CYBERSECURITY

Belgium

LEXOLOGY
Getting The Deal Through

Consulting editor
Ropes & Gray LLP

Cybersecurity

Consulting editors

Edward R McNicholas, Fran Faircloth

Ropes & Gray LLP

Quick reference guide enabling side-by-side comparison of local insights, including into the applicable legal and regulatory framework; best practices, including information sharing and insurance; enforcement, including relevant regulatory authorities, notification obligations, penalties, and avenues of private redress; threat detection and reporting; and recent trends.

Generated 15 February 2023

Table of contents

LEGAL FRAMEWORK

Legislation

Scope and jurisdiction

BEST PRACTICE

Increased protection

Voluntary information sharing

Insurance

ENFORCEMENT

Regulation

Penalties for non-compliance with cybersecurity regulations

THREAT DETECTION AND REPORTING

Policies and procedures

Time frames

Reporting

UPDATE AND TRENDS

Recent developments and future changes

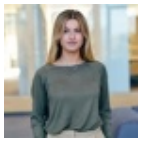
LAW STATED DATE

Correct On

Contributors

Belgium

Carmen Schellekens
Carmen.Schellekens@nautadutilh.com
NautaDutilh



Jill Van Overbeke
jill.vanoverbeke@nautadutilh.com
NautaDutilh

LEGAL FRAMEWORK

Legislation

Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

While there are no dedicated cybersecurity laws, some laws contain provisions relating to cybersecurity.

First, there are general regulations such as the Belgian Criminal Code (BCC, which notably implements the Cybercrime Convention and includes provisions on professional secrecy), the General Data Protection Regulation 2016/679 (GDPR) and the Belgian Act of 30 July 2018 , which supplements the GDPR. Second, there are more sector- or activity-specific rules, such as:

- In respect of essential services, the Belgian Act of 7 April 2019 (Belgian NIS Act) and the Act of 1 July 2011 (Belgian Critical Infrastructures Act), which implement respectively the NIS Directive and the Directive on European Critical Infrastructures. However, on 10 November 2022 the European Parliament approved the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), which will repeal the current NIS Directive. The NIS2 Directive applies to essential and important entities operating in a broader list of sectors. It is expected to be transposed into Belgian law by the end of 2024 or early 2025.
- In the telecommunications sector, Commission Regulation No. 611/2013 and the Belgian Act of 13 June 2005 (BAEC), implementing the ePrivacy Directive and modified in December 2021 to implement the European Electronic Communications Code, as well as the Belgian Act of 20 July 2022 relating to the collection and retention of identification data and metadata in the sector of electronic communications and the provision of such data to the authorities.
- In the financial sector, the European Parliament voted on 10 November 2022 in favour of the Digital Operational Resilience Act (DORA). The final adoption of DORA is expected by the end of 2022, early 2023 at the latest. Since a two-year phase-in period applies, DORA is therefore expected to become applicable by the end of 2024 or early 2025.
- In relation to trust service providers (TSPs), the Regulation no. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).
- In relation to payment service providers (PSPs), the PSD2 Act of 11 March 2018 (implementing the Payment Services Directive Two (PSD2)).

Moreover, the Cybersecurity Act (EU Regulation 2019/881) has been complemented in Belgium by the Act of 20 July 2022 on the cybersecurity certification of information and communication technologies and the Center for Cybersecurity Belgium (CCB) has been designated as the Belgian National Cybersecurity Certification Authority (NCCA).

Law stated - 21 November 2022

Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The sectors of essential services and critical infrastructure are the most affected by cybersecurity laws. These sectors are:

- the energy sector (electricity, petroleum and gas);
- the transport sector (air, rail, water and road transport);

- financial operators (financial institutions, financial trading platforms and PSPs);
- the health sector (healthcare facilities, including hospitals and private clinics);
- the sector dealing with clean water;
- the telecommunications sector;
- TSPs; and
- digital infrastructures (including digital service providers).

In light of the covid-19 pandemic, cloud service providers and providers of solutions allowing homeworking have improved the cybersecurity of their networks. Moreover, high-profile enterprises such as Microsoft, Google and Tesla have issued bug bounty programmes, where anyone can obtain a monetary reward when pointing out one of their security flaws. The automotive sector has also made cybersecurity improvements, notably after the adoption of UN Regulations No. 155 (Cyber security and cyber security management system) and No. 156 (Software update and software update management system), which apply in the European Union since July 2022.

With regard to sectors clearly needing to improve, internet of things devices in general have often been shown to be vulnerable. The same applies to the public sector (schools, government agencies, etc) and healthcare institutions.

The recent cyberwar and attacks of Russia in Ukraine highlight the importance of cybersecurity strategies and measures. In light of that, the Belgian government has added a new cyber component to the army that will be responsible for cybersecurity.

Law stated - 21 November 2022

Has your jurisdiction adopted any international standards related to cybersecurity?

Operators of essential services (OES) must have a security policy in relation to information systems and networks, and the Belgian NIS Act includes the very first recognition of ISO/IEC 27001 in this respect, stating that the required security policy is presumed compliant with the relevant requirements of the Belgian NIS Act if an organisation has ISO/IEC 27001 certification. In addition, the former Belgian Privacy Commission (now replaced by the Belgian Data Protection Authority (BDPA)) had issued guidelines on information security based on ISO 27002:2013, ISO 27005:2011 and ISO 27018:2014. Unfortunately, those guidelines are no longer available and the BDPA has not issued anything referring to such international standards yet (though its case law refers to certain best practices). Nevertheless, the CCB has published the Cybersecurity Strategy Belgium 2.0 for 2021-2025, which puts forward strategic objectives and priorities for the coming years.

Law stated - 21 November 2022

What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

In principle, an employer is liable for the behaviour of its personnel and directors (with certain exceptions). Therefore, in the case of inadequate cybersecurity, the employer will be liable towards a third party for any damage caused provided the party claiming compensation can prove a clear link of subordination between the employer and its personnel; a 'fault' (eg, negligence) made by its personnel; damage or loss arising from such fault; and the link between the fault and the function exercised by the personnel (article 1384 Belgian Civil Code).

For the same reasons, it is likely that any fines will be imposed on the employer, not the personnel or directors

individually.

However, the personnel's (in)action and 'fault' could be considered as gross negligence or be constitutive of an infringement of an internal security policy, leading to the person's dismissal. Moreover, the responsible individual can be held criminally liable in front of criminal jurisdictions.

Law stated - 21 November 2022

How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

Cybercrime, on the one hand, encompasses the crimes of internal and external hacking, which are respectively defined as a person exceeding his or her access rights with fraudulent intent and a person granting to him or herself, knowingly, unauthorised access to an IT system (articles 550-bis sections 1 and 2 BCC). Internal hacking does not cover the reuse of authorised access, but that can be considered as a breach of trust, a more general criminal offence (Cass., 24 January 2017, P 16.0048.N). The criminal handling of hacked data also constitutes a criminal offence (article 505, section1, 1° BCC). Another cybercrime is that of 'data manipulation', which occurs when a person knowingly (directly or indirectly) enters, modifies or deletes data into or from an IT system or modifies the normal use of such data. Furthermore, 'system interference' is the cybercrime of data manipulation that fully or partly hinders the functioning of an IT system (article 550-ter BCC). When such an act occurs with fraudulent intent to acquire an unlawful economic advantage, it is an 'information technology fraud' (article 504-quater BCC).

Cybersecurity, on the other hand, is to be distinguished from data privacy and data protection, as cybersecurity is about protecting information, whether it is personal data or non-personal data, and cybersecurity in relation to personal data is merely one component of data protection (which also encompasses various other aspects, such as storage limitation and data minimisation).

The EU Cybersecurity Act (Regulation 2019/881) further defines cybersecurity as 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats' (article 2(1)).

Information system security is to be distinguished from cybercrime enforcement in practice, due to the involvement of regulatory authorities (and, in particular, specialised police units) in the latter, while the former is more general.

Law stated - 21 November 2022

What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The general rules of Belgian law do not specify any specific minimum measures, such as requirements to use encryption or to have a strong password policy. Instead, these rules provide for a general requirement to implement appropriate technical and organisational measures.

For instance:

- Under data protection rules, this principle applies (see article 32, GDPR), with illustrations such as pseudonymisation and encryption of personal data.
- Regarding trade secrets, organisations must take reasonable steps, considering the circumstances, to keep them a secret and thus benefit from legal protection.
- In the telecommunications sector, providers of public electronic communications networks and of publicly available electronic communications services (ECSP) must take appropriate technical and organisational measures, taking into account the potential risks and the technical state of the art (article 107/2, BAEC). Data relating to user identification must be subject to the same security requirements during storage as when it is on

the network. Such data must be unreadable and useless for anyone who is not authorised to have access to it (article 126(4), BAEC).

- In the realm of essential services, OES must ensure a level of physical and logical security, having regard to the technical state of the art, with appropriate and proportionate technical and organisational measures (article 20, Belgian NIS Act):
  - in addition, digital service providers (DSPs) must take appropriate and proportionate technical and organisational measures, with regard to the technical state of the art, to manage the risks of security of network and information systems (article 33, Belgian NIS Act); and
  - critical infrastructure operators are also required to identify in a security policy the measures taken to prevent, mitigate and neutralise interruption or destruction risks.
  - The new NIS2 directive includes a list of seven elements that all essential and important entities must address or implement as part of the security measures they take, including risk analysis and information system security policies, incident response, business continuity and crisis management, supply chain security, assessment of effectiveness of risk management measures, and encryption and vulnerability disclosure (article 18 NIS2 Directive).
- In the financial sector, PSPs must ensure a high level of technical security and data protection (article 51, PSD2). Moreover, with regards to financial entities, DORA includes requirements on governance and ICT risk management (including documenting strategies, registers, contractual requirements) and also requires most financial entities to establish, maintain and review a digital operational resilience testing programme under which independent parties will test ICT tools and systems.
- Finally, TSPs must, having regard to the latest technological developments, take appropriate technical and organisational measures to manage the risks posed to the security of the trust service they provide (article 19, eIDAS regulation).

Law stated - 21 November 2022

Scope and jurisdiction

Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

First, the rules on professional secrecy prohibit certain professions from disclosing their clients' secrets, except where foreseen by law (article 458, BCC). Moreover, employees are prohibited from disclosing manufacturing secrets (article 309, BCC) and no one is permitted to unlawfully acquire, use or disclose trade secrets.

On the side of more traditional, 'hard' intellectual property rights, patentable inventions must be 'novel' to benefit from protection by way of a patent; secrecy is therefore crucial to benefit from protection (lack of secrecy prior to filing means that the patent application is not novel). However, a clear misuse of rights leading to a breach of secrecy does not prevent the obtaining of a patent (article XI.6, section 6 Belgian Code of Economic Law).

Finally, in the event of 'theft' of a potential trademark, any trademark registration following such breach of secrecy will be made in bad faith and can thus be invalidated (article 2.2-bis section 2, Benelux Convention on Intellectual Property; article 59(1), EU Trade Mark Regulation).

Law stated - 21 November 2022

Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

First, the Belgian NIS Act implements the NIS Directive and contains provisions on cybersecurity for essential services, such as:

- the energy sector (electricity, petroleum and gas);
- the transport sector (air, rail, water and road transport);
- financial operators (financial institutions and financial trading platforms);
- the health sector (healthcare facilities, including hospitals and private clinics);
- the sector dealing with clean water; and
- digital infrastructures.

However, the NIS2 Directive, which replaces the NIS Directive will soon be implemented into Belgian law, applies to essential and important entities operating in a broader list of sectors, including telecom, social media, public administration, food and space.

The Belgian Critical Infrastructures Act also includes specific rules for critical infrastructure operators, such as the obligation to have a security policy identifying measures to handle certain risks.

Second, provisions regarding telecommunications are described in the BAEC, implementing the ePrivacy Directive.

Moreover in the financial sector, DORA provides rules for financial entities concerning the use of ICT, particularly ICT risk management, security and business continuity, digital operation resilience testing, and contracts with ICT service providers, as well as an oversight framework for critical ICT service providers.

Finally, Belgium has adopted the PSD2 Act of 11 March 2011 about payment services.

Law stated - 21 November 2022

Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Belgian law prohibits various kinds of use of electronic communications without the consent of each person directly or indirectly involved in the communication (article 124, BAEC). This prohibition covers both the content of the communication and its metadata, and it includes intentionally becoming aware of the existence of information not intended for the person in question; intentionally identifying the persons involved in the transmission and its content; intentionally obtaining electronic communications data relating to another person; and making any use whatsoever of the aforementioned information, identification or data obtained.

However, there are exceptions to this rule, such as acts performed to verify the proper functioning of the network and the electronic communication service, and the prevention of unwanted electronic communications providing the end-user has given his or her authorisation, as well as combating fraud committed by means of messages using telephone numbers under certain conditions (articles 125, 2°, 6° and 7°, BAEC).

Telecommunications operators are subject to additional rules in relation, for example, to the use of metadata (notably with reference to the obligation to cooperate with competent authorities in the investigation and prosecution of criminal offences, as well as the possibility to use metadata for fraud detection (article 122, sections 1 and 4, BAEC). Location data is subject to even stricter rules and can as a rule only be processed if rendered anonymous or when the processing of location data is part of a location data service (article 123, BAEC).

Law stated - 21 November 2022

What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

First, external hacking and internal hacking are both criminalised (article 550-bis sections 1 and 2, BCC). External hacking occurs when a person knowingly grants him or herself unauthorised access to an IT system, while internal hacking occurs when a person exceeds his or her access rights with fraudulent intent. Internal hacking does not cover the reuse of authorised access, but that can be considered as a breach of trust, a more general criminal offence (Cass., 24 January 2017, P.16.0048.N). The criminal handling of hacked data also constitutes a criminal offence (article 505, section 1, 1°, BCC).

Another cybercrime is that of 'data manipulation', which occurs when a person knowingly (directly or indirectly) enters, modifies or deletes data into or from an IT system or modifies the normal use of such data. Furthermore, 'system interference' is the cybercrime of data manipulation that fully or partly hinders the functioning of an IT system (article 550-ter, BCC). When such an act occurs with fraudulent intent to acquire an unlawful economic advantage, it is an 'information technology fraud' (article 504-quater, BCC).

Secondly, when a person knowingly (directly or indirectly) enters, modifies or deletes data into or from an IT system or modifies the normal use of this data, this is a criminal offence called 'data manipulation'. The offence of 'system interference' is data manipulation that fully or partly hinders the functioning of an IT system (article 550-ter, BCC). When such act occurs with fraudulent intent to acquire an unlawful economic advantage, it is an 'information technology fraud' (article 504-quater, BCC).

Law stated - 21 November 2022

How has your jurisdiction addressed information security challenges associated with cloud computing?

Cloud computing service providers are considered as DSPs under the Belgian NIS Act and must therefore identify risks to the security of network and information systems that they use. Moreover, they must take appropriate and proportionate technical and organisational measures to manage such risks (article 33, Belgian NIS Act). Having regard to the technical state of the art, those measures must take into account the security of systems and facilities; how DSPs handle incidents; the business continuity management; and the monitoring, auditing and testing of security. Furthermore, there are financial sector specific regulations that impose specific requirements on service providers regarding ICT/security risks and ICT outsourcing, such as DORA and the EBA Guidelines of 29 November 2019 on ICT and security risk management. While there is no legal requirement to do so, compliance with international standards, such as those embedded in the Standards Supporting Certification report from the European Union Agency for Cybersecurity (ENISA), can also be a useful means of evidence of such measures.

Law stated - 21 November 2022

How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

This varies from one cybersecurity law to another. Cybersecurity legislation only applies to foreign organisations when it mentions it expressly. Most cybersecurity laws have no extraterritorial scope.

The GDPR affects foreign organisations when they process personal data from citizens of the European Union. The Belgian NIS Act applies to any OES having at least an establishment on Belgian territory and effectively exercising an

activity linked to the provision of at least one essential service on Belgian territory. This Act also applies to DSPs having their registered office in Belgium, as well as to DSPs without an establishment in the EU but that provide services in Belgium and have a representative in Belgium. The BAEC applies to foreign organisations only where they conduct relevant activities in Belgium. The PDS2 Act only applies to European organisations conducting activities in Belgium or organisations that are established in Belgium.

Law stated - 21 November 2022

BEST PRACTICE

Increased protection

Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The Belgian Privacy Commission, predecessor of the Belgian Data Protection Authority (BDPA), had issued guidelines on information security. Unfortunately, those guidelines are no longer available and the BDPA has not issued any guidance of its own. The BDPA's own case law suggests best practices for compliance with the General Data Protection Regulation's (GDPR) general obligation regarding cybersecurity (article 32, GDPR), such as having a Secure Sockets Layer (SSL) for web forms involving the processing of health-related data (decision No. 117/2021 of 22 October 2021) and logging mechanisms and access control for managers as well (decision No. 56/2021 of 26 April 2021).

Beyond regulator publications, it is common practice in Belgium to refer to guidelines from the European Union Agency for Cybersecurity (ENISA) (see notably the recent Railway Cybersecurity – Good Practices in Cyber Risk Management or its Cybersecurity guide for SMEs) and the ecoDa Handbook on Cybersecurity for European Board Members (which provides useful guidance for organisations on how to integrate cybersecurity considerations at board level) as well as the National Institute of Standards and Technology (NIST) Cyber Security Framework.

Law stated - 21 November 2022

How does the government incentivise organisations to improve their cybersecurity?

The government incentivises organisations to improve their cybersecurity through cybersecurity cheques, tax cuts and fines.

First, the Walloon government created a 'cybersecurity cheque', allowing SMEs to receive up to €60,000 in three years, to help them with cybersecurity audits and diagnostics and the creation of a cybersecurity policy. Similar to the cybersecurity cheque, the 'digital maturity cheque' aims to help SMEs to transition into digital and cybersecure organisations.

Second, the Flemish side of the country allows several tax schemes to promote cybersecurity innovations. For instance, they allow up to 85 per cent tax cuts on income generated by innovations related to cybersecurity.

Third, sector-specific legislation often imposes fines following the non-compliance of their provisions. For instance, the BDPA has the ability to give administrative fines of (in theory) up to €10 million or 2 per cent of the total worldwide annual turnover for violations of the GDPR. To date, the amount of fines has been significantly lower, but there is a trend towards increasing fines.

In addition, non-compliance with other legislation can lead to fines and other sanctions:

- criminal fines of up to €400,000 for non-compliance with the Belgian Act of 13 June 2005;

- fines between €500 and €100,000 as well as criminal penalties up to €240,000 for non-compliance by operators of essential services (OESs) and digital service providers (DSPs) with security measures obligations under the Belgian NIS Act, double in the case of recidivism;
- in the case of payment service providers (PSPs), administrative fines between €10,000 and 10 per cent of yearly net turnover (based on the previous accounting year) or penalty fines of maximum €2.5 million per infringement of PSD2 (or both) or a maximum of €50,000 per (further) day of non-compliance; and
- (non-qualified) trust service providers (TSPs) may lose their ability to provide (non-)qualified trust services. The service provider losing its 'qualified' status must inform the users of its services about it (article XV.26, Belgian Code of Economic Law (BCEL)). If the service provider falsely claims having a 'qualified' status, he may face up to €800,000 of criminal penalties.

Law stated - 21 November 2022

Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

Payment service providers (PSPs) must comply with the guidelines and standards issued by the European Banking Authority ((EBA) article 52, the Payment Services Directive Two (PSD2 Act)). Other useful industry standards include those issued by the European Telecommunications Standards Institute (ETSI), such as those on consumer internet of things cybersecurity (ETSI EN 303 645 v2.0.0 [European standard] and ETSI TS 103 645 [technical specification]). Moreover, the European Union Agency for Cybersecurity (ENISA) published a report about Standards Supporting Certification and is working to facilitate European standards. Finally, the ecoDa Handbook includes various references to useful standards and guidance.

Law stated - 21 November 2022

Are there generally recommended best practices and procedures for responding to breaches?

In terms of compliance with legal obligations, in Belgium, reference is often made to the guidance by the former article 29 Working Party (WP29) on personal data breach notification to notify personal data breaches, the EDPB's Guidelines 01/2021 on Examples regarding Personal Data Breach Notification (as modified in December 2021) and ENISA's methodology to assess risks in case of personal data breaches, as well as ENISA's reports on incident notifications for DSPs and TSPs.

PSPs also have the obligation to ensure monitoring, handling and follow-up of security incidents and customer claims linked to security (article 53(1) PSD2 Act), and the EBA's guidelines regarding incident notifications are important for PSPs in this respect.

More generally, regarding the handling of breaches (and not limited to official guidance on notifications), the ecoDa Handbook includes best practices that are increasingly referred to (eg, involvement of third-party forensic firms, sometimes via legal counsel to better protect confidentiality of the findings; regular tests of response to data breaches through simulations; etc).

Law stated - 21 November 2022

Voluntary information sharing

Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Data breaches or specific cyberthreats entail various notification obligations. However, voluntary notifications are also possible. For instance, potential operators of essential services (OES)s can voluntarily notify cybersecurity incidents to the national Computer Security Incident Response Team (CSIRT), the sector-specific authority or sector CSIRT, and to the national authority for identification of operators of essential services (article 30, the Belgian Act of 7 April 2019 (Belgian NIS Act)), although there are no clear incentives in the event of such notifications. More generally, at the level of the Belgian Data Protection Authority (BDPA), voluntary notifications are also possible outside of the cases where a notification is required, and this is generally well perceived by the BDPA.

Other voluntary information-sharing initiatives include for example Quarterly Cyber Threat Report events, organised by the Cyber Threat Research and Intelligence Sharing (CyTRIS) Department of the CCB, which bring together different stakeholders at least once a quarter and inform all participants about active cyber threats.

However, there is also a risk to even voluntary notifications, given that any indication that the breach was due to security failings or that the surrounding circumstances suggest an infringement of applicable requirements (eg, data protection principles) could give rise to an investigation.

Law stated - 21 November 2022

How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The Cybersecurity Certification by the CCB allows companies to evaluate and certify the security of ICT products, services and processes. It aims at maximum alignment with existing European and international reference frameworks. All certificates are published by the EU Agency for Cybersecurity (ENISA) and are valid within the European Union. This certification therefore incentivises companies to demonstrate that cybersecurity requirements, best practices and policies are in place.

Apart from that, there is no true structure for cooperation and the development of cybersecurity standards and procedures. From time to time, actors from the private sector act as consultants for the government regarding cybersecurity, but it typically depends on whether the government is prepared to start a (public or private) consultation process. This lack of interaction can lead to enforcement issues, as cybersecurity and data protection laws are often difficult to implement perfectly from a practical and business point of view.

Law stated - 21 November 2022

Insurance

Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Cyber risk insurance is available in Belgium and adoption thereof is increasing. Most of the insurance offerings provide coverage in case of loss or damage caused by cybercrime, hacker-related damage, cyber-extortion and data theft. Many of the insurances also offer 24/7 (helpdesk) assistance in the event of a cyber-attack or data breach, and/or reimburse costs for legal, IT and PR services that are necessary to limit any damage to the company and its reputation. However, the exclusions and conditions accompanying some insurances – in particular, exclusions of acts of war, given that some cyberattacks can be linked to disputes between nation states – have often given rise to discussions. Moreover, coverage is sometimes conditional upon demonstration of appropriate security measures put in place by the organisation, and insurers often send detailed questionnaires regarding the level of security prior to any premium being calculated. Finally, in practical terms, such insurance policies often require evidence in the form of a complaint with the police before they cover a breach, and although they cover certain costs there are frequently limitations in terms of

which service providers can be covered and up to what amount (or for how many hours or days after an incident occurs all qualifying costs are covered – eg, with the first 24 hours of legal support being covered).

Law stated - 21 November 2022

ENFORCEMENT

Regulation

Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

In relation to personal data, the Belgian Data Protection Authority (BDPA) is the regulatory authority responsible for enforcing the General Data Protection Regulation (GDPR) and the Belgian GDPR Act, which contain security requirements. Other authorities responsible for enforcing compliance with information security standards are different from sector to sector. First, the Belgian National Bank may impose (administrative and penalty) fines to payment service providers (PSPs). Second, the Minister of Economy is in charge of enforcing cybersecurity rules for trust service providers (TSPs), with certain powers for the BDPA. Third, the Belgian Institute for Postal Services and Telecommunications (BIPT) is in charge of compliance with the Belgian Act of 13 June 2005 (BAEC), in the telecommunication sector (with some rules falling within the jurisdiction of the BDPA). Finally, the national Computer Security Incident Response Team (CSIRT), the sector CSIRT, the national authority for identification of operators of essential services (OESs) as well as the Belgian National Bank are responsible for enforcing the the Belgian Act of 7 April 2019 (Belgian NIS Act).

The authorities charged with prosecuting cybercrimes are the police and specialised units. The latter encompass the Regional Computer Crimes Units (RCCU), which conducts technical investigations and identify culprits and the Federal Computer Crime Unit, which has a strategic role and the operational role of supporting RCCU investigations.

Law stated - 21 November 2022

Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Organisations are subject to cooperation obligations under various laws (eg, article 31, GDPR; article 122, sections 1 and 4, BAEC; article 46, Belgian NIS Act).

In addition, certain laws require organisations to actively document their processes (see eg, article 5(2) and 24 GDPR and article 107/3, section 4, BAEC), which creates authorities' expectations that these documents are readily available.

From the perspective of Belgian data protection law, for instance, the BDPA's Inspection Service and Litigation Chamber both tend to interpret articles 24 and 31 GDPR broadly, such that refusal to provide documents – even if they are not particularly relevant for a particular complaint – has been used against controllers in the past.

Law stated - 21 November 2022

What are the most common enforcement issues and how have regulators and the private sector addressed them?

The most common issues that gave rise to enforcement are the assessment of risk in the event of an incident and knowing when to notify an incident and the existence (or lack) of sufficient measures to protect information or personal data.

Notably, one case before the BDPA revolved initially around whether the organisation had an adequate methodology for dealing with potential personal data breaches. After initially bringing the methodology into question, the case ended up focusing on other aspects (such as the role of the Data Protection Officer), likely because as the case progressed, the BDPA recognised the merit of the methodology used.

In 2021, two BDPA decisions had a more marked focus on cybersecurity:

- In a decision of 26 April 2021 (decision No. 56/2021), the BDPA stated that 'the absence of any system for access control of managers' in the relevant case was a 'blatant violation' of article 32 of the GDPR, in particular because the data accessible through the system was 'sensitive financial data'. This nature meant that the risks to the fundamental rights of data subjects were high, such that the measures taken had to be 'all the more appropriate'. The lack of logging or other security measures was also viewed as preventing data subjects from exercising their right of access concerning the (unlawful) processing carried out, since the financial institution did not keep any evidence of such processing.
- In a decision of 22 October 2021 (decision No. 117/2021), the BDPA held in relation to a website that health-related data (and their transfer and transmission) should be 'sufficiently secured' and that they should 'as a result and among others be sent with sufficiently strong encryption from the user's computer to the server for a website with a form. This can take place by use of a security certificate'. This suggests that SSL is considered a minimum requirement for web forms likely to involve health-related data.

In terms of incident response, the private sector has largely started referring to approaches quoted in previous questions, such as the European Union Agency for Cybersecurity (ENISA)'s data breach severity assessment methodology (for data protection), ENISA's digital service providers (DSP) incident notification report (for DSPs under the NIS rules) and the EBA's guidelines for PSPs.

Law stated - 21 November 2022

What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Depending on the applicable legal framework, several distinct notification obligations may apply.

First, under data protection rules, processors must notify controllers of any personal data breach relating to the personal data processed on behalf of the controller; a controller in turn must notify any personal data breach to the authority (in Belgium the BDPA) unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (with three separate use cases having been identified by WP29). Data subjects must be notified of any personal data breach by controllers if such breach is likely to result in a high risk to their rights and freedoms (with three [other] use cases in which the GDPR considers that there is no 'high' risk).

When there is a risk of breach of the network security, publicly available electronic communications services (ECSPs) must notify such risk to the BIPT; where there is a personal data breach, they must notify it to the BDPA. ECSPs must also notify individuals where a personal data breach is likely to adversely affect their data or privacy, unless technological protection measures rendered the data unintelligible to anyone not authorised to access it. In addition, in the case of a specific and significant threat of a cybersecurity incident, the ECSP must inform any users that are potentially affected by such incident.

Under the current Belgian NIS Act, OESs and DSPs are subject to incident notification obligations as well: OESs for any incidents having a significant impact on the continuity of the essential services they provide; DSPs for any incidents having a substantial impact on the provision of the digital service (as defined) provided by the DSP in question. OESs

must notify incidents simultaneously to the national CSIRT, the sector-specific authority or sector CSIRT and the national authority for identification of operators of essential services. FSOs must notify breaches to the National Bank of Belgium (article 25 Belgian, NIS Act and 96 PSD2). Those notification obligations apply even if there is not enough information for the determination of the notion of a 'significant impact'.

The new NIS2 Directive lays out more specific obligations. When there's a cybersecurity incident having a significant impact on the services of essential and important entities, they shall report that incident without undue delay and in any case within 24 hours to the national competent authority or the CSIRT and shall provide them a final report within a month (article 20 NIS2 Directive).

PSPs must notify any major operational or security incident to payment service users, if the incident may have or has an impact on their financial interests (article 96, the Payment Services Directive Two (PSD2)).

TSPs must notify to the BDPA any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein to their customers if it is likely to adversely affect them, without undue delay (article 19, electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)).

Under the Digital Operational Resilience Act (DORA), financial entities will have to notify the competent authority about major ICT-related incidents without undue delay and in any case before the end of the business day, provide an intermediate report no later than a week after the notification and a final report within a month (article 17, DORA).

Law stated - 21 November 2022

Penalties for non-compliance with cybersecurity regulations

What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Failure to comply with the GDPR can in theory lead to administrative fines up to the higher of €10 million or 2 per cent of the total worldwide annual turnover (though to date, the highest fine for non-compliance with article 32, GDPR in Belgium was €100,000). Secondly, non-compliance with the BAEC can lead to criminal fines of up to €400,000. Furthermore, non-compliance with security measures obligations from the NIS can incur a fine between €500 and €100,000 as well as criminal penalties of up to €240,000. The fines are doubled in the event of recidivism. NIS2 will be stricter in that regard as it establishes administrative fines up to €10 million or 2 per cent of the entities' total worldwide turnover, whichever is higher.

Moreover, PSPs may be imposed administrative fines between €10,000 and 10 per cent of their yearly net turnover (based on their previous accounting year) or penalty fines of maximum €2.5 million per infringement of the PSD2 (or both) or a maximum of €50,000 per (further) day of non-compliance.

Finally, (non-qualified) TSPs may lose their ability to provide (non-)qualified trust services. The service provider losing his or her 'qualified' status must inform the users of its services of this (article XV.26 Belgian Code of Economic Law (BCEL)). The false claim of 'qualified' status may lead to a maximum of €800,000 of criminal penalties.

Law stated - 21 November 2022

What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

In theory, the BDPA has the ability to impose administrative fines up to the higher of €10 million or 2 per cent of the

total worldwide annual turnover for failure to comply with the rules on reporting threats and breaches in relation to personal data (including failures from the telecommunication sector).

Furthermore, failure of DSPs and OESs to comply with notification obligations may amount to a fine of between €500 and €75,000 or even to criminal penalties up to €160,000. Fines are doubled for recidivists. NIS2 however provides that when essential and important entities do not comply with the reporting obligations, they shall be subject to fines of a maximum of at least €10 million or 2 per cent of the total worldwide annual turnover.

Moreover, PSPs may receive administrative fines of between €10,000 and 10 per cent of their yearly net turnover (based on their previous accounting year) or penalty fines of maximum €2.5 million per infringement of PSD2 (or both) or a maximum of €50,000 per (further) day of non-compliance.

Finally, (non-qualified) TSPs may lose their ability to provide (non-)qualified trust services. The service provider losing 'qualified' status must inform the users of its services about it (article XV.26, BCEL). The false claim of a 'qualified' status may lead to a maximum of €800,000 of criminal penalties.

Law stated - 21 November 2022

How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Parties may seek private redress in front of the courts against individuals (article 1382, Belgian Civil Code) or organisations (article 82, GDPR) to receive damages, provided demonstration of a 'fault' (eg, negligence) by the individual or the infringement of the GDPR by the organisation; the prejudice suffered by the parties; and the causal link between the aforementioned fault or infringement and prejudice.

Also, more and more organisations acquire the necessary status to initiate class actions to claim for collective redress (articles XVII.36 and XVII.39, BCEL). For instance, the privacy activism organisation NOYB has acquired this right in Belgium.

Law stated - 21 November 2022

THREAT DETECTION AND REPORTING

Policies and procedures

What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Few laws require specific policies or procedures, and even fewer currently require specific measures. Typically, the rule is that the organisation itself must decide what is appropriate – and that can then be challenged by the regulator.

The combination of various data protection principles (including the principles of 'data protection by design' and 'data protection by default') can be viewed as requiring companies to implement procedures to take cybersecurity into account in relation to personal data at every stage of the life cycle of a data-related initiative. For instance, security is an important element to take into account when carrying out a 'data protection impact assessment' when their processing activity poses a high risk to the rights and freedoms of natural persons (article 35, General Data Protection Regulation (GDPR)).

The Belgian Data Protection Authority's (BDPA) predecessor, the Belgian Privacy Commission, had issued more specific guidelines on information security (on the need to have access controls (permissions; authentication) in place, on the importance of a security policy, etc), but those are no longer available. Instead, the BDPA's case law suggests specific measures that are required (eg, having secure sockets layer (SSL) for web forms involving the processing of health-

related data, and logging mechanisms and access control for managers as well).

Some sector-specific laws go further. For instance, qualified trust service providers (TSPs) must train their staff and subcontractors about security and must use trustworthy systems (article 24(2), electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)). Qualified electronic signature creation devices must be subject to certification that involves a security assessment (article 30, eIDAS Regulation). Moreover, the whole process for validating qualified electronic signatures must allow the person requesting validation to detect 'any security relevant issues' (article 32, eIDAS Regulation).

In the Belgian Act of 7 April 2019 (Belgian NIS Act) and critical infrastructure legislation, security policies are required, but the content remains at the discretion of the organisation (although ISO/IEC 27001 certification is evidence of compliance with this requirement, according to the Belgian NIS Act). Nevertheless, the NIS2 Directive includes a list of seven elements that all companies must address or implement as part of the security measures they take, including risk analysis and information system security policies, incident response, business continuity and crisis management, supply chain security, assessment of effectiveness of risk management measures, and encryption and vulnerability disclosure.

Law stated - 21 November 2022

Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Under the GDPR, any controller must document any personal data breaches, including those not notified to an authority or data subject (article 33(5), GDPR). There is no guidance about the specifics of collecting or storing those records, but the BDPA has started to request ever more frequently a copy of such registers of breaches.

In terms of duration, data protection infringements are time-barred after five years in Belgium, as a result of which it is likely organisations will wish to keep such records for at least five years. Other statutes of limitation might however also be relevant, so that it is important to take all limitation periods into account when deciding on the retention period for such records.

Under the Digital Operational Resilience Act (DORA), financial entities shall also record all ICT-related incidents as part of their ICT Business Continuity Policy (article 10 DORA).

Law stated - 21 November 2022

Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Controllers must notify to the BDPA cybersecurity breaches that are likely to result in a risk to the rights and freedoms of natural persons. Such notification must contain the nature of the breach, the person to contact to obtain further information, a description of the likely consequences and the measures (proposed to be) taken to mitigate the adverse effects of the breach.

When there is a risk of breach of the network security, publicly available electronic communications services (ECSPs) must notify such risk to the Belgian Institute for Postal Services and Telecommunications (BIPT). The notification must contain, if the risk cannot be fully mitigated by the ECSP, the measures allowing such mitigation and an indication of their likely cost. If there is a personal data breach, the ECSPs must notify it to the BDPA. Therein, the ECSP must include their identity and their person of contact; the nature of the breach and the incident that caused it; the scope of the breach; the potential consequences for individuals; and the technical and organisational measures (to be) applied.

In the case of a specific and significant threat of a cybersecurity incident, ECSPs must inform the BIPT thereof and

must indicate any protective or remedial action that its users should take and any measures it has taken or plans to take (article 107/3, Belgian Act of 13 June 2005 (BAEC)).

Under the NIS Directive, operators of essential services (OESs), digital service providers (DSPs) and financial services operators (FSOs) must notify incidents having a significant impact on the availability, confidentiality, integrity or authenticity of network and information systems used by the essential service (article 24, Belgian NIS Act). OESs must notify incidents simultaneously to the national CSIRT, the sector-specific authority or sector CSIRT and the national authority for identification of operators of essential services. FSOs must notify breaches to the National Bank of Belgium (article 25, Belgian NIS Act and 96 of the Payment Services Directive Two (PSD2)). These notification obligations apply even if there is not enough information for the determination of the notion of a 'significant impact'. The NIS2 directive, which has a broader scope than NIS1, introduces a new two-stage approach to incident reporting, according to which companies affected by a breach must submit an initial report within 24 hours from when they first become aware of an incident, followed by a final report within one month.

Payment service providers (PSPs) must notify any major operational or security incident to payment service users if the incident may have or has an impact on their financial interests (article 96, PSD2).

TSPs must notify to the BDPA any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein to their customers if it is likely to adversely affect them, without undue delay (article 19 eIDAS).

Law stated - 21 November 2022

Time frames

What is the timeline for reporting to the authorities?

Controllers must notify personal data breaches to the BDPA 'where feasible, not later than 72 hours after having become aware of it'. Justification is required if this timeline is exceeded.

When a security breach occurs, or when the loss of the integrity of personal data entails a significant impact on the functioning of network and services, public electronic communications networks and ECSPs must notify such breach or loss to the BIPT without delay. If a personal data breach occurs, ECSPs must notify it to the BDPA without delay (article 107/3, BAEC).

OESs and DSPs must notify incidents without delay (article 35, Belgian NIS Act). Under NIS2, companies affected by a breach must submit an initial report within 24 hours from when they first become aware of an incident, followed by a final report within one month.

PSPs must notify any major operational or security incident without undue delay (articles 53(2) and 96 PSD2). According to the guidelines of the EBA, there must be an initial report of the major incident within four hours of the first detection followed by reports every three business days at the latest. The final report must be made a maximum of two weeks after the situation is back to normal.

Under DORA, financial entities will have to notify the competent authority about major ICT-related incidents without undue delay and in any case before the end of the business day, provide an intermediate report no later than a week after the notification and a final report within a month (article 17 DORA).

Notifications by TSPs must be made without undue delay, but in any event within 24 hours of having become aware of the relevant incident (article 19, eIDAS).

Law stated - 21 November 2022

Reporting

Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Controllers must notify personal data breaches to the person whose data they process (data subject) if such breach is likely to result in a high risk to the data subject's rights and freedoms. If no contact with individuals is possible, a public communication is required.

Organisations that process personal data on behalf of a controller ('processors' within the GDPR) must communicate personal data breaches to controllers 'without undue delay'. The parties are free to decide how the communication takes place.

ECSPs must notify a personal data breach to individuals when such breach is likely to adversely affect their data or privacy, unless technological protection measures rendered the data unintelligible to anyone not authorised to access it. In addition, in the case of a specific and significant threat of a cybersecurity incident, the ECSP must inform any users that are potentially affected by such an incident.

DSPs providing services to OESs must inform them of any incident with a significant impact on the continuity of those essential services (article 27, Belgian NIS Act). The European Union Agency for Cybersecurity (ENISA) has published a report to help determine if the incident has a significant impact.

PSPs must notify any major operational or security incident to payment service users if the incident may have or has an impact on their financial interests (article 96, PSD2).

TSPs must notify any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein to their customers if it is likely to adversely affect them, without undue delay. The supervisory authority may also require TSPs to issue a public communication (article 19, eIDAS).

Law stated - 21 November 2022

UPDATE AND TRENDS

Recent developments and future changes

What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

The principal challenges are the development of useful, effective and realistic regulations. The government often only consults members of the academic world, which leads to regulations that are difficult to implement from a practical and business point of view. Nevertheless, we expect that the importance of the topic will naturally lead many companies to seek greater interaction with legislators and be more vocal, including about the possibilities, priorities and necessities of investment in cybersecurity.

Current developments are in any case promising:

- The Cybersecurity Strategy 2.0, which aims to ensure that Belgium becomes one of the least vulnerable countries in Europe in the cybersecurity area by 2025. This strategy sets out several strategic objectives that the Center for Cybersecurity Belgium (CCB) intends to pursue in co-operation with all relevant stakeholders in the cybersecurity sector in the upcoming years. Its objectives include:
  - strengthening and increasing trust in the digital environment. For example improve network infrastructure

security by adopting more secure internet standards (DNS security, secure routing, encryption, etc). These standards would provide a safe way to exchange data, namely, a 'safe data transport layer'. Another suggestion is the establishment of a Cyber Green House, an innovation center that aims to evaluate breakthrough cyber solutions and business models in a risk-free environment while disseminating Cybersecurity Guidelines and Best Practices;

- arming users and administrators of computers and networks;
- protecting organisations of vital interest from all cyber threats;
- responding effectively to cyber threats;
- improving public, private and academic collaborations; and
- participating in international commitments.

- The establishment of a Certification framework, which allows companies to demonstrate the implementation within their organisation of basic cybersecurity requirements, best practices and policies and earn a certificate that is recognised in the European Union.
- The EU-led harmonisation to strengthen cybersecurity legislation, especially the NIS2 Directive and the Digital Operational Resilience Act (DORA).

* The author would like to thank Peter Craddock for his contribution to the chapter.

Law stated - 21 November 2022

LAW STATED DATE

Correct On

Give the date on which the information above is accurate.

21 November 2022

Law stated - 21 November 2022

Jurisdictions

Austria	MGLP Rechtsanwälte | Attorneys-at-Law
Belgium	NautaDutilh
China	Fangda Partners
European Union	Taylor Wessing
France	ADSTO
India	AZB & Partners
Italy	ICT Legal Consulting
Japan	TMI Associates
Netherlands	Eversheds Sutherland (International) LLP
Singapore	Drew & Napier LLC
Turkey	Paksoy
United Kingdom	Simmons & Simmons
USA	Ropes & Gray LLP