Legal 500
Country Comparative Guides 2026

Belgium

Data Protection & Cybersecurity

Contributor

Loyens & Loeff

Stéphanie de Smedt

Partner | stephanie.de.smedt@loyensloeff.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Belgium.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Belgium: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

A. The following key laws/regulations apply at European Union level:

(I) Data Protection & Privacy

- **Charter of Fundamental Rights of the European Union ("EU Charter"),** which includes the right to privacy (Article 8) and is directly applicable in all EU Member States.
- **E-Privacy Directive 2002/58 ("E-Privacy Directive"),** which harmonises the laws of EU Member States to ensure an equivalent level of protection of the right to privacy and the processing of personal data in the electronic communications sector. As a Directive, it is not directly applicable, but still needs to be transposed into Member State law.
- **General Data Protection Regulation 2016/679 ("GDPR").**The GDPR is the overarching EU legislation designed to safeguard the rights and privacy of individuals in the processing of their personal data, while also facilitating the free movement of such data. In Belgium, the GDPR has direct effect, empowering individuals to directly invoke and rely on its provisions. The authority responsible for its enforcement is the Belgian Data Protection Authority (*Autorité de protection des données / Gegevensbeschermingsautoriteit*) ("Belgian DPA").
- **Police Data Directive 2016/680 ("Police Data Directive").**The Police Data Directive lays down rules relating to the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. As a Directive, it is not directly applicable, but needs to be transposed into Member State law.
- **European Health Data Space Regulation ("EHDS").**The EHDS is an EU initiative to enhance access to and control over personal electronic health data. The EHDS entered into force on 26 March 2025, marking the start of a long transition period set to conclude in March 2034. Key components of the EHDS are scheduled to take effect in March 2029, including the exchange of the first group of priority health data categories (such as Patient Summaries and ePrescriptions/eDispensations) across all EU Member States. Additionally, rules governing the secondary use of most data categories, including data from electronic health records, will also begin to apply at that time. As a Regulation, the EHDS will be directly applicable in all EU Member States.

(II) Cybersecurity

- **Cybersecurity Act 2019/881.**With a view to increasing cybersecurity in the EU, the CSA establishes a common framework for cybersecurity certification of ICT products, services, and processes, and reinforces the role of the European Union Agency for Cybersecurity ("ENISA"), by granting it enhanced responsibilities in the area of cybersecurity certification.
- **Digital Operational Resilience Act 2022/2554 (DORA).** DORA aims to enhance the IT security of financial institutions, including banks, insurance companies, and investment firms, ensuring that the European financial sector remains resilient in the face of significant operational disruptions. As an EU Regulation, DORA is directly applicable in Belgium. The authorities responsible for its enforcement are the National Bank of Belgium and the Financial Services and Markets Authority ("FSMA").
- **Network and Information Security Directive 2022/2555 ("NIS-2").** NIS-2 is aimed at building cybersecurity capabilities across the EU, mitigating threats to network and information systems used to provide essential services in key sectors, and ensuring the continuity of such services when facing

incidents. NIS-2 is the successor to the first EU NIS Directive and was adopted to respond to the increased exposure of European entities to cyber threats. As a Directive, it is not directly applicable, but needs to be transposed into Member State law. NIS-2 is supplemented by a Commission Implementing Regulation on Critical Entities and Networks, which lays down the technical and methodological requirements of the measures referred to in NIS-2 regarding entities active in the digital sector.

- **Directive on the resilience of critical entities 2022/2557 ("CER").** The CER aims to improve cybersecurity of critical entities by focusing on physical infrastructures: it aims to ensure that key sectors can withstand and respond to various forms of crisis, thereby protecting society and maintaining the continuity of vital services and functions. As a Directive, it is not directly applicable, but needs to be transposed into Member State law.
- **EU Regulation 2024/2847 – Cyber Resilience Act ("CRA")**. The CRA establishes mandatory cybersecurity requirements for products with digital elements to enhance security, transparency, and consumer protection across the internal market. It is designed to improve cybersecurity and cyber resilience for hardware and software products whose intended or foreseeable use involves direct or indirect data connection to a device or network. The authority responsible for its enforcement is the Centre for Cybersecurity Belgium ("CCB"). The implementation of the CRA will occur in different phrases from the end of 2024 to 2027.

Note: At the level of the Council of Europe (not an EU body), the European Convention on Human Rights ("**ECHR**"), which includes the right to respect for private and family life (Article 8), applies and is being enforced by the European Court of Human Rights. Additionally, consideration should be given to Convention 108, an international instrument that requires signatory countries to take the necessary steps in their domestic legislation to apply the principles it lays down ensuring fundamental human rights with regard to the processing of personal information. Convention 108 is seen as the "mother" of the EU's GDPR. It was modernised in 2018 (Convention 108+)

B. The following key national laws/regulations apply at Belgian level:

(iii) Data Protection & Privacy

- The **Constitution** is the foundation on which the political and legal organisation of Belgium is based. Its provisions include the fundamental rights and freedoms of Belgian citizens. Among its dispositions, figures the right to respect for private and family life (Article 22).
- **Code of Economic Law**, which contains certain provisions on direct marketing in its Book VI and is supplemented in this respect by the Royal Decree of 4 April 2003 regulating the sending of advertising by e-mail. The main authority responsible for the enforcement of Book VI of the Code of Economic Law is the Federal Public Service Economy ("FPS Economy").
- **Law of 21 March 2007 on the use of camera surveillance**, which regulates the use of CCTV in public and private areas. The authority responsible for its enforcement is the Belgian Data Protection Authority.
- **Law of 3 December 2017 on the establishment of the Belgian Data Protection Authority**, which establishes the legal status, composition, tasks and powers of the Belgian data protection regulator. This law was recently updated (in 2023 and 2024) to reform the internal composition of the regulator and to allow third parties to appeal enforcement decisions.
- **Law of 30 July 2018 on the protection of individuals with regard to the processing of personal data (the "Belgian Data Protection Act"),**which contains the national transposition of the Police Data Directive and some provisions of the E-Privacy Directive (notably cookie rules). It also supplements the GDPR by incorporating national choices and derogations allowed by the GDPR. The authority responsible for its enforcement is the Belgian Data Protection Authority.

(iv) Cybersecurity

- **Law of 20 July 2022 on the cybersecurity certification of information and communications technologies and designating a national cybersecurity certification authority**. This law provides the Belgian framework for the implementation of the Cybersecurity Act and is supplemented by a Royal Decree of 16 October 2022.

- **Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of public interest for public security ("NIS-2 Act")**, which is the Belgian transposition of NIS-2. The NIS-2 Act is supplemented by a **Royal Decree of 9 May 2024**. The authority responsible for its enforcement is the Centre for Cybersecurity Belgium ("CCB").
- **Belgian CER Law of 19 December 2025**. Aimed at transposing the CER Directive into Belgian law, this law was published in January 2026, with certain provisions entering into force only in April 2026. Providers of essential services that are identified as critical entities will be subject to a number of new obligations under the CER law.

Note: Additional laws and regulations apply at sector-specific level (e.g., for the financial sector, consumer credit, the telecom sector, healthcare etc.) and to certain processing by public bodies. Also the topic of employee privacy is regulated separately, by several Collective Labour Agreements (e.g., regarding electronic monitoring of employees).

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

The following key proposals related to personal data processing and cybersecurity are currently under review and are expected to enter into force in 2026:

- **Digital Omnibus initiatives.** At EU level, amendments to the GDPR, Cybersecurity Act and NIS-2 Directive are being discussed. Once consensus is found, such amendments could be adopted and enter into force in the course of 2026. The Digital Omnibus proposals include a set of technical amendments to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens alike, and to stimulate competitiveness. The immediate objective is to ensure that compliance with the rules comes at a lower cost, delivers on the same objectives, and brings in itself a competitive advantage to responsible businesses.

3. Are there any identifiable trends or regulatory priorities in privacy, data protection and/or cybersecurity-related enforcement activity in your jurisdiction?

The Belgian DPA receives more complaints and handles more cases each passing year. Generally, also the fines imposed by the Belgian DPA tend to increase in value, although they remain very modest compared to other EU jurisdictions.

In the recent years, the Belgian DPA tended to focus its activities on:

- Processing activities after the end of an employment relationship (e.g. retention of and access to professional mailboxes);
- Direct marketing and data brokerage;
- Politics and public representatives (data processing in the context of elections);
- Private use of CCTV;
- Cookies; and
- The role and independence of DPOs.

The DPA's strategic plan for 2026-2028 places a clear focus on case prioritisation and risk-based enforcement. There will be more targeted supervision, a wish for more efficient case handling (e.g. through mediation and dismissal of low-impact complaints), and a strong emphasis on large-scale high-risk data processing. Focus sectors are healthcare, finance, public sector, ad tech and education. In these sectors proactive audits can be expected. The biggest shift in practice is that there will be no more operational guidance from the DPA in individual cases without a strategic or societal impact.

For cybersecurity, as the CCB is a relatively new regulator, competent for ensuring and enforcing compliance with the NIS-2 Act and CRA, its enforcement priorities still need to be identified. There is to our knowledge no enforcement or published case law yet in Belgium since the entry into force NIS-2.

In 2026, we do expect enforcement under NIS-2 to kick off and priorities to become clear. As a more general trend, we note that the CCB focuses mostly on cyber awareness and education. It has published FAQs on the NIS-2 Act, several guidance documents, has given presentations and training, and maintains a very elaborate website with information on various cyber threats.

4. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

There are no mandatory data protection-related registration or licensing requirements for entities under the aforementioned laws, except for the obligation for companies that have appointed a Data Protection Officer ("DPO") to register such DPO with the Belgian DPA.

In the field of cybersecurity, the NIS-2 Act requires all in-scope entities to register with the CCB. Registration must be completed via the online form on the CCB's Safeonweb@Work platform. If an entity has already provided some of the required information to a sectoral authority due to another legal obligation, it only needs to update this information with the sectoral authority, which will then forward it to the CCB. Failure to register may result in sanctions such as warnings, reprimands, or orders to complete the registration. If an entity refuses to comply with an order from the CCB to register, it could face an administrative fine up to 200,000 EUR.

5. What does "personal data," "personal information" or other equivalent terms (hereafter "personal data") mean under data protection laws in your jurisdiction? Does the definition broadly include information about all individuals? For example, would this include individuals acting in a personal or household capacity, as well as those acting in a business or commercial capacity (such as on behalf of a business or corporate entity or employer) or otherwise?

The relevant definitions are those set out in Article 4 GDPR.

Personal data is "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

This definition broadly includes information about all (identified or identifiable) individuals, including those acting in a personal or household capacity, as well as those acting in a business or commercial capacity (such as on behalf of a business or corporate entity or employer).

6. Are certain types of personal data considered more sensitive or highly regulated under data protection laws in your jurisdiction? Please include the relevant defined terms for such data (e.g., special categories of personal data," "sensitive data" or "sensitive personal information"?

Special categories of personal data (commonly referred to as "sensitive data") are a subset of personal data that reveal "*racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership*" or concerns "*genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*" (Article 9 GDPR).

Note: Data related to criminal offences and convictions (Article 10 GDPR) is not included in the definition of special category data, but is commonly also deemed included in the notion of "sensitive data". The same goes for the unique National Registry Number allocated by the government to all Belgian citizens, and the processing of which is in principle prohibited (except where specifically allowed by law).

7. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

There are no specific principles provided in Belgian legislation that deviate from the GDPR. Therefore, the general principles of Articles 5 and 6 GDPR apply, notably:

1. **Lawfulness (Article 5(1)(a) GDPR),** referring to need to have a valid legal basis for the processing of personal data. The GDPR outlines an exhaustive list of legal bases (see Article 6 GDPR) and a specific list of additional requirements for the processing of "sensitive data" (see Article 9 GDPR).
2. **Fairness (Article 5(1)(a) GDPR),** meaning that personal data must be handled in a way data

subjects would reasonably expect.

3. **Transparency (Article 5(1)(a) GDPR)**, according to which data subjects should be provided with information about the processing in a form that is "easily accessible and easy to understand", using "clear and plain language". This is further detailed in Articles 13 and 14 GDPR (see question 28).
4. **Purpose limitation (Article 5(1)(b) GDPR).** Personal data should be processed for "specified, explicit and legitimate purposes". In practice, this principle dictates that before data processing begins, the purpose must be specified and that it is prohibited to process the data for a purpose incompatible with the original intent.
5. **Data minimization (Article 5(1)(c) GDPR),** according to which a data controller should collect only the minimum amount of data needed to meet the purpose of the processing.
6. **Accuracy (Article 5(1)(d) GDPR).** This is about the quality of the data collected, which must be "accurate and, where necessary, kept up to date".
7. **Storage limitation (Article 5(1)(e) GDPR),** according to which personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".
8. **Integrity and confidentiality (Article 5(1)(f) GDPR).** Personal data should be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". This requirement extends beyond cybersecurity and includes both physical and organisational security.

Finally, the data controller shall be responsible and able to demonstrate compliance with these essential processing principles (**Accountability – Article 5(2) GDPR**).

8. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

(i) Circumstances in which consent is required or typically obtained

Consent is one of the legal bases recognized by Article 6 GDPR and Article 9 GDPR. It is typically used as legal basis for the processing of photographs/images of persons, for electronic direct marketing (consent is legally required, except – under strict conditions – for electronic mailings to existing customers), and for the use of non-essential cookies (opt-in consent is required under E-Privacy implementation). In some cases, it is also used to legitimize the processing of "sensitive data" (e.g. health or biometric data) and personal data relating to criminal offences or criminal convictions (cf. Article 10 of the Belgian Data Protection Act).

The validity of a consent as legal basis for processing is determined by Article 7 GDPR, and by ample case law of the Belgian Data Protection Authority. In an employer-employee context (or in other circumstances of manifest imbalance of power), consent is however not deemed appropriate as legal basis, and often declared invalid (as not "freely given").

Finally, Article 22 GDPR also provides that consent is required – with limited exceptions – for automated decision-making which produces legal effects or similarly significantly affects a data subject.

(ii) Rules relating to the form, content and administration of consent

Article 4(11) GDPR defines a valid consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Article 7 GDPR (and recitals 32, 33, 42, and 43) provide additional guidance. Notably, valid consent must be (i) freely given (the data subject must have a genuine choice and not fear negative consequences for refusal), (ii) specific (it must be related to a specific processing operation and a determined purpose, (iii) informed (before giving consent, the individual must receive certain transparency notices), and (iv) unambiguous. In some cases (e.g., for non-essential cookies or for electronic direct marketing), consent must moreover be given explicitly ("opt-in"). Methods such as pre-ticked boxes, bundled consents, or inaction are generally not considered valid forms of consent.

The rules governing the administration of consent are the following:

- The controller must be able to demonstrate at any time that the data subject has consented under valid conditions; and
- The processing of a child's personal data based on consent is only lawful, in Belgium, if the child is at least 13 years old.

9. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

The following categories of personal data are subject to specific processing conditions (Article 4(13)(14)(15), Article 9 and recitals 51 to 56 GDPR):

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data;
- biometric data processed solely to identify a human being;
- health-related data; and
- data concerning a person's sex life or sexual orientation.

The processing of these types of personal data is in principle prohibited, except where a limited exception as set out in Article 9 GDPR applies (e.g.; consent or a legal obligation to process).

Note: Data related to criminal offences and convictions (Article 10 GDPR) is not included in the definition of special category data, but is commonly also deemed included in the notion of "sensitive data". The processing hereof is in principle prohibited, except where explicitly mandated or allowed by law. This notably covers any processing of criminal records or performance of criminal background checks.

Articles 8, 9 and 10 of the Belgian Data Protection Act (i) contain additional exceptions allowing for the processing of "sensitive" and "criminal" data, respectively; and (ii) require the data controller (or, where applicable, the data processor) to take the following additional measures when processing such data:

1. Designating the categories of individuals with access to the data, with a precise description of their function regarding the processing of the data;
2. Making this list of designated categories of individuals available to the supervisory authority upon its request; and
3. Ensuring that the designated individuals are subject to a legal or statutory obligation, or an equivalent contractual provision, to respect the confidentiality of the data concerned.

10. Do the data protection laws in your jurisdiction have special or particular requirements, restriction, or rules regarding the collection, use, disclosure or processing of personal information from or about children or minors? If so, what is the age threshold and key requirements/restrictions that go beyond those applicable, generally?

No specific rules in addition to GDPR. The age threshold is set at 13.

11. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Certain additional derogations, exclusions or limitations (i) cover the processing of the National Registry Number, (ii) apply to the processing by public bodies, government authorities and law enforcement, (iii) apply to the processing for journalistic or academic/artistic/literary purposes, for archiving in the public interest, and for scientific or historical research or statistical purposes, (iv) are included in sector-specific laws, or (v) are governed by specific labor law rules protecting privacy in an employment context.

12. Does your jurisdiction require or recommend privacy risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

Article 35 GDPR imposes an obligation on the data controller to conduct a data protection impact assessment (DPIA) before initiating any processing that

poses a high risk to the rights and freedoms of natural persons, in particular where the intended processing involves (i) an assessment of personal aspects, such as profiling, followed by a decision relating to the natural person concerned; (ii) large-scale processing of data as referred to in Articles 9-10 GDPR; or (iii) the systematic and large-scale monitoring of publicly accessible areas.

To determine whether or not a controller needs to conduct a DPIA, elements such as the types and amount of personal data, the categories and numbers of individuals involved, the nature, context, scope and purpose of the processing, the use of new technologies, and the categories of persons who may have access to the data, are relevant. For a better understanding of whether a DPIA is required, the Belgian DPA has published a DPIA manual and a list of processing activities for which a DPIA is deemed mandatory (e.g., for the use of biometric data for the purpose of uniquely identifying individuals in a public space or in private spaces accessible to the public, when health data of an individual is collected in an automated manner through an active implantable medical device; when there's large-scale and/or systematic processing of telephony, internet, or other communication data, metadata, or location data of or attributable to individuals, etc.).

Even where not mandatory, it's generally also advised to conduct a DPIA for other processing activities, as it helps controllers consider and demonstrate compliance and potential risks.

The Belgian DPA has not published any template DPIA.

Additionally, in the context of international data transfers, a "data transfer impact assessment" may also be required (see question 28).

13. Are there any specific codes of practice, or self-regulatory codes applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

Article 40 GDPR provides an opportunity for stakeholders to develop codes of conduct to ensure the effective implementation of the GDPR within specific sectors or for particular processing activities. In accordance with Article 40(5), associations and other bodies that wish to create, amend, or extend a code of conduct must submit their draft to the competent Data Protection Authority. For codes of conduct covering processing activities across multiple Member States, a cooperation mechanism between national DPAs, the European Data Protection Board (**EDPB**), and the European Commission is in place. Once approved, these codes, along with any amendments or extensions, must be published.

The Belgian DPA has approved the following codes:

- The code of conduct from the National Chamber of Notaries, approved on April 8, 2021. This code outlines specific procedures for appointing a data protection officer, ensuring data security, increasing staff awareness, and informing individuals about their data rights. The National Chamber of Notaries is responsible for ensuring compliance with this code among notaries.
- The transnational EU Cloud Code of Conduct, approved on May 20, 2021. This code implements the requirements of Article 28 of the GDPR (concerning data processors) and other relevant GDPR provisions, aimed at ensuring their application within the cloud market, including for IaaS, PaaS, and SaaS services. Scope Europe is responsible for overseeing compliance with this code.

14. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

The obligation for controllers to keep an internal record of processing activities (or ROPA) is included in Article 30 GDPR. This ROPA needs to contain at least the following:

- Name and contact details of the controller;
- Purpose of processing;
- Description of the categories of the personal data and individuals;
- (Categories of) recipients of the data;
- In case of transfers: identification of a third country or international organization;
- Retention periods; and
- Description of technical and organizational security measures.

According to the same provision, processors need to maintain a more limited ROPA. The record should at least contain information on:

- The name and contact details of each controller by which they are engaged;
- Categories of processing;
- In case of transfers, identification of a third

country or international organisation; and
- Description of technical and organizational security measures.

Article 30(5) GDPR excludes organizations with fewer than 250 employees from the ROPA obligation, except where they process special categories of data or personal data relating to criminal convictions and offences, where the processing they carry out is likely to result in a risk to the rights and freedoms of data subjects, or where the processing is not occasional.

The Belgian legislator has adopted some additional ROPA requirements in relation to processing for archiving in the public interest and for scientific or historical research or statistical purposes.

The Belgian DPA published templates of controller/processor records (in excel format), which companies are free to use on a voluntary basis. Businesses in Belgium typically use these templates, similar excel files or dedicated internal record-keeping software offered on the market by specialized providers.

In addition, to comply generally with the GDPR's accountability obligation (Article 24 GDPR), controllers are advised to establish clear internal processes and written documentation evidencing their GDPR compliance efforts and demonstrating processing decisions and modalities.

15. Do the data protection laws in your jurisdiction specifically impose data retention limitations? If so, please describe such requirement(s).

The storage limitation principle, as set out in Article 5.1.e) GDPR, requires that personal data should only be kept for as long as is necessary for its intended purpose. When no longer necessary for such purpose, personal data should be deleted or anonymised (see also Article 17 GDPR describing the right to erasure or "right to be forgotten"). Neither the GDPR, nor the Belgian Data Protection Act, impose specific data retention periods or additional requirements or procedures (except for some additional pseudonymisation/anonymisation requirements for archiving in the public interest and processing for scientific or historical research or statistical purposes). Certain minimum or maximum retention periods are however determined by other laws for certain specific types of data (e.g., payroll records, accounting documents, CCTV footage).

In practice, most companies establish a data retention policy to comply with this principle. Such policy sets out retention periods (or, at least, the means to determine such retention period) per category of personal data and/or per processing purpose. In most cases, the appropriate retention period is either linked to the expiry of a contract or to the applicable statute of limitation.

16. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

Article 36 GDPR requires that, before implementing a new processing operation that poses a significant risk to the rights and freedoms of individuals, companies are obliged to seek the advice of the competent supervisory authority, unless they can take measures to mitigate such risks. Data processing cannot commence until the Belgian DPA has evaluated the request.

Outside the framework of Article 36 GDPR, no general right or possibility for consultation with the Belgian DPA exists.

17. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

Article 37 GDPR specifies three cases in which it is mandatory to appoint a Data Protection Officer (DPO):

- The processing of data is carried out by a public authority or body, regardless of the data they process, except in the case of courts acting in their judicial capacity;
- The core activities of the controller or processor involve processing operations which, by their nature, scope, and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or
- The core activities of the controller or processor involve large-scale processing of data referred to in Article 9-10 GDPR.

The Belgian Data Protection Act adds a number of additional scenario's in which as well as specific (public) entities for which the appointment of a DPO is mandatory, such as:

- Any company or institution conducting processing for scientific or historical research

or statistical purposes (to the extent the processing may involve a "high risk" as referred to in Article 35 GDPR);
- Any private company processing personal data on behalf of a federal government or to which a federal government transfers personal data (to the extent the processing may involve a "high risk" as referred to in Article 35 GDPR);
- the public benefit foundation 'Foundation for Missing and Sexually Exploited Children', known as "Child Focus";
- the competent authorities when processing personal data with the intention of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- the Belgian intelligence and security services when processing personal data;
- the relevant authorities acting as controllers or processors processing personal data within the framework of the Belgian Act of 11 December 1998 concerning classification, security clearances, security advice and the publicly regulated service; and
- the Coordination Unit for Threat Assessment and the joint database 'Terrorism, Extremism, Radicalisation Process and their processors.

The appointment of a DPO is also mandatory for processors acting on behalf of a Flemish public body.

In addition, the law regulating the National Register of Natural Persons stipulates that those seeking authorization to access the national register must appoint a Data Protection Officer.

The position, tasks and legal responsibilities of the DPO are set out in Articles 38-39 GDPR. The Belgian DPA provides documents / a toolbox on its website that DPO's can use to perform their tasks, including a table summarizing its case law regarding the independence and position of the DPO.

In Belgium, there is no general legal obligation to appoint a CISO or other type of compliance officer, although specific sectoral laws may require similar profiles to be appointed (e.g., in financial services, healthcare and electronic communications).

18. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

While neither the GDPR, nor Belgian law, contains specific obligations regarding employee training, the principle of accountability (Article 24 GDPR) and the obligation to take adequate "organisational" measures to protect personal data processed by an organisation, are generally deemed to imply employee training obligations (as "best practice").

19. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

To comply with the transparency principle included in article 5(1)(a) GDPR, controllers must provide data subjects with information about the processing of their personal data. This obligation applies to data obtained directly from data subjects (article 13 GDPR) and to data obtained from third parties (article 14 GDPR). The information notices should be presented in a concise, transparent, intelligible, and easily accessible manner, using clear and straightforward language, in accordance with the requirements outlined in Article 12 GDPR.

Belgian law contains limited exceptions to the general transparency obligations laid down in the GDPR, notably for processing by courts and tribunals, by public bodies, and for journalistic and academic, artistic and literary purposes, as well as for archiving in the public interest and for scientific or historical research or statistical purposes.

Additionally, there is ample case law of the Belgian DPA addressing the topic of transparency and best practices for providing privacy notices to data subjects.

20. Do the data protection laws in your jurisdiction distinguish between the responsibilities of "controllers" and those of "processors" (or equivalent terms) of personal data? If so, how are such terms defined and what are the key distinctions between the obligations of controllers and processors (or equivalent terms)?

Under the GDPR, there are different roles and obligations

for controllers and processors of personal data. The controller, as defined in Article 4(7) GDPR, is the entity responsible for determining the purposes and means of processing personal data. Essentially, the controller has the primary responsibility for ensuring compliance with the GDPR.

The processor, as defined in Article 4(8) GDPR, is the entity that processes personal data on behalf of the controller and in accordance with the controller's instructions.

The GDPR imposes more limited obligations on processors, including the requirement to enter into a 'data processing agreement' with the controller (Article 28 GDPR), the obligation to maintain an internal record of processing activities (Article 30 GDPR), and data security and data breach notification obligations (Articles 32-33 GDPR).

21. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

Automated Decision-Making and Profiling (Articles 4 and 22 GDPR):

- The GDPR defines profiling in its Article 4 as *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"*.
- Article 22 GDPR regulates the process of making a decision on the basis of personal data processing without any human involvement which produces legal effects concerning the data subject or similarly affects him or her. As a rule, such automated decision-making is prohibited, unless certain exceptions apply.
- The Belgian Data Protection Act contains additional restrictions on profiling and automated decision-making for law enforcement purposes.

Tracking Technologies and Cookies:

- "Cookies" are as such not defined in Belgian law. Belgian legislation implementing the E-Privacy Directive (see question 1) regulates both cookies as well as any other type of online tracking technology. Article 10/2 of the Belgian Data Protection Act applies in this respect to all "*storage of information or the retrieval of information already stored in a subscriber's or user's terminal equipment*".
- Tracking technologies are typically used to track visitors of a website or users of an online application throughout their visit/use, and to monitor their behavior or actions across different platforms. Cookies are one of the most common tracking technologies.
- In this respect, Article 10/2 imposes both (i) transparency requirements (i.e., posting a cookie notice online), and (ii) an opt-in consent requirement for all non-essential cookies (i.e., all cookies that are not strictly necessary to transmit a communication over an electronic communications network or to provide an information society service requested by the user).
- The Belgian DPA has published guidelines and extensive case law on the use of cookies and the applicable transparency and consent requirements (notably in relation to the Transparency & Consent Framework of IAB Europe). A "cookie checklist" has been published as well (Dutch version / French version).

Other types of monitoring:

- See response to question 1: specific Belgian laws and regulations regulate (i) employee monitoring by employers, and (ii) the use of camera surveillance.

22. Do the laws in your jurisdiction include specific rules, requirement or regulator guidance regarding the use of cookies, pixels, online tracking and/or targeted advertising? Please describe any restrictions on targeted advertising and/or cross context behavioral advertising. How are these terms or any similar terms defined?

See above. The Belgian DPA has published guidelines and extensive case law on the use of cookies, pixels, and other online tracking technologies and the applicable

transparency and consent requirements (notably in relation to the Transparency & Consent Framework of IAB Europe). A "cookie checklist" has been published by the Belgian DPA as well (Dutch version / French version).

Targeted advertising requires similar opt-in consent. Although not specifically defined by Belgian law, targeted or behavioral advertising is typically regulated by the general rules included in the GDPR and E-Privacy Directive. Additionally, the EU Digital Services Act regulates all forms of online advertising. Primarily, it provides for more extensive transparency and information obligations, such as the obligation to be transparent about profiling and prohibiting the use of profiling to provide targeted advertisements towards minors, as well as the use of profiling that involves specific categories of personal data, such as religious beliefs or sexual orientation, for targeted advertising.

23. Do the data protection laws in your jurisdiction specifically restrict or regulate the "sale" of personal data and/or "data brokers"? How is "sale" and/or "data broker" or (similar/related terms) defined?

The "sale" of personal data is not defined in Belgian law. It is however a type of "processing" governed by the GDPR. Hence, the rules relating to the processing of personal data set forth by the GDPR and applicable national laws, also apply to the "sale" of personal data.

Note that the Belgian DPA has issued fines to controllers for not complying with their transparency obligations under the GDPR when selling customer data and/or for not performing proper due diligence on data brokers in terms of consent and transparency requirements. In its direct marketing guidance, the DPA specifically addresses the situation of data brokers and is highly critical of data brokerage practices.

24. Do the data protection laws in your jurisdiction specifically regulate or restrict marketing and electronic communications, including telemarketing/telephone solicitations and 'robocalls', email marketing, SMS/text messaging or other direct marketing? Please provide an overview.

Belgian law lacks a definition of direct marketing. Hence, the DPA has adopted its own definition and interpretation as to what constitutes direct marketing. The DPA very recently updated its guidance on direct marketing and published a "Recommendation 01/2025 on the processing of personal data in direct marketing". The new recommendation provides for an updated (and broader) definition of direct marketing, which is: *"all activities that result in the direct communication of messages with a promotional content to one or more identified or identifiable natural persons".* The guidance also includes several examples. It is available in Dutch and French.

The rules regarding direct marketing can be distinguished by the means of communication that are used:

- For **all types of direct marketing** (including ordinary mail), the GDPR applies to the extent it involves personal data processing.
- For **electronic direct marketing** (e.g., by means of e-mail, SMS, pop-ups, etc.), prior opt-in consent must be obtained (Article XII.13 Code of Economic Law). In limited circumstances, an opt-out right however suffices (notably for direct marketing for the company's own products and services to existing customers – not for prospects – provided that transparency requirements are met, and the addressee is provided with the opportunity to object).
- The use of **automated calling systems** without human intervention or faxes for the purpose of direct marketing is also prohibited without the prior, free, specific and informed consent of the addressee (Article VI.110 Code of Economic Law).
- For **direct marketing via telephone** (not falling within any of the two categories mentioned above), a right to object applies, which is implemented in practice by registration on an official "do not call me"-list. It is prohibited to make direct marketing calls to a number included on this list, except on the basis of the recipient's prior opt-in.

Generally, it is also forbidden to conceal the identity of the person or entity on whose behalf a marketing communication is made (Article VI.110 Code of Economic Law), and that any persistent and unwanted solicitation by telephone, fax, e-mail or other remote media towards consumers specifically, is considered an "unfair" (aggressive) commercial practice, which is equally prohibited (Article VI. 103, °3 Code of Economic Law). Finally, the use of an electronic communications network or service or other electronic means of communication to cause nuisance or harm, is prohibited, as well as setting up any "device" intended to commit the foregoing infringement, and attempts to commit it (Article 145 Electronic Communications Act).

25. Do the data protection laws in your jurisdiction regulate, restrict or impose specific obligations on the processing of biometric data, such as facial recognition. If so, how are the relevant terms defined? Are these obligations focused on the collection, use and processing of unique biometric 'identifiers' (rather than any sort of biometric measurements) ?

The processing of biometric data is regulated by the GDPR (Article 9 – as a type of "special category of personal data", see question 6), to the extent the biometric data is intended for the purpose of uniquely identifying a natural person (i.e., the restrictive legal regime of Article 9 GDPR does not apply to just any sort of biometric measurements).

The Belgian DPA has issued Guidelines addressing biometrics, notably when used in an employment context, confirming its position that biometric identification or access tools are generally deemed prohibited in Belgium due to the lack of a specific legal basis in national law and the presumed invalidity of consent in an employment relationship.

Note: The AI Act further restricts the processing of biometric data using artificial intelligence. As per the AI Act, emotion recognition systems in the workplace are classified as carrying an unacceptable risk and are thus prohibited. The AI Act also prohibits biometric categorization of natural persons to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation, as well as real-time remote biometric identification in publicly accessible spaces by law enforcement (subject to limited exceptions). Any other AI-systems using biometrics are typically classified as "high-risk", and are therefore – although not prohibited – subject to the most stringent obligations under the AI Act.

26. Are there any data protection laws in your jurisdiction that specifically address or apply to artificial intelligence or machine learning ("AI"). If so, do these laws specifically apply to the processing of personal information related to AI, or more broadly?

To date, Belgium has not adopted any national legislation on artificial intelligence or machine learning. At EU level, the AI Act has been adopted and has direct effect in Belgium.

The AI Act classifies AI systems according to risk, ranging from unacceptable risk to low risk. The AI Act imposes various requirements on the development and use of AI systems and prohibits certain AI applications that pose a threat to citizens' rights, as already exemplified in question 25. It focuses primarily on strengthening rules on data quality, transparency, human oversight and accountability in the use of AI systems. In that context, the AI Act does not specifically apply to the processing of personal information related to AI, but more broadly.

27. Are there any data localization requirements in your jurisdiction? In other words, are there any circumstances where some or all personal data is required to be stored locally, or prohibited from being transferred to or stored in certain jurisdictions?

No general data localization requirements apply in Belgium.

Neither the EU nor Belgium currently imposes any broad, cross-sector statutory requirement to store data exclusively on servers located in Belgium or even within the EU. Instead, GDPR focuses on ensuring that data (especially personal data) maintains the same high level of protection when transferred abroad rather than outright banning overseas storage (see response to question 28).

However, certain categories of data are subject to specific rules that effectively encourage or require keeping data within the EU or similarly protected jurisdictions. For example, the European Health Data Space ("**EHDS**") gives Member States the option to require that certain health data be stored and processed exclusively within the EU (or in another country with an EU adequacy decision). Similarly, the GDPR, as well as the EU Data Act and Data Governance Act, control and restrict transfers of data outside the EU, notable in case in case of requests for access from foreign government bodies.

28. Is the transfer of personal data outside your jurisdiction restricted, under certain circumstances? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or

notification to or authorization from a regulator?)

Within the European Economic Area ("EEA"), transfers of personal data from one country to another are not restricted, provided that the general principles requirements for lawful data processing – as set out in the GDPR – are respected (e.g. lawful basis for the transfer, transparency, data processing agreement in place (if needed)).

Transfers of personal data from Belgium to a country outside the EEA are regulated by Chapter V of the GDPR. No additional restrictions apply under Belgian law.

Pursuant to Chapter V of the GDPR, whenever personal data are transferred to a recipient outside the EEA, no additional restrictions apply where the country to which the data are transferred has been recognized by the European Commission as a country providing adequate protection, equivalent to the level of protection offered by the GDPR (see European Commission's "white list").

For countries not on the "white list", additional safeguards need to be implemented, except where one of the (limited) derogations set out in Article 49 GDPR applies (e.g., explicit consent, necessity for the execution of a contract with the data subject, necessity for the establishment, exercise or defence of legal claims, or a one-time occasional transfer). Where none of these derogations (which need to be interpreted restrictively) apply, the 'data exporter' and 'data importer' need to set up appropriate safeguards, providing for enforceable data subject rights and effective legal remedies for data subjects. These can include (see Article 46 GDPR), without requiring any specific authorisation from a supervisory authority, (i) Binding Corporate Rules (BCRs) in accordance with Article 47 GDPR, the implementation of Standard Contractual Clauses (SCCs), as adopted by the European Commission or by a national supervisory authority, adherence to an approved code of conduct, and certification. Subject to a prior authorisation from the competent supervisory authority, other appropriate safeguards (e.g. tailor-made contractual clauses, deviating from the SCCs), may also suffice.

Additionally, following case law of the CJEU (Schrems and Schrems II), the data exporter must carry out a transfer impact assessment ("TIA") and identify and implement supplementary measures to ensure an "essentially equivalent" level of protection applies to the personal data transferred to a third country that is not whitelisted.

29. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

Pursuant to Article 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate compliance with these data security requirements.

Additional data security obligations apply to certain sectors, such as telecom, public bodies and entities within the scope of the NIS-2 Act.

The Belgian DPA has already imposed multiple sanctions for lack of (adequate) security measures to protect personal data.

30. Are there more specific security obligations for certain types of personal data (e.g., sensitive data or special categories of personal data)?

No such specific security obligations are imposed by law. Controllers must however always adopt a risk-based approach. The implementation of enhanced security measures may therefore be warranted in case of processing of special categories of personal data.

31. Do the data protection laws in your

jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances and within what timeframe must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Article 4 GDPR defines a 'personal data breach' as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*". The Belgian Data Protection Act additionally addresses personal data breaches within public bodies. This concept is further clarified by guidelines published by the European Data Protection Board ("**EDPB**").

Additionally, the NIS-2 Act defines 'incidents' as "*any event with an actual negative impact on the security of network and information systems*".

The personal data breach notification obligations set out by Articles 33 (notification to the supervisory authority) and 34 (notification to data subjects) of the GDPR apply. Pursuant to these provisions, the Belgian DPA must be informed by the data controller, without undue delay and, where feasible, not later than 72 hours after having become aware of the data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Notifications are filed by uploading a designated notification form onto the website of the Belgian DPA. Data processors, on the other hand, are only required to inform the relevant data controller without undue delay after becoming aware of a personal data breach. When the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall also inform the data subjects concerned of the personal data breach, without undue delay. Limited exceptions apply. This obligation (and its exceptions) is further clarified by EDPB guidelines.

Entities falling within the scope of the NIS-2 Act need to report certain incidents to the local cybersecurity regulator. Notably, providers of essential services shall report without delay any incidents significantly affecting the availability, confidentiality, integrity or authenticity of the network and information systems on which the essential service or services it provides depend to the national CSIRT (the Centre for Cybersecurity), the sectoral authority or its sectoral CSIRT (as designated for energy, transportation, healthcare and digital service providers), and the National Crisis Centre established within the Ministry of Interior Affairs. An online platform is available for the filing of such notifications. Digital service providers shall notify the same regulators, without delay, in case of any incident that has a significant impact on the provision of a service offered by them in the EU, but only when the digital service provider has access to the information necessary to assess all or part of the impact of an incident.

Additional security breach notification obligations apply to providers of electronic communication services and in the financial sector.

Notifications to law enforcement are generally not mandated by law but generally recommended by the regulators and from an insurance perspective.

32. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

Data privacy rights of individuals are laid down in the GDPR, which has direct effect in Belgium. These rights include (cf. articles 12 and 15-21 GDPR) a right to information/access, to rectification, deletion ('right to be forgotten'), restriction of the processing, a right to data portability and a right to object to processing (absolute in case of direct marketing / conditional in case of processing on the basis of legitimate interests).

Additionally, data subjects also have the right to not be subject to automated decision-making which produces legal effects concerning him or her or similarly significantly affects him or her (and to oppose hereto and request to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision). Finally, data subjects also have the right to lodge a complaint with their local supervisory authority.

Article 12 GDPR provides that the controller must respond to the request within one month. This deadline can be extended by two additional months, provided that such extension is duly motivated, and the data subject has been informed about the extension within the first month. The EDPB has published Guidelines on the calculation of this delay and on the modalities for responding to data subject (access) requests.

The exercise of these rights is subject to the conditions and exceptions laid down in the GDPR and the Belgian Data Protection Act. The latter for example includes

exceptions for processing by courts and tribunals, by public bodies, for journalistic and academic, artistic and literary purposes, and for archiving in the public interest and scientific or historical research or statistical purposes.

33. Do the data protection laws in your jurisdiction allow or provide for a private right of action for violations? If so, does your jurisdiction also allow "class action" litigation (i.e., on behalf of a class or ('many') claimants)? Please explain under what circumstances in which a private right of action applies and/or a class action may be brought, and whether types of claims/violations present a higher risk of a private right of action or class action (e.g., are there statutory damages or presumed harm for certain violations)?

Yes, the Belgian Data Protection Act provides for a private right of action. Data subjects can initiate civil court cases, either in cease-and-desist proceedings or in ordinary civil proceedings (e.g. to obtain damages). See questions 34 and 35.

Representative actions are also possible, but only with a mandate from the data subjects (cf. Article 80.1 GDPR) and provided that a list of specific conditions, as set out in Article 220 of the Belgian Data Protection Act are met – in addition to the general procedural requirements to bring collective actions under Belgian law. Note that Article 80.2 GDPR (right to act without a mandate) has not been implemented by the Belgian legislator.

In Belgium, privacy-related litigation is still quire rare. There are no statutory damages or presumed harm for certain violations. Claimants need to prove (i) the infringement of a statutory obligation or other unlawful behavior, (ii) actual damage suffered, and (iii) a causal link between both. See also question 34.

34. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

Individuals are entitled to monetary damages or compensation if they are affected by breaches of data protection law. However, compensation cannot be obtained through administrative enforcement by the Belgian DPA, but requires civil (or criminal) proceedings to be initiated.

Extracontractual claims require the existence of a fault (e.g. a breach of the law), a damage, and a causal link between the two. Belgian law requires actual damage to have been sustained, which includes (sufficiently demonstrated) non-material damage, such as injury to feelings or emotional distress. When damages are granted, these can only compensate for the real prejudice suffered and can never be "punitive". Amounts granted to individuals are therefore typically rather low. It is also possible for representatives to claim damages on behalf of individuals, but only with such individuals' prior mandate and following strict procedural rules (cf. Article 220 of the Data Protection Act). Damages could also be claimed on the basis of contractual liability, in case contractual provisions on the processing of personal data have been breached by a party (e.g. a controller claiming damages from a processor based on a breach of a data processing agreement).

We are not aware of any published Belgian case law in relation to GDPR damages specifically. There has however been extensive case law of the CJEU on this topic (interpretation and application of Article 82 GDPR) in the past couple of years, which is also relevant for Belgium.

35. How are data protection laws in your jurisdiction typically enforced? What regulatory body(ies) have enforcement authority?

Data protection laws in Belgium are enforced primarily through administrative enforcement by the Belgian DPA. The DPA has investigative and corrective powers, including the authority to conduct audits, issue warnings and reprimands, and impose administrative fines for violations of data protection law. Decisions of the Belgian DPA can be appealed before the Brussels Court of Appeal (Markets Court division).

In addition, two types of civil proceedings can be brought for GDPR violations: (i) cease-and-desist proceedings, and (ii) ordinary civil proceedings. More specifically:

(1) As regards cease-and-desist proceedings, a data subject or supervisory authority can ask the President of the Court of First Instance to establish a violation of data protection laws and to take certain actions other than granting damages, if necessary, under penalty (e.g. order the cessation of the violation, order to grant access,

rectify or delete personal data, order to prohibit the use of incorrect, irrelevant, incomplete or illegal data, etc.);

(2) As regards ordinary civil proceedings, a plaintiff may claim damages to a controller or processor based on civil liability law to seek compensation for a prejudice suffered due to the violation of the GDPR by the controller or processor. In such proceedings, certain interim measures (e.g. temporary injunctions) can also be requested.

Finally, certain GDPR violations are also criminally sanctioned in Belgium. Criminal fines can be imposed on the data controller, the data processor and their personnel/representatives, for certain specific infringements enumerated in Articles 222-227 of the Belgian Data Protection Act. For example, the Belgian Data Protection Act provides for criminal fines in case of a.o. processing without a lawful basis, not respecting a data subject's right to object to direct marketing, and non-compliant international data transfers. Both controllers and processors (as well as individuals involved in the processing) can be criminally prosecuted and sanctioned. So far, this has, however, been very rare. Criminal fines could potentially go up to 30,000 EUR (to be multiplied by an indexation factor of 10) – See question 36.

36. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction? Are there any guidelines or rules for the calculation of such fines or the imposition of sanctions?

As regards administrative sanctions for GDPR violations, the Belgian DPA can impose various sanctions, among which:

- warnings and reprimands;
- orders to comply with requests of data subjects, to inform data subjects, to bring the processing into conformity, subject to penalties (e.g., for legal entities up to 25,000 EUR per day or 5% of the daily revenue per day of delay from the day determined in the decision, whichever is higher);
- the freezing, restriction or temporary or final prohibition or suspension of processing, subject to penalties;
- publication of the decision on the DPA's website (in non-anonymised form); and
- administrative fines.Cf. Article 83 GDPR, administrative fines can reach up to 20,000,000 EUR or 4% of the worldwide annual revenue of the undertaking concerned (for lesser infringements: up to 10,000,000 EUR or 2% of the annual turnover). In Belgium, the average fines imposed typically vary between 25,000 and 200,000 EUR. In practice, fines are not the most common sanction imposed by the Belgian DPA, as it tends to issue warnings, reprimands or compliance orders more often.As regards financial penalties linked to a court order in civil proceedings, these can vary widely and are usually determined by the judge based on an amount that is sufficiently dissuasive in relation to the defendant's financial capacity.Finally, as regards criminal sanctions for GDPR infringements, fines vary from 250 to 15,000 EUR (to be multiplied by an indexation factor, set today at 10) per offence. In exceptional cases, more severe fines (up to 20,000 or 30,000 EUR, to be multiplied by the indexation factor of 10) may be imposed. The controller, processor, or his representative in Belgium shall be civilly liable for the payment of fines to which his employees or representatives are convicted.The judge can also order the publication of the judgement in one or more journals as an additional sanction.Other sectorial data protection regulations (e.g. telecom, financial services) are enforced in a similar manner with similar types of sanctions.

The Belgian DPA applies the Guidelines on the calculation of administrative fines, as published by the EDPB.

37. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, they can be appealed before the Brussels Court of Appeal (Markets Court division). The Court of Appeal does not perform a new in-depth factual assessment but rather checks whether the DPA's enforcement decisions respect the scope and limits of its competence, are properly motivated, and respect the principles of due process.

38. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide an

overview of these obligations and explain their scope/applicability. For example, are all organizations subject to the requirement or only to certain organizations (e.g., based on size, sector, critical infrastructure designation, public company)? Are there specific and/or additional regulations for different industries (e.g., finance, healthcare, government)?.

1. Belgian Law of 26 April 2024 (NIS-2 Act)

This law transposes Directive (EU) 2022/2555 (NIS-2 Directive) into Belgian law and establishes a framework for securing networks and information systems of public interest. The Belgian NIS-2 Act covers the same list of sectors as annexed to the NIS-2 Directive (notably, for example, healthcare, energy, food, medical devices, managed IT and cloud computing services, transportation, public sector, etc.). In addition to fitting within one of the sectors listed in the annex, the applicability of the NIS-2 Act, and the identification of an entity as either "important" or "essential" under NIS-2, depends on the relevant organization's size (at group level) taking into account the calculation of SME thresholds as published by the European Commission in its 2003 Recommendation on micro-, small- and medium-sized enterprises.

The NIS-2 Act imposes the following main obligations on in-scope entities:

- Cybersecurity Risk Management: Organizations must adopt measures to manage cybersecurity risks, mitigate incidents, and protect service recipients;

The law mandates 11 specific measures:

1. Having risk analysis and information security policies in place;
2. Incident handling
3. Business continuity and crisis management
4. Ensuring supply chain security;
5. Ensuring security in the acquisition, development and maintenance of network and information systems;
6. Regular assessment and testing of cybersecurity risk management measures;
7. Cyber hygiene and cybersecurity trainings;
8. Cryptography and encryption;
9. HR security, access controls and access management
10. Multi-factor authentication solutions and secured communication systems; and
11. A coordinated vulnerability disclosure policy;

- Incident Notification: Entities must report significant cybersecurity incidents;
- Governance & Oversight: The management board must approve and oversee cybersecurity risk management and undergo cybersecurity training to ensure compliance; and
- Registration: Entities that are in-scope must self-register with the NIS-2 regulator, which is the Centre for Cybersecurity Belgium (CCB).

2. Belgian Law of 19 December 2025 (CER Law)

This law transposes Directive (EU) 2022/2557 and applies to providers of essential services that are expressly identified as "critical entities" by national sectoral regulators. Like NIS-2, the CER Law applies to specific sectors only (notably, for example, energy, transport, banking, public administration, food, etc.), but – within those sectors – only to entities explicitly designated as "critical" by the competent sectoral regulators. Designation takes place after discussion between the regulator and the entities concerned and remains confidential (there is no publicly available list). Note that critical entities under the CER Law will also automatically qualify as "essential" entities under NIS-2.

The CER Law requires enhanced risk management measures for critical entities (which are not specifically targeted at cybersecurity or network and information systems, but apply more generally to the infrastructure of such entities):

- Performance of comprehensive, periodic risk assessments (first one to be performed within 9 months after being designated as a critical entity);
- Establishment, maintenance and implementation of resilience measures and an appropriate resilience plan, taking into account the risks posed to the critical entity (first one within 10 months after being designated as a critical entity);
- Notification of "significant" incidents within 24 hours, with a follow-up notification within 1 month where needed;
- Mandatory cooperation with competent authorities and the sharing of information with such authorities (notably by appointing a point of contact that is available 24/7 within 6 months after being designated as a critical entity));
- Possibility to perform background checks for certain categories of personnel, subject to

compliance with data protection rules; and
- Carrying out periodic resilience exercises and updates.

These measures may be further specified by the competent sectoral authorities.

3. Regulation (EU) 2022/2554 (DORA Regulation)

DORA applies directly across the EU, including in Belgium, and imposes the following main obligations on entities within the financial sector:

- ICT Risk Management Framework: Design and implement robust ICT risk management frameworks;
- Implementation of detection mechanism/reactive measures;
- Training and awareness;
- Business continuity management;
- Oversight of third-party service providers supporting critical functions;
- Incident Reporting: Report major ICT-related incidents to the FSMA, following a structured reporting process (initial, interim, and final reports);
- Digital Operational Resilience Testing: Perform regular testing to assess and improve digital resilience;
- Third-Party Risk Management:

- Conduct due diligence on ICT third-party service providers (TPSPs);
- Enter into specific contractual agreements with ICT TPSPs; and
- Maintain and update a register of ICT TPSP relationships

- Client Communication: Notify clients if a serious ICT-related incident affects their financial interests and inform them of mitigation measures;
- Cyberthreat Notification (Voluntary): Optionally notify FSMA of significant cyberthreats that could impact financial stability, service users, or clients;
- Cross-Border Information Sharing: Provide relevant ICT incident information to enable FSMA coordination with other authorities;
- Customer Protection: Inform affected clients about protection measures in case of a significant cyber threat; and
- Outsourcing Reporting Duties: Possible delegation of reporting obligations, but the financial entity remains fully responsible for compliance.

Note that DORA mandates specific entities to perform advanced threat-led penetration testing, but this requirement applies only to selected financial entities.

39. Do the cybersecurity laws in your jurisdiction impose formal cybersecurity audit or certification requirements? If so, please provide an overview.

It is mandatory for “essential” entities under the NIS-2 Law to undergo regular conformity assessments. This assessment is carried out on the basis of a choice made by the entity between three options: (i) A CyberFundamentals (CyFun®) certification granted by a conformity assessment body authorised by the CCB;

(ii) An ISO/IEC 27001 certification; or

(iii) An inspection by the CCB's inspection service (or by a sectoral inspection service).

The inspection service may also control essential entities at any time (in the absence of an incident – ex ante – and after an incident or with sufficient evidence of non-compliance with the law – ex post).

For “important” entities, no certification requirements apply. Supervision is only carried out ex post by the inspection service, i.e. after an incident or in the light of evidence, indications, or information that an important entity is not complying with its obligations under NIS-2. However, these entities may also choose to voluntarily submit to the same certification regime as “essential” entities.

40. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding vendor and supply chain management? If so, please provide details of these requirements.

1. Belgian Law of April 26, 2024 (NIS-2 Act)

The NIS-2 Act mandates that organizations implement measures to secure their supply chain, managing risks that could impact the security of their networks and information systems. These measures aim to mitigate the effects of cybersecurity incidents on their services and end users. The law does not provide detailed guidance on how entities subject to its regulations should manage supply chain security obligations. However, the CCB recommends that entities subject to the NIS-2 Act require their suppliers to meet specific labeling or certification obligations. Additionally, entities under this legislation should consider incorporating specific cybersecurity

clauses in their contracts with suppliers.

2. Regulation (EU) 2022/2554 (DORA Regulation)

DORA requires financial entities to ensure that their operational resilience covers third-party ICT service providers. This includes developing comprehensive risk management frameworks addressing the entire supply chain. These frameworks must incorporate, among other things:

- Risk management controls;
- Incident reporting requirements;
- Testing and security guarantees; and
- Business continuity plans.

Additionally, entities are required to incorporate specific contractual obligations into their outsourcing agreements and in agreements with subcontractors. The following elements must be clearly outlined and agreed upon in contracts with ICT third-party service providers:

- Clear and complete service descriptions;
- Service and data location transparency;
- Provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data;
- Access and recovery of data;
- Service levels and revisions;
- ICT incident support;
- Cooperation with supervisory authorities;
- Termination rights and notice periods; and
- Participation in security and resilience programs.

For ICT services supporting critical or important functions, contracts must include 'enhanced' requirements, as well as for critical or important subcontractors. The following elements must be clearly outlined (in addition to the aforementioned requirements):

- Full service level descriptions;
- Notice periods and reporting obligations;
- Business contingency plans and security measures;
- Participation in financial entity's threat-led penetration testing;
- Ongoing monitoring and access rights for the financial entity and FSMA; and
- Exit strategies and transition period.

It is important to emphasize that DORA not only requires the explicit inclusion of technical, commercial, and information security aspects in the contract itself, but also mandates that each of these measures/elements be formally documented.

3. Belgian Law of 19 December 2025 (CER Law)

The CER Law requires enhanced risk management measures for critical entities (which are not specifically targeted at cybersecurity or network and information systems, but apply more generally to the infrastructure of such entities). Such risk management measures may include measures to secure their supply chain and manage supply chain security.

41. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, please provide an overview of the requirement, including whether there are any formalities that must be observed regarding such appointment (e.g., board-approval, reporting line structure, notification to regulatory body).

1. Belgian Law of April 26, 2024 (NIS-2 Act)

If an in-scope entity in the digital sector (not applicable for the other sectors under the NIS-2 Act) is not established in the EU, it must designate a representative within the EU and notify its appointment to the CCB. The representative must be established in one of the member states where services are provided. The designation of a representative by a digital entity does not affect any legal actions that may be brought against the digital entity itself.

There is no obligation for any entity under NIS-2 Act to appoint a specific physical contact person within the entity regarding cybersecurity. Members of management (including directors) are, however, responsible for the entity's compliance with the NIS-2 Act.

No specific formalities are imposed by the NIS-2 Act regarding the appointment of these representatives or contact persons.

2. Belgian Law of 19 December 2025 (CER Law)

Critical entities must designate a point of contact and communicate their details to the relevant authorities. This person is responsible for all matters related to the security and protection of the infrastructure and acts as the main liaison between the entity, the competent authorities and the police services. They need to be available 24/7.

No specific formalities are imposed by the CER Law regarding the appointment of these contact persons.

3. Regulation (EU) 2022/2554 (DORA Regulation)

There is no obligation in this regard.

42. Do the cybersecurity laws in your jurisdiction impose specific reporting or notice obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and what are the reporting and notification requirements (please also note whether these laws require reporting of certain cyber security incidents, regardless of whether there has been a 'breach of personal data')?

1. Belgian Law of April 26, 2024 (NIS-2 Act)

Under the NIS-2 Act, a significant incident is defined as: "*any incident having a significant impact on the provision of any of the services provided in the sectors or subsectors listed in Annexes I and II of the law and which:*

1° has caused or is likely to cause a severe operational disruption of any of the services provided in the sectors or subsectors listed in Annexes I and II or financial losses for the concerned entity; or

2° has affected or is likely to affect other natural or legal persons by causing significant material, bodily, or moral damage."

This definition applies regardless of whether there has been a 'breach of personal data' under GDPR.

Note that the European Commission has adopted an Implementing Regulation 2024/2690, which provides a more precise definition of what constitutes a significant incident for *digital entities* specifically.

The NIS-2 Act requires in-scope entities to notify without unjustified delay any significant incident to the CCB, as well as to the recipients of their services (when the incident is likely to disrupt the delivery of services in critical sectors for society, as mentioned in the annexes of the legislation). These recipients must then be informed of the corrective measures that can be applied and, if necessary, of the cyber threat itself.

The notification to the CCB must be prompt and take place in several stages, allowing for an appropriate and coordinated response. Generally, as soon as an entity becomes aware of a significant incident in its network or information systems, it must issue an early alert within 24 hours of this discovery, specifying whether the incident may result from illicit or malicious activities, and whether there may be cross-border implications. A second notification must follow within 72 hours, updating the previous information and providing an initial assessment of the severity and impact of the incident, as well as indicators of compromise when available. A final report, within one month after the second notification, must be submitted, which must include certain elements explicitly mentioned in the law. Finally, upon request from the authorities, interim reports may be required.

The national authority, for its part, must provide initial feedback on the significant incident and, upon the entity's request, operational guidance or advice on the implementation of potential mitigation measures. It must also provide additional technical support upon request from the entity concerned.

In addition to these requirements, all entities, regardless of whether they fall under the scope of the NIS-2 Directive, have the option to voluntarily notify cyber threats encountered and/or incidents avoided to the CCB.

2. Belgian Law of 19 December 2025 (CER Law)

The CER Law mandates the reporting of any potential threats to the security of critical infrastructure. Significant incidents should be notified to the competent authorities within 24 hours, with a detailed follow-up report within one month (if needed). This obligation applies regardless of whether there has been a 'breach of personal data' under GDPR.

3. RegulatiOn (EU) 2022/2554 (DORA Regulation)

Under DORA, the following definitions apply:

- 'ICT-related incident' is defined as "*a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity";*
- 'Significant cyber threat' is defined as "*a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident*";
- 'Major ICT-related incident' is defined as "*an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity";*

- 'Operational or security payment-related incident' is defined as "*a single event or a series of linked events unplanned by the financial entities referred to in Article 2(1), points (a) to (d), whether ICT-related or not, that has an adverse impact on the availability, authenticity, integrity or confidentiality of payment-related data, or on the payment-related services provided by the financial entity*".

When serious, financial entities must report *ICT-related incidents* to the FSMA through an initial, interim, and final report. An interim report is required if there are significant changes to the incident or at the FSMA's request. The final report includes the incident's cause analysis and its impact. When an incident affects client financial interests, entities must inform them of the incident and mitigation measures.

DORA also allows voluntary reporting of *significant cyberthreats* (cyberthreats that could result in a *major ICT-related incident* or a major *operational or security payment-related incident*). Entities may also notify significant cyberthreats to the FSMA on a voluntary basis, if they believe the threat affects the financial system, service users or clients. There are no specific timelines for this, and companies can report them at any time when they believe the cyber threat is relevant to the financial sector. The FSMA is allowed to share this with relevant authorities.

For significant cyber threats, entities may need to advise affected clients as well on appropriate protection measures.

These obligations apply regardless of whether there has been a 'breach of personal data' under GDPR.

43. Can individuals bring a private right of action for cybersecurity incidents or other violations of cybersecurity laws? If so, does your jurisdiction also allow "class action" litigation (i.e., on behalf of a class or ('many') claimants)? Please explain under what circumstances in which a private right of action and/or a class action may be brought?

While not explicitly provided for by law in case of breach of any of the aforementioned cybersecurity laws, claimants could initiate civil court cases, either in cease-and-desist proceedings or in ordinary civil proceedings (e.g. to obtain damages) in accordance with the general provisions of national tort law, provided that the applicable conditions are met.

Representative actions are not provided for.

44. How are cybersecurity laws in your jurisdiction typically enforced? What regulatory body(ies) have enforcement authority?

1. Belgian Law of April 26, 2024 (NIS-2 Act)

The national cybersecurity authority (CCB) oversees compliance with the NIS-2 Act with support from sectoral authorities, and serves as the central contact for NIS-2 implementation. The sector-specific authorities, designated by royal decree, include:

- Energy: Federal Minister for Energy or designated senior official;
- Transportation:
    - Transport (excluding waterborne): Federal Minister for Transport or designated senior official;
    - Waterborne Transport: Federal Minister for Maritime Mobility or designated senior official;
- Healthcare and life sciences:
    - Research, pharmaceutical manufacturing, and critical medical devices: Federal Agency for Medicines and Health Products (AFMPS);
    - Public Health: Federal Minister for Public Health or designated senior official;
- Digital Infrastructure: Belgian Institute for Post and Telecommunications (IBPT);
- Trust Service Providers: Federal Minister for the Economy or designated senior official;
- Digital Providers: Federal Minister for the Economy or designated senior official;
- Space and Research: Federal Minister for Scientific Policy or designated senior official;
- Drinking Water: National Security Committee;
- Banking: National Bank of Belgium (NBB);
- Financial Market Infrastructure: Financial Services and Markets Authority (FSMA);
- Medical Devices and In Vitro Diagnostics: Federal Agency for Medicines and Health Products (AFMPS).

These entities may intervene, when necessary, in the following tasks:

- Additional identification of entities that should be subject to the NIS-2 regime (consulting and proposing);
- Registration of entities;
- Organization of sector-specific exercises;
- Analysis and management of the consequences of an incident for a sector;
- Participation in certain activities of the NIS Cooperation Group;
- Raising awareness among entities in their sectors;
- National-level cooperation;
- Additional cybersecurity risk management measures;
- Incident notification (transmitting significant incidents reported by the national CSIRT to the sector-specific authorities, consulting in different situations on this matter);
- Supervision and inspection (joint or delegated);
- Administrative fines (see question 46);
- Information assistance.

2. Belgian Law of 19 December 2025 (CER Law)

The CER Law is primarily enforced by an inspection service set up in each relevant sector or sub-sector. They can impose administrative fines. Separately, criminal sanctions could also be imposed after criminal prosecution. See also question 46.

3. Regulation (EU) 2022/2554 (DORA Regulation)

The FSMA will primarily handle DORA compliance. DORA also aligns EU financial authorities, such as the European Banking Authority and European Securities and Markets Authority, to harmonize ICT risk supervision.

DORA allows EU authorities to impose fines for violations (see response to question 46).

DORA also introduces a new oversight framework, designating one of the key EU financial authorities (such as the European Banking Authority or the European Securities and Markets Authority) as the lead overseer responsible for monitoring the activities of critical ICT third-party service providers. This lead overseer will have the authority to conduct investigations, including on-site and off-site inspections, and can impose periodic penalty payments to ensure that critical ICT third-party service providers cooperate with the lead overseer during an investigation.

45. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

1. Belgian Law of April 26, 2024 (NIS-2 Act)

The CCB is empowered to oversee compliance with cybersecurity risk management measures and incident reporting requirements. For essential entities, this oversight may be both ex-ante and ex-post, including regular and targeted security audits conducted by an independent body. In contrast, for important entities, oversight is limited to ex-post assessments, triggered by evidence, indications, or information suggesting non-compliance with the NIS-2 Act.

In exercising this oversight, the CCB may:

- Request access to and obtain a copy of any document or information necessary for carrying out their supervisory mission;
- Carry out, on-site or remotely, any examination, inspection, and interview, including random checks;
- Conduct audits;
- Request any information they deem necessary for assessing the cybersecurity risk management measures adopted by the concerned entity, including documented cybersecurity policies, compliance with the obligation to submit information to the national cybersecurity authority or the relevant sectoral authority in accordance with Title I, and the implementation of the present law;
- Perform security scans based on objective, non-discriminatory, fair, and transparent risk assessment criteria, if necessary, with the cooperation of the concerned entity;
- Identify individuals present on premises used by the entity, whose interview they consider necessary for fulfilling their mission;
- Where applicable, request assistance from federal or local police forces in the event of the use of force;
- Request information from the personnel referred to in Article 9 of the Law of 15 April 1994 on the protection of the population and the environment against the hazards of ionizing radiation and concerning the Federal Agency for Nuclear Control, for the purposes of enforcing the provisions of this law;
- Enter, without prior notice and upon presentation of their official identification card, any premises used by the entity; they may only access inhabited premises with prior

authorization issued by an investigating judge.

2. Belgian Law of 19 December 2025 (CER Law)

The CER Law is primarily enforced by an inspection service set up in each relevant sector or sub-sector.

Members of the relevant inspection services may:

- Enter all areas of the critical infrastructure (conversely, they may only access habited places with prior authorization issued by a court judge);
- Review the security plans, as well as any acts, documents, and other necessary sources of information;
- Conduct any examination, inspection, and hearing, and request all necessary information; and
- Conduct ID checks and interrogations of natural persons.

3. Regulation (EU) 2022/2554 (DORA Regulation)

1. Supervisory Powers

Under DORA, the FSMA may:

- Request information: Entities must provide any information required to assess compliance with DORA — this includes documentation, policies, risk assessments, test results, incident reports, contracts with third-party providers, etc.;
- Conduct investigations and inspections: both on-site and off-site inspections of the financial entity's premises and ICT systems;
- Interview staff: They may question staff, including senior management, to understand processes and assess compliance; and
- Access data and systems: access to systems, logs, and other ICT data to evaluate operational resilience.

2. Oversight of Critical ICT third-party providers

For ICT third-party providers deemed "critical", such as major cloud or infrastructure service providers, a "Lead Overseer" (assigned by the European Supervisory Authorities – ESAs) is appointed.

The Lead Overseer has powers to:

- Request documentation and information;
- Conduct inspections, including on-site at the provider's premises; and
- Issue recommendations to mitigate risks to the financial system. These recommendations are binding in effect — financial entities must consider them in their own risk management.

46. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction? What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction? Are there any guidelines or rules for the calculation of such fines or the imposition of sanctions?

1. Belgian Law of April 26, 2024 (NIS-2 Act)

The CCB has the power to impose measures and administrative fines on companies that fail to comply with their obligations under the NIS-2 Act.

Among the list of administrative measures are:

- Warnings;
- Binding instructions or an injunction requiring remedying identified deficiencies or violations;
- Orders to cease any behaviour that violates the law and not to repeat it;
- Orders to ensure compliance with risk management measures or with incident notification obligations, within a specified timeframe;
- Instructions to inform natural or legal persons for whom the concerned entity provides services or carries out activities, that may be affected by a significant cyber threat, of the nature of the threat and any preventive or remedial measures they could take in response to this threat;
- Instructions to implement recommendations made following a security audit within a reasonable timeframe; and
- Instructions to publicly disclose specific aspects of the identified breaches.

If the measures requested are not taken within the time limit set, the following orders may be imposed:

- Order to temporarily suspend a certification or authorisation concerning all or part of the relevant services provided, or relevant activities carried out by the entity concerned; or
- Order to temporarily prohibit a natural person from exercising managerial responsibilities at

the level of managing director or legal representative in the entity concerned from exercising managerial responsibilities.

Companies that neglect to comply with this legislation may also face administrative fines. The following administrative fines can be imposed (doubled when repeated behaviour within a period of 3 years):

- 500 to 125,000 EUR for non-compliance with information obligations;
- 500 to 200,000 EUR for an entity that has sanctioned one of its employees or subcontractors for performing the obligations of the law in good faith and within the scope of their duties;
- 500 to 200,000 EUR for non-compliance with supervision obligations;
- 500 to 7,000,000 € or 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs, whichever is higher [important entities];
- 500 to 10,000,000 € or 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs, whichever is higher [essential entities].

2. Belgian Law of 19 December 2025 (CER Law)

Non-compliance with the CER Law can lead to the following criminal sanctions:

- Any critical entity that fails to comply with the obligations regarding internal resilience measures and the exchange of information can be punished with imprisonment from 8 days to 1 year and/or a criminal fine ranging from 26 EUR to 10,000 EUR (to be multiplied by an indexation factor of 10);
- Any person who voluntarily prevents or obstructs the inspection carried out by members of the inspection service, refuses to provide the information requested in connection with this inspection, or intentionally provides false or incomplete information can be punished with imprisonment from 8 days to 1 month and/or a criminal fine ranging from 26 EUR to 10,000 EUR (to be multiplied by an indexation factor of 10);.
- In case of repeated infringements, the fine shall be doubled and extended prison sentences may be applied.

Alternatively, through administrative enforcement by a sectoral authority, the following administrative fines may be applied:

- Failure to comply with the obligations regarding the exchange of information imposed is punishable by a fine ranging between 500 and 75,000 EUR;
- Failure to comply with the obligations regarding resilience measures is punishable by a fine ranging between 500 and 100,000 EUR;
- Failure to comply with the obligations regarding the exchange of information is punishable by a fine ranging between 500 and 100,000 EUR; and
- Failure to comply with the obligations regarding the conduct of inspections and audits is punishable by a fine ranging between 500 and 125,000 EUR. Any person who voluntarily prevents or obstructs the inspection carried out by members of the inspection service, who refuses to provide information requested in connection with this inspection, or who intentionally provides incorrect or incomplete information, can be punished by the same fine.

3. Regulation (EU) 2022/2554 (DORA Regulation)

Consequences for failing to comply may include administrative fines, mandatory corrective actions, public warnings, revocation of operating authorization, and compensation for damages resulting from breaches.

Non-compliance with DORA requirements can lead to administrative fines of up to 2% of a company's total annual global turnover or up to 1% of its average daily global turnover. Both individuals and companies could face fines as high as 1,000,000 EUR. Additionally, critical third-party ICT service providers supporting financial entities are subject to even higher fines, reaching up to 5,000,000 EUR for companies or 500,000 EUR for individuals.

47. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Generally, enforcement decisions are indeed subject to appeal, depending on their nature either before the Brussels Court of Appeal (Markets Court division) or in the context of an administrative appeal with the Council of State.

Contributors

Stéphanie de Smedt
Partner

stephanie.de.smedt@loyensloeff.com