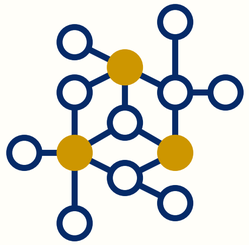
Overview of new data legislation

eubelius
advocaten avocats attorneys

January 2025



Data Governance Act (DGA)

READ MORE

Data Act

READ MORE

Digital Markets Act (DMA)

READ MORE

Digital Services Act (DSA)

READ MORE

Artificial Intelligence Act (AIA)

READ MORE

Network Information Security Directive 2 (NIS2)

READ MORE

Digital Operational Resilience Act (DORA)

READ MORE

Cyber Resilience Act (CRA)

READ MORE

Data Governance Act (DGA) — 1/2

Regulation 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act)

Legal instrument

→ Regulation

Status

✓ Applicable

Why?

→ Facilitates **data sharing** by companies, individuals and the public sector
→ Makes public sector data available for re-use in situations where such data is subject to rights of others
→ Introduces three governance mechanisms for voluntary data sharing

How could it be relevant to you?

→ Any entity that has large data sets, *e.g.* insurance companies, financial companies and institutions, mobile operators
→ Any entity that wants to re-use non-open public sector data, *e.g.* businesses and start-ups that want to use non-open public sector data in strategic domains like health, mobility, environment, energy, agriculture, finance, manufacturing, public administration and professional services
→ Entities that can benefit from data altruism (*i.e.* voluntary sharing of data on the basis of consent or permission without seeking a reward)

All sectors (specific rules for re-use of non-open public sector data)

Who?

Horizontal application:

→ Data holders (*e.g.* an employer, public sector)
→ Data subjects
→ Data users (*e.g.* companies, organisations and public sector bodies)
→ Data intermediation services that facilitate sharing of data (*e.g.* companies or public sector bodies that want to establish a commercial relationship between data holders and data users)
→ Data altruism organisations

What?

→ Voluntary sharing of data

How?

Voluntary sharing of data through 3 governance models:

1. **Re-use of public sector data,** subject to the rights of others (commercial confidentiality, statistical confidentiality, IP, personal data protected under the GDPR)
2. **Data intermediation** services, applicable to all data
3. **Data altruism**, applicable to all data

CONTINUE →

Data Governance Act (DGA) — 2/2

Regulation 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act)

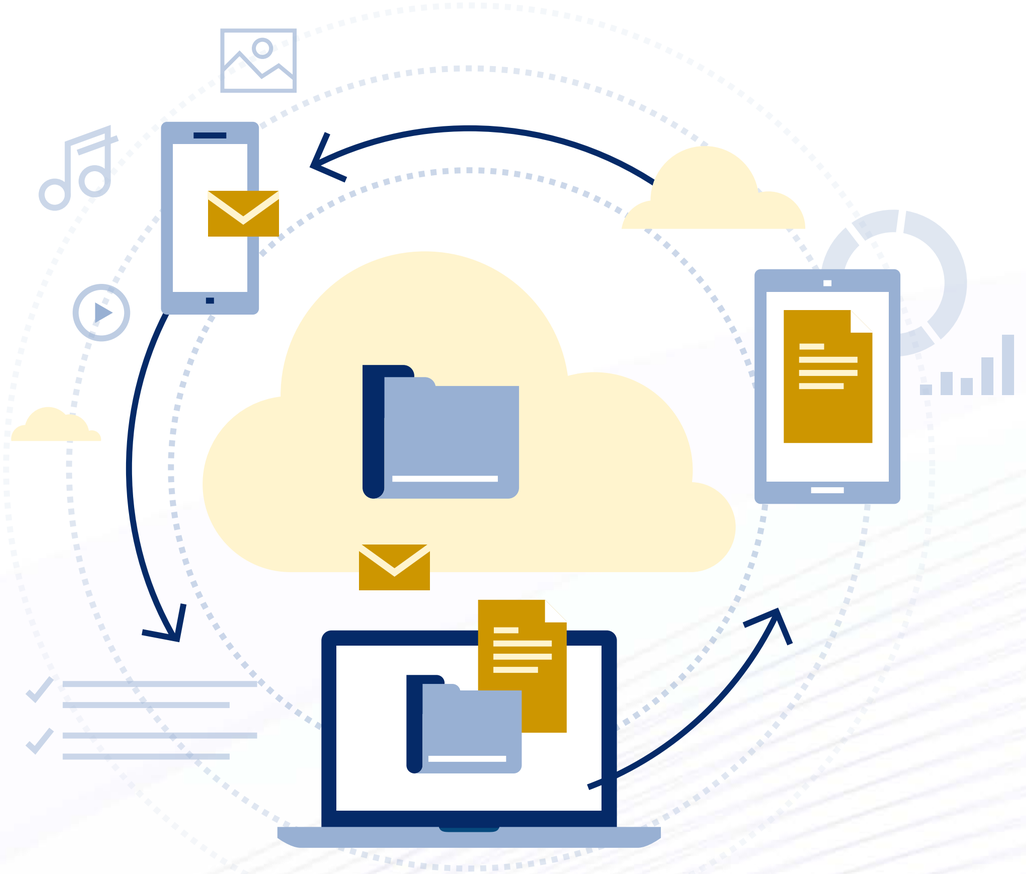
Supervision?

- European Data Innovation Board
- Designated national competent authorities

Sanctions?

Decentralised enforcement:

- Member States will decide on penalties (and will determine the amount) and will enforce them
- Designated national competent authorities can impose penalties and sanctions against data intermediation services and data altruism organisations



When?

- Applicable as of 24 September 2023
- Chapter applicable to intermediation services existing on 23 June 2022 as of 24 September 2024

CONTACT

CONTINUE

Data Act — 1/2

Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

Legal instrument

→ Regulation

Status

✓ Adopted

How could it be relevant to you?

→ Users of data generating devices (*e.g.* factory machines, smart devices, ...)
→ Users of cloud services
→ Parties exchanging data
→ Micro enterprises and SMEs
→ Creators of innovative products / services
→ Aftermarket / repair services

In all sectors (public and private)

Who?

Horizontal application:

→ Product / service manufacturers
→ Digital service providers
→ Users (data recipients)
→ Data holders that make data available to data recipients in the EU
→ Public sector bodies and EU institutions, agencies and bodies

How?

→ **Data sharing**
- Rules for the rights of data users of connected devices and related services to data generated by them and to share data (B2C and B2B)
- Horizontal rules for data sharing (B2B)

→ Measures to prevent abuse of **contractual imbalances** in data sharing contracts for all companies
→ Access to data by public bodies in exceptional need
→ Interoperability obligations, cloud switching and safeguards for international non-personal data transfers

Why?

→ Provides access to data: opening up (industrial / IoT) data to the users that help create it (*e.g.* users of data generating devices) and maximising value of data so that more data is available for innovative use

What?

Create **better access to data**: make data available

→ Clarifies who can create value with data and on which terms
→ Applies to data generated by the use of a product or related service that is made available to the user

CONTINUE

Data Act — 2/2

Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

Supervision?

- Designated national competent supervisory bodies and 1 data coordinator for each Member State
- National supervisory authorities GDPR / EDPS
- National dispute settlement bodies for disputes on data sharing

When?

- Applicable as of 12 September 2025
  - Obligations to make data accessible to the user: for products and services placed on the market as of 12 September 2026
  - Chapter on unfair terms: applicable to contracts concluded on or after 12 September 2025

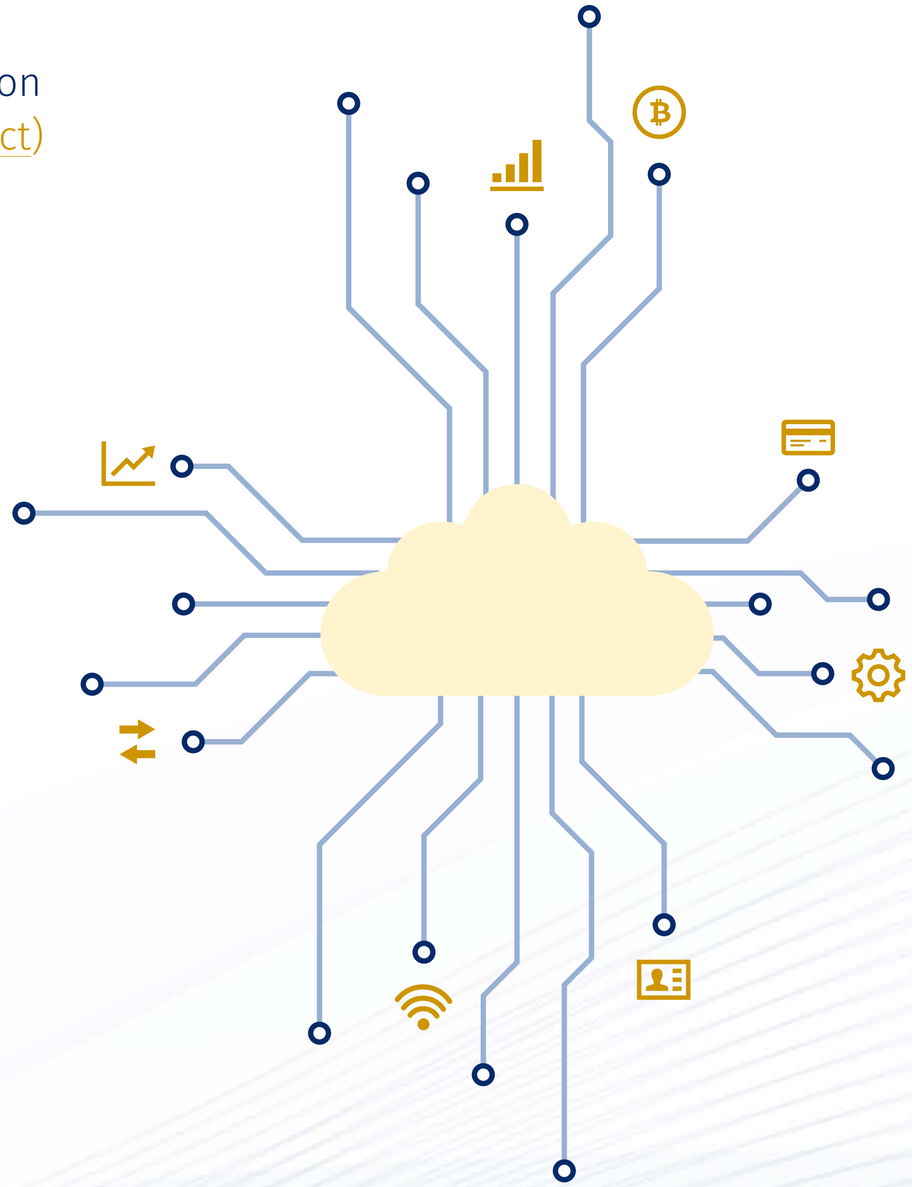
Sanctions?

Decentralised enforcement:

- National supervisory authorities under GDPR can impose **(administrative) fines** (in line with the GDPR) for non-compliance
- Sectoral authorities competent for specific sectoral data exchange
- Designated national competent authorities can impose **penalties and implementing measures**

Centralised enforcement for Union institutions:

- EDPS can impose **administrative fines**



CONTACT

CONTINUE

Digital Markets Act (DMA) — 1/2

Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act)

Legal instrument

→ Regulation

Status

✓ Adopted

Why?

→ Addresses the negative consequences arising from platforms acting as digital "gatekeepers" to the internal market

→ Promotes better competition in digital markets

How could it be relevant to you?

→ Providers of core platform services (gatekeepers), *e.g.*
- online intermediation services
- online search engines
- social networks
- video sharing platforms
- operating systems
- web browsers
- cloud computing systems
- ...

→ Businesses interacting with these services

All sectors, but mainly digital sector

What?

The DMA lays down harmonised rules ensuring contestable and fair markets in the digital sector across the Union where gatekeepers are present

Who?

Vertical application:

Applies to:

→ **Gatekeepers**, companies that provide code platform services (I) in at least 3 Member States, (II) turnover threshold, (III) minimum number of active users

→ **Core platform services**
- a. online intermediation services
- b. online search engines
- c. social networks
- d. video sharing platforms
- e. number of independent interpersonal communication services
- f. operating systems
- g. web browsers
- h. virtual assistants
- i. cloud computing systems
- j. online advertising services by an undertaking that provides any services listed in a) to i)

Does not apply to:
- a. electronic communications networks
- b. electronic communications services other than interpersonal communication services, *e.g.* internet access services

CONTINUE

Digital Markets Act (DMA) — 2/2

Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act)

How?

Gatekeeper platforms will have to:

- allow third parties to interoperate with the gatekeeper's own services in certain specific situations
- allow their business users to access the data that they generate in their use of the gatekeeper's platform
- provide companies advertising on their platform (I) with tools and information to verify ad inventories and (II) with information on prices for a given ad and advertising services
- allow their business users to promote their offer and conclude contracts with their customers outside the gatekeeper's platform
- allow installation of third-party apps and app stores on OS
- have FRAND conditions of access to app store for business users
- facilitate data portability
- allow uninstalling of any pre-installed software or app

Gatekeeper platforms may no longer:

- engage in self-preferencing in ranking
- engage in tying practices
- restrict users from unsubscribing or switching between apps and services while using the gatekeeper's OS
- prevent consumers from linking up to businesses outside their platforms
- use sensitive information from business users when competing with them
- combine personal data from different services or for delivering targeted advertising
- impose most-favoured nation clauses
- restrict business users from complaining to public authorities
- require business users to use, offer or interoperate with an identification service of the gatekeeper

The DMA also introduces specific data-related obligations:

- not to combine data from different core platform services
- to provide information to advertising companies and publishers
- to submit independent data audits to the EC
- not to use business and end user data
- to provide access to data
- to allow data portability

Supervision?

- Commission for initiation of proceedings with a view to the possible adoption of decisions
- Digital Markets Advisory Committee for the provision of opinions to the Commission

Sanctions?

Exclusive centralised enforcement by the European Commission:

- **Periodic penalty payments** not exceeding 5% of the average daily turnover in the preceding financial year per day
- **Fines** in case of a non-compliance decision up to 10% of the total turnover in the preceding year

When?

- Entry into force: 1 November 2022 (20 days after publication)
- Applicable as of 2 May 2023 (6 months after entry into force)

CONTINUE

Digital Services Act (DSA) — 1/2

Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)

Legal instrument

→ Regulation

Status

✓ Adopted

How could it be relevant to you?

→ Any provider of intermediary services in B2C and B2B markets
e.g. internet access providers, cloud and webhosting services, ...
→ Digital advertising players
e.g. ad networks, social tools, agencies, ...
→ Traders selling via online market places
e.g. (second-hand) online marketplaces, social media platforms, app stores

All sectors, but mainly digital sector

Why?

→ Amends outdated eCommerce Directive of 2000 and aligns it with developments in digital technologies and business models and new societal challenges that have emerged since (*e.g.* hate speech, fake news, ...)
→ Creates a safer and trusted online environment, adopting different responsibilities for different types of services and introduces more transparency, accountability and regulatory oversight in the EU digital landscape

Who?

Horizontal application:

Applies to:
→ **Providers of intermediary services:** mere conduit, caching, internet access providers
→ **Hosting services:** cloud and webhosting services
→ **Online platforms:** online marketplaces, app stores, social media platforms
→ **VLOPs: Very Large Online Platforms:** platforms reaching more than 10% or 450 million consumers in the EU
→ **VLOSEs: Very Large Online Search Engines:** search engines reaching a number of average monthly active recipients of the service in the EU equal to or higher than 45 million

Does not apply to:
→ any service that is not an intermediary service
→ any requirements imposed in respect of such a service, irrespective of whether the service is provided through the use of an intermediary service

CONTINUE

Digital Services Act (DSA) — 2/2

Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)

What?

The DSA lays down harmonised rules on the provision of intermediary services in the internal market. In particular, it establishes:

a. a framework for the conditional exemption from liability of providers of intermediary services
b. rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services
c. rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and coordination between the competent authorities

The DSA applies to "intermediary services", i.e. three types of information society services: mere conduit, caching and hosting. The DSA introduces "(very large) online platforms and online search engines" as a subcategory of hosting. The DSA sets out the obligations based on the intermediary concerned: it includes basic obligations for all providers of intermediary services and adds additional obligations depending on each kind of intermediary service.

How?

- Liability regime and additional obligations re illegal content
- Transparency requirements
- Measures to counter illegal goods, services or content online (trusted flaggers)
- Effective safeguards for users
- Systemic risk management requirements if +45 million users
- Additional transparency requirements (*e.g.* advertising)
- Restrictions on targeted advertising
- Appointment of qualified compliance officers
- Access to data on key platforms for researchers
- Codes of conduct and technical standards to become compliant

Supervision?

- European Board for Digital Services
- National Digital Services Coordinators (BIPT jointly with VMR, CSA and Medienrat)

Sanctions?

(Partly) Centralised enforcement for VLOPs and VLOSEs by the European Commission:

- **Periodic penalty payments** not exceeding 5% of the average daily turnover in the preceding financial year per day
- **Fines** in case of a non-compliance decision up to 6% of the total turnover in the preceding year

Decentralised enforcement at Member State level: Member States will decide on penalties applicable to infringements of the DSA by providers of intermediary services under their jurisdiction (with a maximum 6% of the annual income or turnover) and impose them.

When?

- Entry into force: 16 November 2022 (20 days after publication)
- Applicable as of 17 February 2024 (however, certain provisions will apply as from 16 November 2022, *e.g.* the provisions related to the transparency reporting obligations of online platforms, delegated acts, and the designation of very large online platforms and very large online search engines)

CONTINUE

Artificial Intelligence Act (AIA) — 1/2

European Commission: Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

Legal instrument

→ Regulation

Status

✓ Adopted

How could it be relevant to you?

- → AI systems
- → General-purpose AI models (GPAIM)
- → Providers of AI systems
- → Deployers of AI systems
- → Importers of AI systems
- → Distributors of AI systems
- → Product manufacturers
- → EU authorised representatives

In all sectors (public and private)

Why?

Enacting harmonised rules for the development, placement on the market and use of AI systems in the EU

Who?

Horizontal application:

Applies to:

- → **providers** developing an AI system or GPAIM, or having an AI system or GPAIM developed and placing it on the market or putting it into service, under its own name or trade mark, whether for payment or free of charge
- → **deployers** using an AI system under their authority

But also: importers, distributors and product manufacturers.

Does not apply to:

- → Under certain conditions, public authorities in a third country nor to international organisations when using AI-systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the EU or with its Member States.
- → Use by deployer in the course of a personal, non-professional activity.

What?

Artificial Intelligence System (AI system), defined as: "a machine-based system that is designed to operate with varying levels of autonomy, and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

General Purpose AI Model (GPAIM), defined as: "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market."

Exceptions:

The Regulation does not apply to certain AI systems (and/or GPAIM) under certain conditions *e.g.* in the context of military, defence or national security purposes, scientific research and development, used for purely non-professional activities, released under free and open-source licences, AI research, testing or development etc.

CONTINUE →

Artificial Intelligence Act (AIA) — 2/2

European Commission: Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

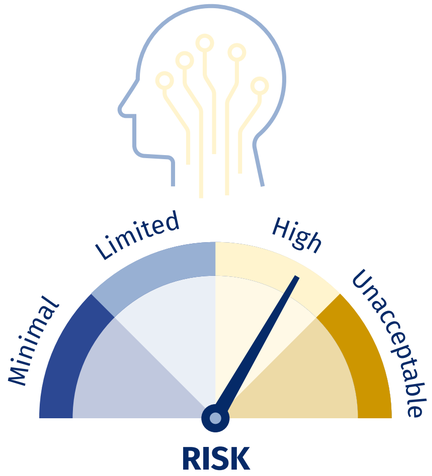
How?

The AI Act takes a **risk-based approach** and introduces a classification of various AI systems and GPAIM. Different risk levels (minimal, limited, high and unacceptable risk) for AI systems and (no) systemic risk for GPAIM come with **different requirements and obligations**

E.g. prohibited AI practices such as social scoring, real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement, emotion recognition in the workplace etc.

E.g. compliance with several strict mandatory requirements for high-risk AI systems (fundamental rights impact assessment, conformity assessment procedure, post-market monitoring system etc.).

E.g. transparency obligations for certain AI-systems, including AI-systems with limited risk.



When?

- Entry into force: 1 August 2024
- Gradual application of the provisions, *e.g.*:
  - Prohibited practices: 2 February 2025
  - Obligations and codes of practice GPAIM: 2 August 2025
  - Most other provisions, such as obligations for high-risk AI-systems in Annex III: 2 August 2026
  - Obligations high-risk AI-systems Annex I: 2 August 2027

Supervision?

- European AI Office
- European AI Board
- National competent authorities, such as market surveillance authorities, national public authorities, notifying authorities etc.

Sanctions?

Decentralised enforcement mostly by the market surveillance authorities:

- Corrective measures *e.g.* to bring into compliance, withdraw or recall AI systems
- Administrative fines of varying scales (up to EUR 35 million or 7% of the worldwide annual turnover, whichever is higher), depending on the severity of the infringement (more proportionate caps for SMEs and start-ups).
- Member States will need to lay down rules on penalties, administrative fines and other enforcement measures.

CONTACT

CONTINUE

Network Information Security Directive 2 (NIS2) and NIS 2 Laws — 1/2

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

The Act of 26 April 2024 on establishing a framework for cybersecurity of network- and information systems of general public security interest

The Royal Decree of 9 June 2024 implementing the Law of 26 April 2024 establishing a framework for cybersecurity of network- and information systems of general public security interest

Status

✓ Applicable

Why?

→ A higher level of cybersecurity in the EU: providing adapted, coordinated and innovative responses to increasing cyber threat and providing a higher level of cybersecurity and resilience

→ Expanding scope of cybersecurity rules (NIS 1) to new sectors and entities and avoiding fragmentation among member states

How could it be relevant to you?

→ Entities that are classified as a “NIS 2 entity”.

→ Entities in the supply chain of a NIS 2 entity are not directly covered by the legislation but may have more stringent contractual obligations.

→ Management bodies of entities (and their members) are responsible for approving and monitoring implementation within the entity and might face liability claims. Members of the management bodies must participate in training.

Who?

General rule: private or public medium-sized or large enterprises providing services in the following sectors (exhaustive list):

→ **Sectors of high criticality:**
- energy
- transport
- banking
- financial market infrastructures
- healthcare
- drinking water
- waste water
- digital infrastructure
- ICT service management (B2B)
- public administration
- space

→ **Other critical sectors:**
- postal and courier services
- waste management
- manufacture, production and distribution of chemicals
- production, processing and distribution of food
- manufacturing
- digital providers of online marketplaces, online search engines and social networking services platform
- research organizations

→ **Exceptions, regardless of size:**
- providers of public electronic communication networks or of publicly available electronic communications services
- trust service providers
- top-level domain name registries and domain name system service providers
- entities identified by the Centre of Cybersecurity Belgium (CCB) (*e.g.* entities that are the exclusive provider of a service essential for maintaining critical societal or economic activities)
- public administration entities of the federal state, at regional level or assistance zones
- operators of critical infrastructure
- domain name registration providers.

CONTINUE

Network Information Security Directive 2 (NIS2) and NIS 2 Laws — 2/2

What?

- Registration of NIS 2 entities
- Appropriate and proportionate technical, operational and organizational security measures
- Incident reporting
- Conformity assessments and certification

Supervision?

By the national competent authority and the CSIRT: Centre of Cybersecurity Belgium (CCB) and sectoral authorities (if applicable).

Sanctions and enforcement?

- Essential and important entities may face strict supervision by the Inspection service, including information requests and security scans. Important entities are only supervised retrospectively.
- The CCB and sectoral authorities can issue warnings, give binding instructions, appoint a supervising officer, and publicize certain infringements.
- Administrative fines for essential entities can have a maximum amount of 10 million euro, or if higher at least 2% of the total annual global turnover in the previous financial year. Important entities can be subject to an administrative fine with a maximum amount of 7 million euro, or if higher, 1,4% of the total annual global turnover in the previous financial year.

How?

- **Risk-based and all-hazards approach**, tailored to network systems and their environments, to mitigate risks, prevent incidents, and reduce consequences for service recipients.
- **Implementing the necessary cybersecurity risk-management** measures including *e.g.* policies on risk analysis and information system security, incident handling and supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.
- **Report significant incidents** to the CCB following an incident report scheme that includes several steps: early warning, incident report, interim report upon request, and final report. Reports may also be sent to the service recipients.
- **Reporting significant cyberthreats** to recipients of the services that are potentially affected.
- **Mandatory conformity assessments** (including certification) for essential entities. Important entities can choose this voluntarily (CyberFundamentals certification, ISO 27001 certification or own framework that is audited by Conformity Assessment Bodies).

When?

- The NIS 2 Act and Royal Decree are applicable as from 18 October 2024.
- Entities must register as a NIS 2 entity by 18 March 2025, except some which have until 18 December 2024.
- Essential entities must be aware of the certification deadlines of 18 April 2026 and 18 April 2027.

CONTINUE

Digital Operational Resilience Act (DORA) — 1/2

(incl. Regulatory Technical Standards and Implementing Technical Standards)

Regulation 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector and the relevant Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS)

The Act on the digital operational resilience for the financial sector transposing the Regulation 2022/2554 is not yet final.

Status

✓ Applicable (yet awaiting national transposition)

Why?

→ Establishing a uniform minimum framework for digital operational resilience of the financial sector at the European level, including third-party services providers (in the supply chain of the financial entity)

→ Ensuring technological security, proper functioning and rapid recovery from ICT related incidents and security breaches

How could it be relevant to you?

→ *Lex specialis* of NIS 2 for the financial sector

→ Introduces obligations for financial sector entities with regards to operational resilience, namely ICT-related incidents en cyber threats

→ Includes both financial sector entities and ICT third-party service providers (in the supply chain of the financial entity)

Who?

Both financial entities and ICT third-party service providers are included. Exemptions apply to certain categories, such as specific alternative investment fund managers or insurance intermediaries.

→ **Financial entities:**
- credit institutions
- payment institutions and e-money institutions
- investment firms
- account information service providers
- crypto-asset service providers and issuers of asset-referenced tokens
- central securities depositories
- central counterparties
- trading venues
- trade repositories
- managers of alternative investment funds
- management companies
- data reporting service providers
- insurance and reinsurance undertakings
- insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
- institutions for occupational retirement provision
- credit rating agencies
- administrators of critical benchmarks
- crowdfunding service providers
- securitisation repositories

→ **ICT third-party service providers, including for instance:**
- cloud computing service providers
- software providers
- data analytics services
- providers of data centre services
- penetration testing providers
- payment solutions providers

CONTACT

CONTINUE →

Digital Operational Resilience Act (DORA) — 2/2

(incl. Regulatory Technical Standards and Implementing Technical Standards)

What?

- ICT risk management (framework)
- Incident reporting of major ICT-related incidents and of significant cyber threats
- Operational resilience testing
- ICT third-party risk management, including key contractual provisions for contractual arrangements concluded between ICT third-party service providers and financial entities
- Information sharing between entities and cyberthreat intelligence

Supervision?

- The competent authority is usually determined by the underlying legislation.
- Financial institutions supervised by the FSMA are also subject to their oversight for DORA. Institutions under the supervision of the National Bank of Belgium (NBB), are also subject to their oversight.

How?

- **Setting up an ICT risk management framework** (as set out in the relevant RTS) including setting up the relevant policies and procedures, mapping and establishing assets and dependencies, business continuity management and disaster recovery.

- **Setting up an ICT-related incident management process including the incident reporting of**:
  - **Major ICT-related incidents** must be reported to the relevant authority and possibly clients, along with measures to mitigate their impact. Reporting includes initial notification, intermediate report, and final report.
  - **Significant cyber threats** to clients should be promptly reported to the relevant authority. Inform potentially affected clients of any protective measures they can take.

- Establishing and implementing **digital operational resilience testing requirements and third-party risk management requirements**.

- **List of minimum requirements for contractual arrangements** concluded between ICT third-party service providers and financial entities and an additional list in case of critical or important functions including clauses on access, recovery and return of personal and non-personal data, SLA's, obligation to provide assistance in case of related ICT-incidents and cooperation with competition authorities, notice periods etc.

Sanctions and enforcement?

Administrative penalties, criminal penalties, and remedial measures are not established by the Regulation itself but may be implemented at the national level.

When?

DORA took effect on January 16, 2023, with obligations starting from January 17, 2025.

CONTINUE

Cyber Resilience Act (CRA) — 1/2

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828

Status

✓ Applicable

Why?

Improving the security of the 'internet of things' (IoT):

- → Ensuring manufacturers design more cyber-secure products and help users maintain security throughout a product's lifecycle
- → Enhancing cybersecurity to reduce vulnerability to cyber-attacks for individuals and organizations, both public and private

How could it be relevant to you?

- → Introduces minimum cybersecurity requirements for all products with digital elements put on the EU market
- → Includes the entire EU supply chain (manufacturers, importers, distributors, open-source software stewards, conformity assessment bodies, and public authorities)

Who?

Companies placing "products with digital elements" on the EU market, regardless of location. This includes manufacturers, importers, distributors, open-source software stewards, conformity assessment bodies, and public authorities.

"Products with digital elements":

- → Connected hardware (*e.g.*, smartphones, laptops, home cameras, smartwatches, modems, firewalls, smart meters).
- → Standalone software (*e.g.*, accounting software, online games, mobile apps).

Excluded:

- → Products regulated under specific EU frameworks:
  - Medical devices (Regulations 2017/745 and 2017/746).
  - Motor vehicles and trailers (Regulation 2019/2144).
  - Civil aviation products (Regulation 2018/1139).
  - Marine equipment (Directive 2014/90/EU).
- → Identical spare parts for replacement.
- → Products for national security or defence, or designed for classified information.

CRA partially or fully excluded for products with digital elements already covered by other EU rules:

- → The product complies with existing regulations consistent with the CRA framework.
- → The existing regulations provide equivalent or higher protection.

CONTINUE →

Cyber Resilience Act (CRA) — 2/2

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828

What?

- Cybersecurity by design
- Cybersecurity by default
- User transparency
- Vulnerability and incident reporting

How?

- Connected products must be designed with cybersecurity in mind
- Measures include encrypting data stored or transmitted by the product and minimizing the attack surface
- Default settings should reduce vulnerabilities
- Users must be informed about the product's cybersecurity level
- The end-of-support date (when security updates stop) must be clearly disclosed on the product or its packaging
- Manufacturers must report actively exploited vulnerabilities and major security incidents within 72 hours, with an early warning within 24 hours
- A new centralized reporting platform with national "end-points" will simplify reporting and ensure secure data sharing among CSIRT and ENISA

Sanctions and enforcement?

Non-compliant digital products on the EU market may require corrective actions, including withdrawal or recall. The CRA enforces compliance through strict penalties, such as:

- Administrative orders to stop non-compliant activities.
- Fines up to €15 million or 2.5% of global annual turnover (whichever is higher).
- Additional corrective measures as mandated by authorities.

Supervision?

- By the national competent authority. (yet to be appointed)
- For reporting requirements: CSIRT and Enisa coordinate

When?

- The CRA will officially take effect 20 days after its publication, starting on 10 December 2024.
- Reporting requirement (article 14) will be applicable starting from 11 September 2026
- Chapter IV (notification of conformity assessment bodies) will be applicable starting from 11 June 2026

CONTINUE

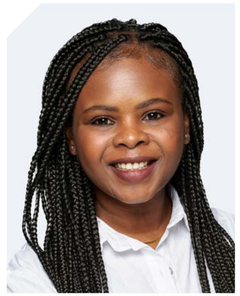
Contact

Anneleen Van de Meulebroucke
Partner
+32 2 543 32 07
anneleen.vandemeulebroucke@eubelius.com

Kim Gillade
Counsel
+32 2 543 32 56
kim.gillade@eubelius.com

Laura Deschuyteneer
Attorney
+32 2 543 32 18
laura.deschuyteneer@eubelius.com

Ellen Caen
Attorney
+32 2 543 31 48
ellen.caen@eubelius.com

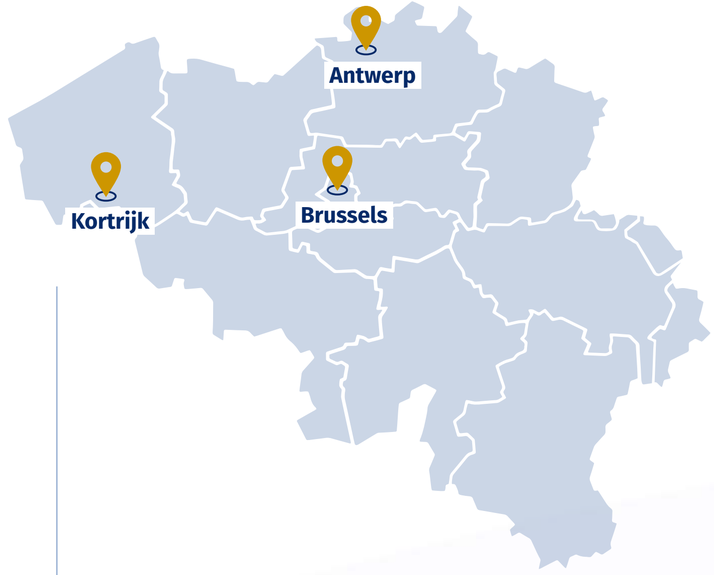


Loise Waithira
Attorney
+32 2 543 32 22
loise.waithira@eubelius.com

Sophie Devogele
Attorney
+ 32 2 543 32 78
sophie.devogele@eubelius.com

Helena Schellekens
Attorney
+32 2 543 32 72
helena.schellekens@eubelius.com

Laura Baten
Attorney
+32 2 543 35 45
laura.baten@eubelius.com



Brussels
Louizalaan 99 Avenue Louise
B-1050 Brussels
+32 2 543 31 00

Antwerp
Cockerillkaai 18
B-2000 Antwerp
+32 3 260 86 70

Kortrijk
President Kennedypark 30A
B-8500 Kortrijk
+32 56 23 51 11

CONTINUE

The information provided in this document is of a general nature and is not adapted to personal or specific circumstances of a particular person, company or other entity. This information is not intended for legal, personal or professional advice or its equivalent. The use of this information is at your own risk. If you would like legal advice tailored to your personal situation, we invite you to contact one of our attorneys or knowledge@eubelius.com.

eubelius
advocaten avocats attorneys

January 2025