COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Belgium

DATA PROTECTION & CYBERSECURITY

Contributor

Loyens & Loeff

Stéphanie de Smedt

Attorney at law – Partner | stephanie.de.smedt@loyensloeff.com

Bram Goetry

Attorney at law | bram.goetry@loyensloeff.com

Virginie de France

Attorney at law & Knowledge manager | virginie.de.france@loyensloeff.com

The authors would like to thank Hugo Nieuwenhuyse and Louise Verschueren for their valuable contributions to this chapter.

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 by them; 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 provisions of the EU Member States to ensure an equivalent level of protection of the right to privacy and the processing of personal data in the electronic communication sector. As an EU Directive, it is not directly applicable, but 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*).
- **Police Data Directive 2016/680 ("Police Data Directive").** The Police Data Directive lays down the rules relating to the protection of natural persons with regard to 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 an EU Directive, it is not directly applicable, but needs to be transposed into Member State law.

(ii) Cybersecurity

- **Network and Information Security Directive 2016/1148 ("NIS-1").** The purpose of NIS-1 is to strengthen and streamline cybersecurity and the resistance against cyber threats across the EU by imposing a minimum level of information security for network and information systems for operators of essential services, which are considered crucial for economy and society. As an EU Directive, it is not directly applicable, but needs to be transposed into Member State law.
- **Cybersecurity Act 2019/881 ("CSA").** With a view to increase cybersecurity in the EU, the CSA establishes a common European 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.

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:

(i) 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.**
- **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.

(ii) Cybersecurity

- **Law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security ("NIS Act")**, which is the Belgian transposition of NIS-1. The authority responsible for its enforcement is the Belgian Centre for Cybersecurity (*Centre pour la Cybersécurité Belgique/ Centrum voor Cybersecurity België).*
- **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 CSA and is supplemented by a **Royal Decree of 16 October 2022.**

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 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

The following key proposals related to personal data processing and cybersecurity are currently under review and are expected to enter into force in 2024-2025:

- **Regulation on digital operational resilience for the financial sector 2022/2554 ("DORA").** DORA lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities, in order to achieve a high common level of digital operational resilience. The text has already entered into force. However, it shall apply only as from 17 January 2025.
- **Directive on measures for a high common level of cybersecurity across the Union 2022/2555 ("NIS-2")**. This EU Directive replaces NIS-1. It has already been approved and entered into force, but needs to be transposed into the national laws of each EU Member State by 17 October 2024 (as it will become fully applicable on 18 October 2024). In March 2024, the Belgian implementation project has been submitted to

the Commission Interior Affairs of the Belgian Parliament.

- **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 are able to withstand and respond to various forms of crisis, thereby protecting society and maintaining the continuity of vital services and functions. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall apply those measures from 18 October 2024.
- **EU Artificial Intelligence Act ("AI Act")**, designed to safeguard fundamental rights, democracy, the rule of law, and environmental sustainability against AI systems posing excessive risks, establishing obligations for AI based on its potential risks and level of impact. The EU co-legislators reached an agreement on the text in December 2023. The European Parliament approved the agreement on 13 March 2024. The final text is expected be subject to formal endorsement by the Council of the EU in April or May 2024. Following formal approval, the AI Act will likely enter into force by the end of May 2024 and become fully applicable in the 2-3 following years. As a Regulation, the AI Act will be directly applicable in all EU Member States.
- **EU Cyber Resilience Act ("CRA").** The CRA focuses on the cybersecurity features of products themselves. In March 2024, the proposal was adopted in first reading by the Parliament. The Council still has to approve the text.
- **European Health Data Space Act ("EHDS").** The EHDS is an EU initiative to enhance access to and control over personal electronic health data. In March 2024, a political agreement was reached between the EU Parliament and the Council.
- **E-Privacy Regulation.** The E-Privacy Regulation is intended to replace the E-Privacy Directive. The proposed text has seen multiple substantial revisions over the past years and might still take several years to be adopted (if at all).

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

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.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

The relevant definitions are those set out in Article 4 of the 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*". **Special categories of personal data (commonly called "sensitive data")** is any subset of personal data that reveals "*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*".

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).

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing

personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

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. It 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)**.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

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 of the 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.

7. 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)?

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) f**reely given** (the data subject must have a genuine choice and not fear negative consequences for refusal), (ii) s**pecific** (it must be related to a specific processing operation and a determined purpose, (iii) i**nformed** (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.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

The following personal data is considered 'sensitive' and is 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.

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.

9. How do the data protection laws in your jurisdiction address health data?

See question 8 and Article 9 of the Belgian Data Protection Act, which mandates the implementation of supplementary measures when processing genetic, biometric, or health-related data. Collective Labour Agreements and labor laws also address the processing of health data of employees by their employer. Additional rules also apply to health data processing in the medical and insurance sector.

10. Do the data protection laws in your jurisdiction include any derogations, 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.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

The Belgian legislator has opted to lower the age required for minors to express valid consent in relation to information society services to 13 (Article 7 Belgian Data Protection Act). For the processing of personal data of children below the age of 13 in this context, consent from the child's legal representative is required.

The Belgian BDPA operates a website entitled "ikbeslis.be" aimed at providing children and teenagers, as well as parents and teachers, with more information on the protection of children's personal data. The website also elaborates on topics such as privacy online and at school, smart toys, sexting, photographs and videos, etc.

Note: The Digital Services Act (DSA) also introduces provisions aimed at protecting minors. For example, the DSA requires very large online platforms to take measures to protect children's rights and ensure a high level of privacy, safety and security. Moreover, the DSA prohibits profiling and personalized advertising aimed at minors.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

We refer to the legislative framework set out under question 1. Except for certain "online" offences included in the Belgian Criminal Code (e.g.; sanctioning the non-consensual dissemination of sexual images), additional legislative regimes specifically address online safety.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

The Belgian DPA is the general regulator with oversight of processing of personal data (including children's and teenagers' personal data). The enforcement powers of the DPA do not significantly differ from those set out in the GDPR. The BDPA can, request information, conduct investigations and obtain access to personal data, perform dawn-raids, impose provisional measures, as well as corrective measures and fines. We refer to questions 43-47 in this respect.

Online safety is further monitored by the Centre for Cybersecurity Belgium (see questions 1 and 38), the Cyber Emergency Response Team (CERT, which aims to analyse, contain, mitigate and combat cyberattacks in Belgium and also provides technical expertise and assistance) and the Belgian law enforcement authorities. These various bodies often consult and cooperate.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

The Belgian legislator is currently in the process of transposing NIS-2 (see question 1). Although NIS-2 does not aim to enhance online safety specifically, it aims at boosting the overall level of cybersecurity. Hence, indirectly, it will also assist in ensuring more online safety. Further changes may also result from the DSA that has become fully applicable early 2024.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

Article 25 of the GDPR sets out the principles of data protection by design and by default. These principles aim to build privacy-enhancing features into systems and procedures from the outset, ensuring that data protection is prioritised in the default settings for data processing.

Data protection by design requires data controllers to build compliance with data protection rules into the initial stages of projects involving the processing of personal data. Data protection by default requires data controllers to carefully assess certain parameters, such as the amount of personal data collected, the purposes of processing, data retention periods and data accessibility. They must then implement appropriate technical and organisational measures to ensure that, by default, only the personal data necessary for the intended purposes are processed.

The EDPB has published extensive Guidelines on data protection by design and default. The Belgian legislator

has not adopted any additional requirements in this regard.

16. Are controllers and/or processors of personal data required to maintain any internal 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 also 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.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? 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). 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).

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, the applicable statute of limitation, or certain minimum or maximum retention periods determined by law for certain types of data (e.g., payroll records, accounting documents, CCTV footage).

As regards data disposal/deletion, the Belgian DPA published in 2021 a document with guidelines concerning techniques for data cleansing and the destruction of data carriers. These guidelines discuss techniques such as overwriting, cryptographic erasure, demagnetization, etc. for different types of media (HD, SSD, paper, etc.) that either make it impossible to access the data on a protected medium (erasure without the possibility of reconstruction and encryption) or bring about the destruction of the medium (without the possibility of reconstruction). Depending on the type of storage medium, the DPA lists the recommended clean-up and destruction techniques to achieve the desired level of confidentiality.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection

regulator(s)?

Article 36 of the 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 DPA has evaluated the request. Typically, the DPA furnishes written guidance to the data controller within 8 weeks from receipt of the request. In complex cases, it may extend this timeframe by 6 weeks.

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

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

Article 35 of the 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 when 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 32).

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and 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 two additional scenario's in which the appointment of a DPO is mandatory (to the extent the processing may involve a "high risk" as referred to in Article 35 GDPR):

- A company or institution conducting processing for scientific or historical research or statistical purposes;
- A private company processing personal data on behalf of a federal government or to which a federal government transfers personal data.

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. Finally, the NIS Act provides that every essential services provider and digital service provider is required to 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).

21. 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).

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

22. 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.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

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).

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

Article 28 GDPR mandates that any processing of personal data by a processor must be governed by a contract, commonly known as a "data processing agreement", between the controller and the processor. Article 29 GDPR emphasises that the processor may not process personal data unless instructed to do so by the controller, unless otherwise required by EU or national law. If a processor acts independently when processing personal data, it effectively assumes the role of the controller.

The required minimum contract terms are determined by Article 28 GDPR. No additional requirements have been adopted in Belgium.

25. Are there any other restrictions

relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

Limited additional obligations apply to processors engaged by public bodies (e.g. requirement to appoint a DPO).

26. 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 terms defined, and what restrictions on their use are imposed, if any?

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:

- 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.
- Belgian legislation implementing the E-Privacy Directive (see question 1) regulates both cookies as well as any other type of online tracking technology, by imposing (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).

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.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

Neither one of these notions is expressly defined in the GDPR or Belgian law. They are regulated by the general rules included in the GDPR and E-Privacy Directive, as targeted advertising still often relies on the use of cookies. Hence, we refer to question 15.

Additionally, the DSA 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.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

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 already issues fines to

controllers for not complying with their transparency obligations under the GDPR when selling customer data.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

As Belgian law lacks a definition of direct marketing, the DPA has adopted the following definition in its Direct Marketing Guidelines: *"Any communication, in any form, solicited or unsolicited, coming from an organisation or person and aimed at the promotion or sale of services, products (whether or not for payment), as well as brands or ideas, addressed by an organisation or person acting in a commercial or non-commercial context, which is directly addressed to one or more natural persons in a private or professional context and involves the processing of personal data."*

The rules regarding direct marketing can be distinguished by the communications means used:

- For **all types of direct marketing** (including ordinary mail), the GDPR applies to the extent this 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).

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

The processing of biometric data is regulated by the GDPR (Article 9 – as a category of "sensitive data", see question 8 above).

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

Note: The AI Act is expected to further restrict the processing of biometric data using artificial intelligence.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

To date, Belgium has not adopted any national legislation on artificial intelligence or machine learning. At EU level, the AI Act is very close to being adopted and will have direct effect in Belgium (see question 1). The AI Act is expected to classify AI systems according to risk. It imposes various requirements on the development and use of AI systems and prohibits certain AI applications that pose a threat to citizens' rights. It focuses primarily on strengthening rules on data quality, transparency, human oversight and accountability.

32. Is the transfer of personal data outside your jurisdiction restricted? 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 data transfer impact assessment (**DTIA**) 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 white-listed.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

Pursuant to Article 32 of the 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 Act. Further changes are to be expected when the NIS-2 Directive is implemented into Belgian law.

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

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

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 of the European Data Protection Board.

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

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

Digital service providers (online marketplaces, search engines and cloud storage providers) and providers of essential services (e.g. in the transportation, healthcare, energy sector), as defined in the NIS Act, are subject to specific security requirements. The scope hereof will be extended upon the implementation of the NIS-2 Directive.

Separate security requirements also apply to the electronic communications sector, the financial sector (see also DORA) and for providers of trust services.

Further requirements for the use of artificial intelligence are expected to apply once the EU AI Act becomes applicable.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

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 personal 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) are further clarified by Guidelines of the EDPB.

Entities falling within the scope of the NIS 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 notification. 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.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

Outside of the context of notification obligations set out above, there are no specific legal requirements in Belgium for dealing with cybercrime. The competent regulators and the Belgian police (cybercrime unit) do regularly publish guidelines and recommendations, generally taking the position that ransom should not be paid.

38. Does your jurisdiction have a separate

cybersecurity regulator? If so, please provide details.

There is no separate, cross-sectorial cybersecurity regulator in Belgium. The Centre for Cybersecurity, which is the designated regulator under the NIS Act, does however generally assume the role of publishing guidance and advising businesses on cybersecurity and related topics.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, 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, any exceptions and any other relevant details.

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.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Individual data privacy rights in Belgium are exercisable through both the judicial system and administrative/regulatory enforcement. Individuals can file complaints with the Belgian DPA regarding violations of their privacy rights, which may cause the DPA to impose corrective measures such as a binding order to comply with a data subject request. Additionally, under the Belgian Data Protection Act, individuals have the right to seek judicial remedies, including injunctions (subject to penalties) and monetary compensation, through the competent courts.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

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). Representative actions are also possible, but only with a mandate from the data subjects (cf. Article 80.1 GDPR) and provided that the conditions set out in Article 220 of the Belgian Data Protection Act are met.

Finally, some infringements of GDPR are also criminally sanctioned. 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.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is 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 rather 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 representative organisations to claim damages on behalf of a group 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 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.

43. How are data protection laws in your jurisdiction enforced?

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.

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 criminally sanctioned. 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.

Violations of the NIS Act are investigated and sanctioned by the competent NIS regulators (see question 36). They have both investigative and corrective powers. They can either impose administrative fines or transfer the file to the public prosecutor for criminal enforcement.

Both decisions of the Belgian DPA and those of the NIS regulators can be appealed before the Brussels Court of Appeal (Markets Court division).

Other sectorial data protection and cybersecurity regulations (e.g. telecom, financial services) are enforced in a similar manner by the competent sectorial regulators.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

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). The highest fine imposed in Belgium to date amounted to 600,000 EUR, while more common fines typically vary between 25,000 and 100,000 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 generally vary from 250 to 15,000 EUR (to be multiplied by an indexation factor, set today at 8) per offence. In exceptional cases, more severe sanctions (up to 20,000 or 30,000 EUR, to be multiplied by the indexation factor) apply. 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.

As regards the enforcement of the cybersecurity requirements in the NIS Act:

- Criminal sanctions include possible imprisonment from 8 days to 1 year and a fine ranging from 26 to 50,000 EUR (to be multiplied by the indexation factor), or by either of these penalties alone;
- For any voluntary prevention or obstruction of the performance of the inspection by the members of the inspection service, refusal to communicate the information requested as a result of this inspection, or intentional communication of erroneous or incomplete information, higher sanctions apply: imprisonment from 8 days to 2 years and/or a fine from 26 to 75,000 EUR (to be multiplied by the indexation factor); and
- Administrative fines may range from 500 to 75,000 EUR for some 'lighter' infringements, or up to 200,000 EUR for more severe infringements.

Other sectorial data protection and cybersecurity regulations (e.g. telecom, financial services) are enforced in a similar manner with similar types of sanctions.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

The Belgian DPA applies the Guidelines on the calculation of administrative fines, as published by the EDPB. Additionally, the Belgian DPA has published its own (i) guidelines on financial penalties, and (ii) guidelines on the publication of decisions by the Litigation Chamber:

1. As regards the guidelines on financial penalties, the imposition of penalties is motivated by the required compliance with the principal condemnation. The Litigation Chamber will consider a penalty if it has doubts as to whether the infringer will spontaneously comply with the principal condemnation. The penalty can only be imposed as an accessory to the principal condemnation. The criteria taken into account are as follows: financial capacity of the condemned party, nature and gravity of the violation, financial advantage of continuing / maintaining the violation, repetition of the violation, expected resistance or cooperation of the party(ies) in enforcing the condemnation, sufficiently high amount of the penalty.
2. As regards the guidelines on the publication of enforcement decisions, the Litigation Chamber indicates that it operates on the basis of the principle that all its decisions, with a few exceptions, are published on its website, with the general aim of transparency, visibility and accountability. Publication for sanction purposes is decided on a case-by-case basis, and duly justified as such. As a rule, personal data contained in the published decisions are pseudonymized. However, the Belgian DPA can decide to publish a decision without pseudonymizing it first, as a sanction. As regards non-personal data concerning the identification of to legal entities, the Belgian DPA applies a similar reasoning, i.e. the name of the infringer will in principle be deleted, except, for instance, if the publication is imposed as a sanction, in case of retention of identification data at the request of the legal entity or if the identification of the legal entity is in the public interest.

46. Can controllers operating in your

jurisdiction appeal to the courts against orders of the regulators?

Yes, the decisions of the Litigation Chamber of the Belgian DPA (as well as the decisions of the NIS and other regulators) can be appealed before the Markets Court (section of the Brussels Court of Appeal), both by the parties involved in the proceeding before the DPA and by interested third parties.

This appeal must be directed against the decision rendered by the Belgian DPA and does not allow the parties to re-argue the points of law and fact developed before the Belgian DPA. It only concerns the legality of the decision taken by the Belgian DPA and a review of the principles of due process.

The decisions of the Markets Court can then be appealed, under certain circumstances, before the Belgian Supreme Court (on points of law/procedural flaws only).

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

The Belgian DPA receives more complaints and handles more cases each passing year and the fines imposed by the Belgian DPA tend to increase in value.

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);
- Spamming and direct marketing;
- Politics and public representatives (data processing in the context of elections);
- Private use of CCTV;
- Cookies and data brokerage; and
- The role and independence of DPOs.

Each year, the DPA publishes an annual report with a summary of its activities during the past year and a preview of its enforcement priorities for the next year.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

We are not aware of proposals for reforming the Belgian Data Protection Act.
However, there are legislative prospects regarding related topics (see response to question 2 above) at EU level, which require also Belgian implementation. For example, the NIS-2 Directive was adopted in December 2022 and must be implemented into national law by 17 October 2024 (see point 2 above). In addition, important regulations with direct applicability in Belgium are being voted on at EU level, in particular the Digital Services Act, the Cyber Resilience Act, the AI Act, the Data Act, the Data Governance Act and the European Health Data Space Act.

Contributors

Stéphanie de Smedt
Attorney at law – Partner
stephanie.de.smedt@loyensloeff.com

Bram Goetry
Attorney at law
bram.goetry@loyensloeff.com

Virginie de France
Attorney at law & Knowledge manager
virginie.de.france@loyensloeff.com

The authors would like to thank Hugo Nieuwenhuyse and Louise Verschueren for their valuable contributions to this chapter.

