2)

Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity - COM/2021/281 final

Legacy:
- *Amending Regulation (EU) no 910/2014 (eIDAS 1)*
  - *Repealing Directive 1999/93/EC (eSignature Directive)*

Requirements:
- *Mandatory cybersecurity requirements*
- *Mandatory EU DI wallet cybersecurity certification*

The European e-ID, or European Digital Identity Regulation (eIDAS2), aims to establish a robust framework for digital identity within the EU, addressing the increasing need for secure and trusted electronic identification. The text builds on the 2014 eIDAS Regulation which had some limits since it was based on national eID systems that follow varying standards and focuses on a relatively small segment of the electronic identification. Moreover, the regulation did not require EU Member States to develop a national digital ID and to make it interoperable.

Key objectives of eIDAS

The new eID framework aims the alignment with the objectives of the digital compass, ensuring that by 2030, key public services are available online. Key objectives include:

- Ensuring universal access to secure electronic identification;
- Facilitating seamless access to both public and private services across the EU;
- Empowering users with control over their identity data;
- Ensuring equal conditions for the provision of qualified trust services in the EU and their acceptance.

It will require robust security measures for all aspects of the digital identity provision, including issuing a European digital identity wallet and establishing infrastructure for data collection, storage, and disclosure.

Scope and Coverage

The regulation mandates the issuance of European Digital Identity Wallets by Member States, enabling secure sharing of identity data and attributes for various purposes such as accessing public services (healthcare, education, or social benefits), and private services (banking, e-commerce, or online reservations). It also requires acceptance by public services, designated online platforms, and private services requiring user authentication. Additionally, Member States are required to notify a compatible eID scheme allowing citizens to integrate existing IDs into the wallet and access free eSignatures for personal use.

The regulation aims to move away from solely using national digital identity solutions. Instead, it focuses on offering electronic attestations of attributes recognised throughout Europe. Providers of electronic attestations of attributes will have clear and consistent rules to follow, and public administrations should be able to rely on electronic documents in a standardised format.

The European digital identity wallet shall include the official identity data as issued by Member States and other identity attributes as the electronic attestations of attributes. Member States are required to rely on national cybersecurity certification schemes and in the future, European ones, to ensure the EU ID wallet compliance with the requirement of the regulation.

Additionally, the regulation provides that the user should be in full control of the wallet. Strict requirements for data protection and privacy are established for the issuers of the European digital identity wallet and for qualified providers of attestations of attributes, including compliance with GDPR requirements.

Furthermore, to enhance website transparency, the proposal mandates web browser providers to make it easier for users to identify website owners by

displaying qualified certificates for website authentication (QWACs) in a user-friendly format.

Recommendations, technical specifications, and common standards

To meet the 12-month deadline for a European digital identity wallet to be issued in each Member State, the Commission adopted a Toolbox so as to avoid fragmentation and barriers due to diverging standards. This toolbox aims to accelerate the work by defining a common technical architecture, a reference framework, and common standards to be developed with Member States, as well as best practices and guidelines.

Delegated Acts

Delegated acts include technical specifications for the EU Digital Identity Wallet and certification requirements, which Member States must implement within 24 months of adoption to ensure compliance with the regulation.

Timeline and next steps

- June 3rd, 2021: Commission presents proposal for a European Digital Identity Regulation.
- June 3rd, 2021: Commission Recommendation (EU) 2021/946 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.
- February 10th, 2023: First version of a common EU Toolbox to implement the EU Digital Identity Wallet was published by the Commission.
- February 22nd, 2023: eIDAS expert group adopted an outline of an Architecture and Reference Framework (ARF) for a future EU Digital Identity Wallet.
- March 6th, 2023: Version 1.3 of ARF released on GitHub.
- February 29th, 2024: The European Parliament adopted the text as its first reading position on the proposed eIDAS2 Regulation.
- May 20th, 2024: The regulation will enter into force.
- Expected by the end of 2024 or beginning of 2025: The Commission shall establish a list of reference standards, specifications, and procedures for the implementation of the European Digital Identity (EUDI) Wallet.
- Expected by mid-2026: Member States must provide EU-DI Wallets.

Digital Industrial Policy

Industrial policy can be defined as a deliberate attempt by governments to steer industrial development towards specific paths. Industrial policy encompasses managing industrial ecosystems to bolster both national and EU competitiveness and employment opportunities. It also focuses on individual firms to ensure that their interests align with broader public interests. A new aspect involves proactively addressing geopolitics as a significant factor influencing industrial policy decisions. In this context, the European Union endeavours to tackle the concept of "digital strategic autonomy."

The European Commission has appropriately set “industrial revival” as a target at the beginning of the 2014 term. But the nature of “industry” as policy target has changed drastically. Within its different strategies the Commission tries to address the evolving nature of this industry, it intensifies the efforts to promote the digital sector, notably including the 2010 Digital Agenda for Europe, the 2015 Digital Single Market, the 2016 Gigabit Society, and the 2021 Digital decade.

The pandemic crisis and the war in Ukraine have revealed the already known issues surrounding digital strategic autonomy. As part of this approach, the Commission and Member States' policies have focused on two major areas: cloud computing and semiconductors.

The EU Chips Act entails a comprehensive investment program with three main objectives. The first pillar fosters technological innovation for cutting-edge chips. The second pillar focuses on expanding production capacities, while the third aims to enhance readiness to address semiconductor supply crises.

The EU's cloud policy is still evolving. The EU Alliance for Industrial Data, Edge, and Cloud has been launched, and the EU's cybersecurity agency ENISA is developing cloud security certification schemes. Extensive financial support for cloud R&D is provided through the Horizon Europe program, and support to cloud deployment comes from the Digital Europe. The large-scale GAIA-X initiative, initiated and supported by Germany and France and involving several other EU countries, though executed by the private sector, develops and tests specifications for trusted and interoperable clouds and runs a wide range of sectoral pilots.

Important Projects of Common European Interest (IPCEIs) are additional tools to support the Digital Industrial Strategy. Funded by state aid, projects concern Microelectronics and Communication Technologies, as well as Next Generation Cloud Infrastructure and Services.

European Chips Act

Regulation (EU) 2023/1781 establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)

Legacy:	Requirements:
✓ *New regulation*	⚠ *Voluntary framework*

The European Chips Act, embodied in Regulation (EU) 2023/1781, is a pivotal initiative aimed at fortifying the EU's semiconductor industry and amplifying its global competitive standing. With a strategic focus on resilience and innovation, the European Chips Acts responds to disruptions in chip supply chains, propelling efforts to increase Europe's semiconductor production capabilities and mitigate dependency on limited suppliers.

Key objectives of the European Chips Act

The European Chips Act aims at enhancing Resilience by addressing disruptions in chip supply chains through increasing Europe's semiconductor production capacity and reducing dependency on limited suppliers. Another objective is to promote innovation by supporting research, technological advancement, and innovation in semiconductor design, manufacturing, and packaging to boost Europe's competitiveness. Finally, another objective is to ensure security of supply, which involves establishing criteria for integrated production facilities and open EU foundries to enhance semiconductor production capacities within the EU, thereby ensuring security of supply.

Scope and Coverage

The proposed framework for reinforcing the EU chip sector is based on three pillars:

- The Chips for Europe Initiative supports technological capacity building, innovation, and funding avenues for start-ups. The Initiative will be supported by €3.3 billion of EU funds.
- The Security of Supply Framework guarantees the security of semiconductor supply by incentivising investments and bolstering production capabilities in semiconductor manufacturing. This involves creating a framework for Integrated Production Facilities and Open EU Foundries that are "first-of-a-kind" in the Union and contribute to the security of supply and to a resilient ecosystem in the Union interest.
- The Coordination Mechanism facilitates collaboration between Member States and the Commission to monitor semiconductor supply, anticipate shortages, and implement crisis responses.

On November 30, 2023, the European Commission created the Chips Joint Undertaking (Chips JU) to carry out the Chips for Europe Initiative. This initiative has a projected total budget of €15.8 billion until 2030. The Chips JU's goal is to enhance Europe's semiconductor industry and economic stability. It will manage around €11 billion by 2030, funded by the EU and participating States.

Timeline

- February 24th, 2022: Commission presents proposal for a European Chips Act.
- September 28th, 2023: European Chips Act entered into force.

Timelines

EU Policies	2008		2009		2010		2011		2012		2013	
	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester
EU Events	*SI Presidency*	*FR Presidency*	*CZ Presidency* *EP elections*	*SE Presidency* *New Commission*	*ES Presidency*	*BE Presidency*	*HU Presidency*	*PL Presidency*	*DK Presidency*	*CY Presidency*	*IE Presidency*	*LT Presidency*
Cyber Resilience Act												
Cybersecurity Act												
DORA												
NIS 1											Legislative proposal NIS 1	
Cyber Solidarity Act												
AI Act												
RED Delegated Act												
Liability for digital products												
General Product Safety												
Accreditation and Market Surveillance	Entry into force				Fully applicable							
European Data Act											Legislative proposal	
General Data Protection											Legislative proposal	
Digital Markets Act												
Digital Services Act												
eIDAS 1											Legislative proposal eIDAS 1	
European Chips Act												

Legislative or non-legislative proposal

Entry into force (certain/estimate)

Specific obligations enter into force (certain/estimate)

Fully applicable date (certain/estimate)

Adoption date (published/estimate)

Evaluation/revision/additional procedural rules (certain/estimate)

Relevant court cases

EU Policies	2014		2015		2016		2017		2018		2019	
	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester
EU Events	*EL Presidency* *EP elections*	*IT Presidency* *New Commission*	*LV Presidency* *Digital Single Market Strategy*	*LU Presidency*	*NL Presidency*	*SK Presidency*	*MT Presidency*	*EE Presidency*	*BG Presidency*	*AT Presidency*	*RO Presidency* *EP elections*	*FI Presidency* *New Commission*
Cyber Resilience Act												
Cybersecurity Act							Legislative proposal				Adoption	Entry into force
DORA												
NIS 1					Adoption of NIS 1	Entry into force of NIS1						
Cyber Solidarity Act												
AI Act												
RED Delegated Act												
Liability for digital products												
General Product Safety												
Accreditation and Market Surveillance												
European Data Act												
General Data Protection			Safe Harbor agreement invalid		Adoption Entry into force							
Digital Markets Act												
Digital Services Act												
eIDAS 1	Adoption Entry into force				Full applicability							
European Chips Act												

Legislative or non-legislative proposal

Entry into force (certain/estimate)

Specific obligations enter into force (certain/estimate)

Fully applicable date (certain/estimate)

Adoption date (published/estimate)

Evaluation/revision/additional procedural rules (certain/estimate)

Relevant court cases

EU Policies	2020		2021		2022		2023		2024		2025	
	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester
EU Events	*HR Presidency*	*DE Presidency*	*PT Presidency*	*SI Presidency*	*FR Presidency*	*CZ Presidency*	*SE Presidency*	*ES Presidency*	*BE Presidency*	*HU Presidency*	*PL Presidency*	*DK Presidency*
			Digital Decade Strategy						*EP elections*	*New Commission*		
Cyber Resilience Act						Legislative proposal				Est. entry into force Est. Adoption		Technical description of important products
Cybersecurity Act							Proposal for "managed security services" certify.	EC's Evaluation report	EUCC CC implementing regulation			
DORA		Legislative proposal				Adoption	Entry into force				Full applicability	
NIS 1 & 2		Legislative proposal NIS 2				Adoption of NIS 2	Entry into force of NIS 2			National transposal deadline Est. delegated acts	Lists of essential and important entities	
Cyber Solidarity Act							Legislative proposal		Est. adoption Est. entry into force			
AI Act			Legislative proposal						Est. adoption Est. entry into force	Estimate enforcement of specific obligations	Estimate enforcement of specific obligations	
RED Delegated Act								Delegated Regulation Standard. request		Full applicability		
Liability for digital products						EC's proposal to recast the 1985 directive			Estimated adoption	Estimate entry into force		
General Product Safety			Legislative proposal to recast the directive				Entry into force			Full applicability		
Accreditation and Market Surveillance								EC's evaluation / revision				
European Data Act					Legislative proposal			Adoption	Entry into force			Applicability
General Data Protection		Privacy Shield invalid						Additional procedural rules	EC 's evaluation report			
Digital Markets Act		Legislative proposal				Adoption Entry into force	Enforcement of specific obligations		Enforcement of specific obligations		EC's annual implementation report	
Digital Services Act		Legislative proposal				Adoption Entry into force		Enforcement of specific obligations	Full applicability			
eIDAS 1 & European Digital Identity			Legislative proposal EU ID framework						Adoption Entry into force	List of reference standards cross-border ID matching	List of ref. standards for id and attrib. verif.	
European Chips Act					Legislative proposal			Adoption Entry into force				

Legislative or non-legislative proposal

Entry into force (certain/estimate)

Specific obligations enter into force (certain/estimate)

Fully applicable date (certain/estimate)

Adoption date (published/estimate)

Evaluation/revision/additional procedural rules (certain/estimate)

Relevant court cases

EU Policies	2026		2027		2028		2029		2030		2031	
	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester	1st Semester	2nd Semester
EU Events	*CY Presidency*	*IE Presidency*	*LT Presidency*	*EL Presidency*	*IT Presidency*	*LV Presidency*	*LU Presidency* *EP elections*	*NL Presidency* *New Commission*	*SK Presidency*	*MT Presidency*	*EE Presidency*	*BG Presidency*
Cyber Resilience Act		**Reporting obligation** **Evaluation report**		**Estimated full application**		**Evaluation report**				**Evaluation report**		
Cybersecurity Act												
DORA												
NIS2 Directive				**Directive's review**								
Cyber Solidarity Act												
AI Act			**Estimate enforcement of specific obligations**									
RED Delegated Act					**Repealed**							
Product liability		**National transposition deadline**										
General Product Safety												
Accreditation and Market Surveillance												
European Data Act					**Enforcement of specific obligations**	**Evaluation of the Act's implementation**						
General Data Protection												
Digital Markets Act	**EC's annual implementation report**		**EC's annual implementation report**		**EC's annual implementation report**		**EC's annual implementation report**		**EC's annual implementation report**		**EC's annual implementation report**	
Digital Services Act												
European Digital Identity	**Estimate enforcement of specific obligations**	**Estimation of full applicability**										
European Chips Act												

Legislative or non-legislative proposal

Entry into force (certain/estimate)

Specific obligations enter into force (certain/estimate)

Fully applicable date (certain/estimate)

Adoption date (published/estimate)

Evaluation/revision/additional procedural rules (certain/estimate)

Relevant court cases

Join Eurosmart shaping digital security standards and legislations

Eurosmart extends a warm invitation to all interested parties to join us in our pivotal mission to influence, promote, and advise on legislative frameworks concerning digital security standards and certifications. As we advocate for robust regulatory measures, the support of industry partners is paramount to our success. Whether your operations are within Europe or beyond, your collaboration is vital in bolstering our collective efforts towards fostering a secure digital environment.

Membership with Eurosmart offers the opportunity to contribute to impactful initiatives, providing access to an esteemed network of professionals, exclusive resources, and strategic partnerships. By aligning with Eurosmart, members gain a platform to actively participate in discussions, shape policies, and drive positive change in the realm of cybersecurity standards.

In navigating the complexities of evolving regulations, your partnership plays a pivotal role in advancing our shared objectives. Together, let us uphold the best regulatory and technical approaches, ensuring a safer digital future for all.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com