International
Comparative
Legal Guides

Practical cross-border insights into data protection law

Data Protection 2022

Ninth Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

Belgium

Sirius Legal

Bart Van den Brande

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

1.2 Is there any other general legislation that impacts data protection?

The law of 30 July 2018 on the protection of individuals with respect to the processing of personal data (the "**GDPR Framework Act**"), abolishes and replaces the 1992 Data Protection Act and the 2001 Royal Decree which implemented it and implements GDPR into Belgian law and addresses the introduction of substantial specifications and derogations, including the age of consent for children in an online context and providing specific legal grounds and imposing additional security measures in relation to sensitive data.

The law of 3 December 2017 on the establishment of the Data Protection Authority implements the requirements of the GDPR with respect to national supervisory authorities, and reforms the Belgian Commission for the Protection of Privacy. This law is currently already under review, following a series of formal investigations into the organisation and functioning of the Belgian Data Protection Authority and a proposal of the Law of 4 March 2021 to change the law of 3 December 2017 on the establishment of the Data Protection Authority is currently pending.

The law of 13 June 2005 on electronic communications implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy regulation (the "**ePrivacy Regulation**") that would harmonise the applicable rules across the EU Member States and replace the current ePrivacy Directive (and its implementing national legislation). Originally, the ePrivacy Regulation was intended to apply from 25 May 2018 together with the General Data Protection Regulation. Unlike with the GDPR, however, the EU states have not yet been able to agree on the draft legislation.

1.3 Is there any sector-specific legislation that impacts data protection?

Book XII of the Belgian Code of Economic Law, concerning certain legal aspects of information society services, provides specific rules on the use of personal data for electronic direct marketing purposes (including email, direct messaging, SMS and comparable technology).

Books VI and XIV of the Belgian Code of Economic Law, concerning market practices and consumer protection, provide a specific set of rules regarding the use of personal data for direct marketing purposes via telephone, fax and automatic calling machines without human intervention.

Article 129 of the law of 13 June 2005 on electronic communications provides specific rules on the use of cookies and trackers on websites and in apps and software tools.

The Belgian Camera Act of 21 March 2007 regulates the installation and use of surveillance cameras in publicly accessible buildings and locations.

The law of 3 August 2012 contains provisions relating to the processing of personal data carried out by the Federal Public Service Finance in the framework of the carrying out of its mission.

The Flemish Decree of 18 July 2008 provides a specific set of rules concerning the exchange of administrative data by regional authorities within the Flemish region.

As regards employee monitoring, Collective Bargaining Agreement No 68 on the use of cameras in the workplace and Collective Bargaining Agreement No 81 on the monitoring of electronic communications in the workplace are relevant.

On 8 October 2020, the Belgian legislator approved an Act prohibiting life and health insurers from processing health sensor data. The Belgian legislator intends to prevent insurers from providing discounts on the basis of health-sensor data, even if the insurers have their policy-holders' consent.

1.4 What authority(ies) are responsible for data protection?

The "Data Protection Authority" ("*Gegevensbeschermingsautoriteit*", in Dutch, "*Autorité de Protection de Données*" in French) is the federal data protection authority. It has full powers and competences as required under the GDPR.

On the region level, the "Flemish Supervisory Commission" ("*Vlaamse Toezichtscommissie*") is the supplementing data protection authority that supervises the application of the GDPR and national data protection laws by Flemish government agencies, public authorities and Flemish administrative bodies. The

Flemish Supervisory Commission can act independently and in parallel with the Data Protection Authority. Neither has exclusive authority. There are no similar authorities in the Walloon or Brussels-Capital region yet.

The "Controlling Body on Police Information" ("*Controleorgaan op de Politionale Informatie*" or "**COC**") is the competent data protection authority for all federal and local police forces.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural 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.
- "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**" means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**" are personal data, revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**" means 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.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step

to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
  Additionally, the data subject may request a copy of the personal data being processed.
- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "**right to be forgotten**") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.
- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right protecting against solely automated decision-making and profiling**
  Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects that concern (or similarly significantly affect) them. This right is restricted where the solely automated decision: (i) is necessary for entering into, or the performance of, a contract between the data subject and controller; (ii) is authorised by EU or Member State law to which the controller is subject (and which contains suitable measures to safeguard the data subject's rights); or (iii) is based on the data subject's explicit consent.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with (the data protection authority in your jurisdiction), if the data subjects live in (the name of your jurisdiction) or the alleged infringement occurred in (the name of your jurisdiction).
- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The Belgian law of 28 March 2014 installed a system of collective

redress ("class action"), that allows for consumers to search collective redress in matters of consumer protection. The law is subject to a number of restrictions that strongly limit its usability and success. One of the main restrictions lies in the fact that a non-profit organisation has to be appointed by Ministerial Decree as an agreed body to file collective redress proceedings. A September 2022 Ministerial Decree appointed privacy activist group NOYB as the first privacy and data protection-related qualified entity under the collective redress action scheme of the Belgian Code of Economic Law. This means that NOYB can now file representative actions in Belgium and claim damages on behalf of users of a company for the violation of various laws relating to consumer protection, including data protection legislation.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Where information society services are offered directly to a child under the age of 13, and the lawful basis of processing their personal data is consent, such consent must be obtained from or authorised by the individual with parental responsibility over the child. The controller must make reasonable efforts to verify that consent has been given, or authorised, by the holder of parental responsibility in light of available technology. There is no EU standard response on whether the national law of the relevant jurisdiction has lowered the minimum age for these purposes.

Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in a clear and plain language that the child can easily understand.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There no longer is a registration or notification obligation in Belgium since the entry into force of the GDPR on 25 May 2018.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in Belgium.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in Belgium.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in Belgium.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in Belgium.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable in Belgium.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Belgium.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Belgium.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable in Belgium.

7.10 Can the registration/notification be completed online?

This is not applicable in Belgium.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in Belgium.

7.12 How long does a typical registration/notification process take?

This is not applicable in Belgium.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer ("**DPO**") for controllers or processors is only mandatory in some

circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

In addition, the appointment of a DPO is required for all processors processing data on behalf of the federal government.

It is highly recommended to any business processing personal data to voluntarily appoint a Privacy Officer or a Privacy Team, without formally appointing a DPO. Designating a DPO voluntarily is also possible, although in that case the requirements of the GDPR apply as though the appointment were mandatory.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a DPO is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed DPO should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single DPO is permitted by a group of undertakings provided that the DPO is easily accessible from each establishment. In case possible conflicts of interest might arise between group entities, it is highly recommended to appoint separate and independent DPOs.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge. At present, there are no official degrees required to qualify as a DPO.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A DPO should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority/authorities of the contact details of the designated DPO.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The DPO does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the DPO must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "**WP29**") (now the European Data Protection Board (the "**EDPB**")) recommended in its 2017 guidance on DPOs that both the data protection authority and employees should be notified of the name and contact details of the DPO.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Electronic direct marketing requires the recipient's prior,

explicit and free consent. This goes for both business-to-consumer ("**B2C**") and business-to-business ("**B2B**") relationships. The consent does not have to be obtained through a so-called "double opt-in", although for documentation and evidence reasons, such can be advisable.

There are two exceptions to this rule. Electronic direct marketing is allowed without opt-in if the recipient is an existing client and if the marketing is for similar goods or services as those bought priorly. Electronic direct marketing is also allowed if the recipient e-mail address is a strictly non-personal email address that does not relate to an individually identifiable person (e.g., info@ or sales@).

All electronic direct marketing should at all times contain an easily accessible opt-out link.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The restrictions apply to B2C marketing as well as in a B2B context.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Telemarketing is subject to an opt-out regime, based on a national "Do-Not-Call-Me" register that is managed by the Belgian marketing sector. Any telemarketing initiative requires the prior consultation of the Do-Not-Call-Me register and any phone number, both business and personal and both fixed and mobile, listed in the register cannot be used for telemarketing purposes.

Classic paper direct marketing does not require the prior consent of the addressee, but is subject to an opt-out regime based on a national opt-out register "Robinson List") managed by the Belgian Association for Marketing BAM. The Robinson List opt-out regime is not mandatory and is a voluntary regime by the Belgian marketing sector.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the restrictions noted above apply to marketing sent from other jurisdictions.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Belgian Data Protection Authority has the right to carry out investigations and enforce any breaches of GDPR in a marketing context. The Economic Inspection (which operates under the Federal Public Service Economic Affairs) enforces any violations of consumer protection rules and specific direct marketing rules that follow from Books VI, XII and XIV of the Code of Economic Law. Both authorities have complementing activities in enforcement of breaches of marketing restrictions.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes. Buying, leasing or renting data from third parties such as data brokers is legal, provided that all applicable obligations under the GDPR are met, including lawful basis, compliance with the opt-in and opt-out rules, transparency, purpose limitation, accuracy, security and confidentiality.

Businesses should ensure appropriate legal guarantees from the provider of commercial data to ensure that the data have been gathered and processed in compliance with the GDPR, that prior consent has been obtained where needed and transparency obligations were respected.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Based on a breach of Books VI, XII and XIV of the Code of Economic Law, in case of proceedings before Belgian criminal courts, the maximum penalty for sending marketing communications in breach of applicable restrictions is a criminal fine of EUR 10,000. This amount is to be multiplied by eight in accordance with the law on criminal surcharges. Based on a breach of GDPR, in case of proceedings before the Belgian Data Protection Authority, the maximum penalty is the higher of EUR 20,000,000 or 4% of worldwide turnover.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The law of 13 June 2005 on electronic communications implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies and other tracking technology, including for instance pixels, server side tracking, html5 request, … on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (i.e., a service provided over the internet) requested by the subscriber or user, which means that it must be essential to fulfil the user's request.

The use of cookies or other tracking technology is only authorised if the person has had, before any use of cookies, clear and precise information concerning the purpose of the processing and his/her rights. The controller must also freely give the opportunity to the subscriber or users to withdraw their consent at any time. Information must also be provided with respect to the term of validity of the cookies used.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Applicable restrictions do not distinguish between session cookies and permanent cookies or first-party and third-party cookies. Prior consent is always required for the use of all cookies, with the sole exception of cookies that are strictly necessary to provide the requested service (i.e. in most cases access to a website).

Contrary to a number of other jurisdictions, statistical or analytics cookies are considered to be not strictly necessary and therefore always require prior consent.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes, they have.

The Data Protection Authority took aim at Facebook in connection with the use of cookies for the purposes of tracking internet users and instituted proceedings against Facebook in connection therewith. By a decision dated 16 February 2018, Facebook was condemned by the Brussels Court of First Instance for having tracked an internet user without them either knowing or consenting. The court issued a fine of EUR 250,000 per day with a maximum fine of EUR 100,000,000.

In 2019, the Belgian Data Protection Authority imposed an administrative fine of EUR 15,000 on a company that manages a website with legal news and information, as the company did not comply with the provisions of the GDPR and the provisions of the ePrivacy Directive.

In 2021, a local tourism board received a warning for the non-compliant use of cookies on their website.

In 2022, IAB Europe was fined EUR 250,000 and imposed upon a number of remedies under constraint for breaches of cookie regulations in the context of IAB Europe's "Transparency and Consent Framework TCF 2.0". The appeal is pending.

In 2022, the websites of several Belgian media outlets were investigated simultaneously. A number of breaches were identified and warnings were issued. One specific media outlet was fined EUR 50,000.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The law of 13 June 2005 on electronic communications does not contain any specific sanctions linked to the breach of the applicable cookie restrictions. To the extent the breach also constitutes a breach of the applicable data protection laws (which is in practice almost always the case), the controller can be sanctioned with fines applicable for breaches of the data protection laws, including those under GPDR.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the "**EEA**") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer.

The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Under the GDPR, transfers are only allowed to countries that provide an adequate level of protection, or under one of the other provisions of Chapter 5 of the GDPR.

The EU Commission has compiled a list of third countries that are deemed to offer an adequate level of protection to EU personal data. This list contains a limited number of countries, including amongst others Argentina, Canada, Japan, Israel, South Korea and Switzerland.

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules ("**BCRs**").

Following the *Schrems II* decision of the European Court of Justice, the transfer of personal data to the USA is no longer possible based on the former EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US. All EU-US data transfers now require a new legal basis (SCCs, BCRs or other), combined with a prior risk assessment and the implementation of additional measure to ensure data privacy.

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between: (i) controllers; (ii) processors; (iii) a controller (as exporter) and a processor (as importer); and (iv) a processor (as exporter) and a controller (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. BCRs will always need approval from the relevant data protection authority. Most importantly, BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

When personal data is transferred to an Adequate Jurisdiction or using Standard Contractual Clauses, prior approval from the relevant data protection authority is not required.

On the contrary, international data transfers based upon BCRs, bespoke contractual clauses, codes of conduct or certification mechanisms require prior approval from the relevant data protection authority.

12.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

A single (brief) guidance of the Belgian Data Protection Authority summarises the conclusions of the Court of Justice, advises companies to consult the FAQ published by the EDPB and explains that the Belgian Data Protection Authority is investigating the consequences of *Schrems II* but has so far not published any additional guidance.

The Vlaamse Toezichtcommissie VTC issued guidance VTC/A/2020/05, containing a matrix with possible scenarios and guidance on the use of non-EU-based cloud providers in each of these scenarios.

The EDPB issued several opinions and guidelines on data transfers, including Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Guidelines 04/2021 on Codes of Conduct as tools for transfers.

12.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses published on 4 June 2021?

No guidance has been published by the Belgian Data Protection Authority/Authorities in this respect.

The new Standard Contractual Clauses published by the European Commission on 4 June 2021 (the "**2021 SCCs**") replace the Standard Contractual Clauses adopted under the Data Protection Directive (the "**2010 SCCs**"). Until 27 December 2022, controllers and processors can continue to rely on the 2010 SCCs for contracts that were concluded before 27 September 2021.

For contracts concluded after 27 September 2021, the 2021 SCCs must be incorporated.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistleblowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistleblowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistleblowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

A 2007 recommendation by the former Commission for the Protection of Privacy provides guidance to organisations on how to implement and operate whistleblowing schemes in accordance with data protection law. It was largely inspired by the WP29 Opinion 1/2006 and remains valid today, even though the former Commission for the Protection of Privacy has meanwhile been replaced with the Belgian Data Protection Authority.

Since 2019, the Directive (EU) 2019/1937 applies to both the private and public sectors and applies to anyone who reports or discloses information obtained concerning breaches in their professional context, regardless of their rank or working statute.

The Directive covers breaches in financial services and markets, money laundering, public procurement, transport safety, protection of the environment, consumer protection, public health, protection of privacy and personal data, as well as breaches relating to the internal market.

The implementation deadline was set on 17 December 2021, but Belgium has not managed to implement the Directive into Belgian law yet. A first draft of proposal is currently being discussed within the government. At present, the only whistleblower legislation already in place, covers the banking and insurance sectors and certain public bodies.

It is not yet clear whether, and if so to what extent, Belgium will provide more protective rules.

However, since the 17 December 2021 implementation date has passed, the Directive has direct effect in Belgium awaiting the future Belgian law.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistleblower scheme.

An individual who intends to report to a whistleblowing system should be aware that he/she will not suffer due to his/her action. The whistleblower, at the time of establishing the first contact with the scheme, should be informed that his/her

identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistleblowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The Belgian Camera Act requires prior notification of any surveillance cameras in publicly accessible private buildings or places. Notification should be made to the local police through a website set up specifically for that purpose. A number of requirements should be met before starting the use of CCTV security cameras. Amongst others a registry of processing activities is required (independently from the data registers under GDPR), warning signs should warn visitors for the use of cameras at all entrances and in certain cases approval by employee representation is required. Retention of CCTV images is limited to 60 days and no images of public areas (streets and sidewalks, etc.) can be made.

According to the Police Service Act, installing CCTV in public areas (public streets and squares) is only permitted after positive advice from the city council and local police.

A data protection impact assessment ("**DPIA**") must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

14.2 Are there limits on the purposes for which CCTV data may be used?

The use of CCTV for surveillance purposes is limited to preventing, recording or detecting of offences, preventing, recording or detecting disturbances or maintaining public order.

CCTV can only be used in the workplace for health and safety reasons, protection of company property, surveillance of the production process, monitoring of the work of employees. All purposes have to be defined and notified to the employees in advance and any use for non-notified purposes are forbidden.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Collective Bargaining Agreement nr. 68 on the use of CCTV in the workplace and Collective Bargaining Agreement nr. 81 on the monitoring of electronic communications in the workplace determine the types of employee monitoring that are permitted:

- Monitoring of working hours through a time registration system, but only after prior information of the employees.
- Consultation of employees' electronic agenda if such is absolutely necessary for proper functioning of the business.
- Systematic monitoring of professional telephone conversations for quality monitoring purposes only and subject to prior information of the employee.
- There is discussion on the accessing of, even professional, e-mails by the employer in the absence of the employee, even if access is taken in order to ensure the continuity of service and employers are advised to have strong internal privacy policies and e-mail use policies that ensure GDPR compliance at all times in relation to their employees.
- Monitoring (without accessing and reading) electronic communications in the workplace is permitted to the extent the data protection laws and Collective Bargaining Agreement nr. 81 are complied with.
- The use of geo-localisation data is in principle permitted, but only in case of absolute necessity and under strict conditions.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent is not required. It would most likely be considered invalid, since the imbalance of power between employer and employee implies that consent in most cases cannot be freely given, taking into account the imbalance of power between the employer and the employee.

Appropriate legal basis usually counts as legitimate interest. Employees should be notified in advance through an "employee privacy policy" and an internal privacy awareness programme.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Following Collective Bargaining Agreement nr. 68 on the protection of privacy of workers with regard to CCTV in the workplace and Collective Bargaining Agreement nr. 81 concerning the protection of workers' private lives in respect of the monitoring of electronic communications in the workplace, the Council of Employees or, in the absence of a Council of Employees, the Committee for Health and Safety or the employee representatives, must be informed prior to any use of CCTV in the workplace and the monitoring of electronic communications in the workplace. They should be informed of the use of CCTV in itself, the location of CCTV cameras and the areas that will be filmed as well as the purposes for which the images will be used.

15.4 Are employers entitled to process information on an employee's COVID-19 vaccination status?

A person's vaccination status is considered health data under

article 9 GDPR. Health data is particularly sensitive and may therefore only be processed in a very limited number of cases and only on the basis of a legal provision that allows it. Systematic processing of vaccination status by employers is not allowed. In Decision 143/2021 the Belgian Data Protection Authority ordered a hospital group to immediately suspend the monitoring of applicants' vaccination status on this exact argument.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; an ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisation measures for ensuring the security of processing.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

16.4 What are the maximum penalties for data security breaches?

Maximum penalty is the higher of €20 million or 4% of worldwide turnover.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Investigative Powers**: The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out a review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data including any data processing equipment. No criminal sanctions apply.

(b) **Corrective Powers**: The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below). No criminal sanctions apply.

(c) **Authorisation and Advisory Powers**: The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR. No criminal sanctions apply.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The GDPR provides for administrative fines which can be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year. No criminal sanctions apply.

(e) **Non-compliance with a data protection authority**: The GDPR provides for administrative fines which will be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher. No criminal sanctions apply.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

The law of 3 December 2017 on the establishment of the Data Protection Authority allows the Inspection Chamber of the Data Protection Authority to order injunctive measures, such as the suspension, limitation or freezing of the processing under review. The Litigation Chamber can subsequently order the temporary or definitive freezing, restriction or prohibition of the processing.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Suspending or prohibiting specific processing activities is standard part of the Data Protection Authorities procedures and decisions.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The Data Protection Authority does act against businesses established outside of Belgium. By way of example we cite the Brussels Court of First Instance case against Facebook, including Facebook Ireland Limited and Facebook Inc., on the initiative of the Belgian Data Protection Authority, for the tracking of internet users without consent nor transparency. The court ordered Facebook to cease of the unlawful processing, under the penalty of a fine of EUR 250,000 per day with a maximum of EUR 100,000,000.

18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

If e-discovery requests or requests for disclosure from foreign law enforcement agencies require a transfer of personal data to non-EEA countries not offering adequate protection of personal data, businesses typically either agree if possible on appropriate safeguards with the recipient, obtain explicit consent from the data subjects, anonymise data, and/or provide a legal opinion to confirm that the disclosure and transfer is not permitted under applicable data protection laws.

18.2 What guidance has/have the data protection authority(ies) issued?

The Belgian Data Protection Authority has not issued any specific opinions on the subject, but has referenced WP29 opinion 1/2009 on the matter in the past.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The number of decisions by the Data Protection Authority's Litigation Chamber is at a steady rise, after a somewhat slow start between 2018 and 2020. The sanctions imposed are diverse, as are the subject matters involved.

Recent relevant cases include:

- The IAB TCF case, in which IAB Europe was fined for non-compliance with GDPR and cookie regulations in the use of the IAB TCF Framework for targeted advertising. The appeal is currently pending.
- Belgian telecoms operator Proximus was fined EUR 50,000 for appointing a Data Protection Officer that did not meet the criteria of independence.
- Several Belgian media outlets were investigated and one was fined EUR 50,000 for non-respect of cookie regulations.
- Local authorities were fined for the use of CCTV cameras in tourist areas to monitor visitor flows and crowd control during periods when COVID-19 was particularly rampant.

19.2 What "hot topics" are currently a focus for the data protection regulator?

In its 2019–2025 Strategic Plan, the Belgian Data Protection Authority indicated that it will focus its actions on the following aspects of the GDPR:

- the role of the data protection officer, with a particular focus on companies that have appointed a data protection officer without allowing them to act in accordance with the GDPR;
- the lawfulness of data processing activities, and more particularly the (abusive) processing of personal data based on the legitimate interests legal basis; and
- data subjects' rights, specifically the scope of some of these rights.

The Data Protection Authority also has a number of social issues high on its agenda, such as photos and cameras, data protection online and sensitive data.

In practice, we also see numerous decisions on direct marketing, the use of cookies and lack of respect for basic principles and data subject rights.

Bart Van den Brande has been a member of the Dutch-speaking Brussels Bar Association since 2001.
Bart has worked at several well-known Brussels law firms and has built extensive expertise in media and advertisement law, market practices and consumer protection, intellectual property, internet and e-commerce, privacy and data protection, IT, software development and gambling law.
Parallel to his law practice, Bart was a part-time teaching assistant at Brussels University VUB between 2005 and 2013. He is the author of several articles, is an experienced speaker in seminars and for training courses, and is regularly asked to comment on current legal events in the national media. Several court cases handled by Bart were later published.

Sirius Legal
Spaces Court of Justice
Wolstraat 68/72
1000 Brussels
Belgium

Tel: +32 2 721 13 00
Fax: +32 2 725 13 01
Email: bart@siriuslegal.be
URL: www.siriuslegal.be

Sirius Legal is a boutique law firm with a multidisciplinary team of lawyers, marketing consultants and tech consultants, specialising in technology, the digital economy and data protection. We serve a very diverse clientele, ranging from start-ups over a successful SME to multinationals.
At Sirius Legal, we do not just follow legal evolutions, we are an active part of legal change. Through blogs, white papers, webinars and training sessions, we share our years of accumulated knowledge and keep our clients informed of all the latest legal developments. We play a very active role in sector organisations and engage actively in lobbying activities on behalf of our partners. In other words, we make sure our voice as well as our partner's voice is heard in the legal debate. We keep a close eye on technological trends and developments and assess the legal impact of any new technology for our clients long before others do. We prepare our clients for the future with tailor-made no-nonsense advice, just as it should be.

www.siriuslegal.be

SIRIUS.LEGAL
BUSINESS LAW FIRM

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group