International
Comparative
Legal Guides

Data Protection 2021

A practical cross-border insight into data protection law

Eighth Edition

Featuring contributions from:

Anderson Mōri & Tomotsune
Arthur Cox LLP
Chandler MHM Limited
CO:PLAY Advokatpartnerselskab
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
FABIAN PRIVACY LEGAL GmbH
Foucaud Tchekhoff Pochet et Associés (FTPA)
H & A Partners
in association with Anderson Mōri & Tomotsune
Hajji & Associés
Hammad and Al-Mehdar Law Firm
Homburger
Iriarte & Asociados
Khaitan & Co LLP
King & Wood Mallesons
Klochenko & Partners Attorneys at Law
Koushos Korfiotis Papacharalambous LLC
Law Firm Pirc Musar & Lemut Strle Ltd
Lee and Li, Attorneys At Law
Leśniewski Borkiewicz & Partners
LPS L@W
LYDIAN
McMillan LLP
MinterEllison
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
Nikolinakos & Partners Law Firm
OLIVARES
Pinheiro Neto Advogados
PLANIT // LEGAL
S. U. Khan Associates Corporate & Legal Consultants
SEOR Law Firm
White & Case LLP
Wikborg Rein Advokatfirma AS

ICLG.com

ISBN 978-1-83918-127-6
ISSN 2054-3786

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Data Protection 2021

Eighth Edition

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

Expert Analysis Chapters

1 **The Rapid Evolution of Data Protection Laws**
Dr. Detlev Gabel & Tim Hickman, White & Case LLP

7 **Privacy By Design as a Fundamental Requirement for the Processing of Personal Data**
Daniela Fábián Masoch, FABIAN PRIVACY LEGAL GmbH

12 **Initiatives to Boost Data Business in Japan**
Takashi Nakazaki, Anderson Mōri & Tomotsune

Q&A Chapters

19 **Australia**
MinterEllison: Anthony Borgese

32 **Belgium**
LYDIAN: Bastiaan Bruyndonckx, Olivia Santantonio & Liese Kuyken

44 **Brazil**
Pinheiro Neto Advogados: Larissa Galimberti, Carla Rapé Nascimento & Luiza Fonseca de Araujo

56 **Canada**
McMillan LLP: Lyndsay A. Wasser & Kristen Pennington

68 **China**
King & Wood Mallesons: Susan Ning & Han Wu

82 **Cyprus**
Koushos Korfiotis Papacharalambous LLC: Loizos Papacharalambous & Anastasios Kareklas

96 **Denmark**
CO:PLAY Advokatpartnerselskab: Heidi Højmark Helveg & Niels Dahl-Nielsen

108 **France**
Foucaud Tchekhoff Pochet et Associés (FTPA): Boriana Guimberteau & Clémence Louvet

118 **Germany**
PLANIT // LEGAL: Dr. Bernhard Freund & Dr. Bernd Schmidt

129 **Greece**
Nikolinakos & Partners Law Firm: Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou & Alexis N. Spyropoulos

139 **India**
Khaitan & Co LLP: Harsh Walia & Supratim Chakraborty

149 **Indonesia**
H & A Partners in association with Anderson Mōri & Tomotsune: Steffen Hadi, Sianti Candra & Dimas Andri Himawan

161 **Ireland**
Arthur Cox LLP: Colin Rooney & Aoife Coll

172 **Isle of Man**
DQ Advocates Limited: Kathryn Sharman & Sinead O'Connor

182 **Israel**
Naschitz, Brandes, Amir & Co., Advocates: Dalit Ben-Israel & Efrat Artzi

193 **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi & Masaki Yukawa

205 **Korea**
D'LIGHT Law Group: Iris Hyejin Hwang & Hye In Lee

215 **Mexico**
OLIVARES: Abraham Diaz Arceo & Gustavo Alcocer

224 **Morocco**
Hajji & Associés: Ayoub Berdai

234 **Norway**
Wikborg Rein Advokatfirma AS: Gry Hvidsten & Emily M. Weitzenboeck

246 **Pakistan**
S. U. Khan Associates Corporate & Legal Consultants: Saifullah Khan & Saeed Hasan Khan

254 **Peru**
Iriarte & Asociados: Erick Iriarte Ahón & Fátima Toche Vega

262 **Poland**
Leśniewski Borkiewicz & Partners: Grzegorz Leśniewski, Mateusz Borkiewicz & Jacek Cieśliński

274 **Russia**
Klochenko & Partners Attorneys at Law: Lilia Klochenko

284 **Saudi Arabia**
Hammad and Al-Mehdar Law Firm: Suhaib Hammad

Q&A Chapters Continued

293 **Senegal**
LPS L@W: Léon Patrice SARR

302 **Singapore**
Drew & Napier LLC: Lim Chong Kin

317 **Slovenia**
Law Firm Pirc Musar & Lemut Strle Ltd: Nataša Pirc Musar & Rosana Lemut Strle

328 **Switzerland**
Homburger: Dr. Gregor Bühler, Luca Dal Molin & Dr. Kirsten Wesiak-Schmidt

337 **Taiwan**
Lee and Li, Attorneys At Law: Ken-Ying Tseng & Sam Huang

347 **Thailand**
Chandler MHM Limited / Mori Hamada & Matsumoto: Pranat Laohapairoj & Atsushi Okada

355 **Turkey**
SEOR Law Firm: Okan Or & Ali Feyyaz Gül

365 **United Kingdom**
White & Case LLP: Tim Hickman & Joe Devine

376 **USA**
White & Case LLP: F. Paul Pittman & Kyle Levenberg

ICLG.com

Belgium


Bastiaan Bruyndonckx


Olivia Santantonio


Liese Kuyken

LYDIAN

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 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (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 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. The last draft was published on 5 January 2021.

In addition, the Belgian legislator has adopted secondary legislation pursuant to the GDPR.

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. As of 25 May 2018, the Belgian Commission for the Protection of Privacy carries the name "**Data Protection Authority**" and has the powers and competences that the GDPR requires national supervisory authorities to possess.

A second act, the law of 30 July 2018 on the protection of individuals with respect to the processing of personal data (the "**GDPR Implementation Act**"), addresses the national substantive aspects of the GDPR and introduces several specifications and derogations, such as determining 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. At the same time, it abolishes and replaces the 1992 Data Protection Act and the 2001 Royal Decree which implemented it.

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

Book XII of the Code of Economic Law, which deals with certain legal aspects of information society services, provides a specific set of rules regarding the use of personal data for direct marketing purposes via electronic post, which includes email, SMS and MMS. Books VI and XIV of the Code of Economic Law, which deal with 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.

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.

The Camera Act of 21 March 2007 regulates the installation and use of surveillance cameras.

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?

Since 25 May 2018, the former Commission for the Protection of Privacy carries the name "**Data Protection Authority**" and has the powers and competences that the GDPR requires national supervisory authorities to possess.

The "**Flemish Supervisory Commission**" was established by the Decree of 8 June 2018. As a supervisory authority, the Flemish Supervisory Commission is responsible for supervising the application of the GDPR by the Flemish administrative bodies. The competences of the Flemish Supervisory Commission are in addition, and without prejudice, to the competences of the Data Protection Authority. There are no similar authorities in the Walloon or Brussels-Capital region yet.

2 Definitions

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

- "**Personal Data**"
  This 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**"
  This 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**"
  This 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**"
  This means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**"
  This means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"
  These are personal data revealing racial or ethnic origin, 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**"
  This 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.
- *Other key definitions*
  "Personal Data relating to Criminal Convictions" are personal data relating to criminal convictions and offences or related security measures.

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).

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).
  It should be noted 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 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.
- **Proportionality**
  The processing of personal data must be balanced between the means used and the intended aim.
- **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 the 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 override 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 his/her consent, freely, 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, freely, at any time, and without justification, to the processing of personal data for the purpose of direct marketing, including profiling.
- **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, if the data subjects live in Belgium or the alleged infringement occurred in Belgium.
- **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. This is, in principle, proactively provided by the controller at the start of collecting personal data or when entering into contact for the first time with the data subject.

6 Registration Formalities and Prior Approval

6.1 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?

No, the obligation to notify the Data Protection Authority of any wholly or partially automated processing of personal data, which existed prior to the entry into force of the GDPR, has been abolished as of the entry into force of the GDPR on 25 May 2018.

6.2 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 our jurisdiction.

6.3 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 our jurisdiction.

6.4 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 our jurisdiction.

6.5 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 our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

Prior approval of the Data Protection Authority is required for transfers outside the European Economic Area (the "**EEA**") to a country not offering adequate protection of personal data and that are based upon (i) bespoke contractual safeguards rather than Standard Contractual Clauses approved by the EU Commission, (ii) Binding Corporate Rules, (iii) a code of conduct, or (iv) a certification mechanism.

6.10 Can the registration/notification be completed online?

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

7 Appointment of a Data Protection Officer

7.1 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 for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; (ii) large-scale processing of sensitive personal data; or (iii) processing carried out by a public authority or body, except in the exercise of judicial functions by courts.

The Belgian legislator has not adopted secondary legislation that renders the appointment of a Data Protection Officer mandatory in cases other than those described in the GDPR.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory. In order to avoid this, it is recommended to call such person a 'Privacy Manager' or 'Privacy Responsible', for instance.

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

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

7.3 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 Data Protection Officer should not be dismissed or penalised for performing his/her tasks and should report directly to the highest management level of the controller or processor.

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

A group of undertakings may appoint a single Data Protection

Officer provided that the Data Protection Officer is easily accessible from each establishment.

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

The Data Protection Officer should be appointed because 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.

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

The Data Protection Officer 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 Data Protection Authority's primary contact point for issues related to data processing.

7.7 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 of the contact details of the designated Data Protection Officer.

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

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer 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 Data Protection Officers that both the Data Protection Authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 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.

8.2 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, and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

9 Marketing

9.1 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?).

Direct marketing per electronic post (which includes email, SMS and MMS) is only authorised where the recipient specifically and freely consented to it (opt-in). However, there are two exceptions to this rule. Firstly, sending electronic direct marketing to legal entities using a non-personal email address (e.g., info@company.com) is allowed on an opt-out basis. Secondly, sending electronic direct marketing to existing customers about identical or similar products is also allowed on an opt-out basis, provided a number of strict conditions are met. It should be noted that, even when the recipient previously consented to the use of his/her electronic contact details for direct marketing purposes, he/she can at any time oppose the further use of his/her electronic contact details for direct marketing purposes.

9.2 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 business-to-consumer marketing as well as in a business-to-business context.

9.3 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.).

For marketing by telephone, a national opt-out register (the so-called "Do Not Call Me Robinson List") exists and businesses carrying out direct marketing by telephone are required to check this list in advance.

Direct marketing by post does not require the prior consent of the addressee but can be carried out on an opt-out basis. For direct marketing (on a personalised basis) by post, a national opt-out register has been put in place but is only mandatory for businesses that are members of the Belgian Direct Marketing Association (the "**BDMA**"). For non-personalised advertising by post, anyone can ask to be provided with "Stop-Pub" stickers to stick on his/her mailbox.

For marketing by fax or via automated calling machines without human intervention, the prior consent of the recipient is required (opt-in).

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

Yes, they do.

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

Under the GDPR, the Data Protection Authority will have the right to carry out investigations and enforce the GDPR, including by imposing administrative sanctions. Aside from the Data Protection Authority, the Economic Inspection (which is part of the Federal Public Service Economy) has powers to enforce the specific rules on direct marketing which form part of Books VI, XII and XIV of the Code of Economic Law. Both authorities are active in enforcement of breaches of marketing restrictions. Most investigations are, however, started on the basis of complaints filed by individuals.

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

Yes, provided that data protection legislation is complied with. This means, amongst others, that the collection and processing of the data must have been carried out in compliance with the principles of the GDPR (including lawful basis, compliance with the opt-in and opt-out rules, transparency, purpose limitation, accuracy, security and confidentiality).

Businesses are strongly advised to seek appropriate guarantees from the seller of marketing lists, including with respect to: (i) the fact that the data have been gathered and processed in compliance with the GDPR; (ii) the fact that the individuals whose data are included have consented to the use of their data for direct marketing purposes; and (iii) the fact that the transfer of the data is in accordance with the fair processing notices provided to the individuals and with the GDPR.

9.7 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 GPDR, 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.

10 Cookies

10.1 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 (or other data) 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 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.

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

The applicable restrictions indeed distinguish between different types of cookies. A distinction is made, amongst others, between session cookies (which have a time limit and are deleted after the browsing session) and permanent cookies (which are kept on the user's hard drive for an indefinite duration). Furthermore, a distinction is made between first-party cookies (which are placed by the website owner) and third-party cookies (which are placed by a third party, e.g., Facebook or Google). A distinction is also made between tracking cookies (which are used to collect data about the browsing behaviour of the user on various websites) and other cookies. In principle, the storage of cookies on an end user's device requires prior consent. This does not, however, apply to merely technical cookies and necessary cookies.

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

The Belgian Institute of Postal Services and Telecommunications (the "**BIPT/IBPT**") is in charge of monitoring compliance by businesses with the law of 13 June 2005 on electronic communications, together with the Data Protection Authority. In 2017, the Commission for the Protection of Privacy (being the predecessor of 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 addition, recently, 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.

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

There are no specific (criminal) sanctions linked to the breach of the applicable cookie restrictions as laid down in the law of 13 June 2005 on electronic communications. To the extent the breach also constitutes a breach of the applicable data protection laws (e.g., the obligation to inform the data subject of the processing of personal data), the controller could, however, be sanctioned with fines applicable for breaches of the data protection laws. Indeed, based on a breach of GPDR, 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 Restrictions on International Data Transfers

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

Data transfers to other jurisdictions that are not within 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.

11.2 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 such as Andorra, Argentina, Canada, Japan, and Switzerland. Since the recent *Schrems II* Decision of the Court of Justice, the United States no longer benefits from the Privacy Shield mechanism and is not considered a country offering adequate protection. On the other hand, the Court of Justice declared that examination of Decision 2010/87 on Standard Contractual Clauses ("**SCCs Decision**") in light of the Charter of Fundamental Rights (the "**Charter**") has disclosed nothing to affect the validity of that decision, but nevertheless questioned the Standard Contractual Clauses ("**SCCs**") validity for transfers to the US and other third countries.

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 SCCs or Binding Corporate Rules ("**BCRs**").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, transfers from controller to a processor or from a processor to a controller and transfers between processors. New sets of SCC have been published on 4 June 2021 by the EU Commission. Moreover, based on the *Schrems II* Decision, organisations needed to re-evaluate their data transfers to third countries if based on SCCs. Whether the SCCs are still a sufficient safeguard for transfers to certain third countries will require further examination. For instance, in the US, it is hard to see how the concerns raised by the CJEU regarding the Privacy Shield would not apply when the SCCs are at issue. 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. The BCRs will always need approval from the relevant data protection authority. Most importantly, the 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.

11.3 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.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs. 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.

11.4 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)?

The (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.

11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?

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

12 Whistle-blower Hotlines

12.1 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 whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing 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 whistle-blowing 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 whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing 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.

In 2007, the Commission for the Protection of Privacy also issued a recommendation on internal whistle-blowing schemes. The recommendation provides guidance to organisations on how to implement and operate whistle-blowing schemes in accordance with data protection law, and is largely inspired by the WP29 Opinion 1/2006 discussed above.

Moreover, the Directive (EU) 2019/1937 applies to both the private and public sectors and applies to anyone who reports or discloses the obtained information concerning breaches in a work-related context. (Ex-)employees, civil servants, consultants, (un)remunerated trainees, directors and shareholders are all protected when they report a breach in good faith.

The material scope of the Directive is wide. It concerns, *inter alia*, breaches on 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 national legislation can extend this scope with a view to ensuring that there is a comprehensive and coherent whistle-blower protection framework.

Belgium has to implement this directive in national legislation by 17 December 2021.

There is currently no legislation in place, except for the banking and insurance sectors and for certain public authorities or organisations. It is not yet clear whether, and if so to what extent, Belgium will provide more protective rules.

However, by 17 December 2021, all companies with 50 or more employees in the private sector and all public sector organisations must comply with the minimum obligations of the directive. For companies with 50 to 249 employees, a Member State can still provide an exception regarding the obligation to set up internal reporting channels: this obligation can be postponed until 17 December 2023.

12.2 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 whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, 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. Whistle-blowers 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.

13 CCTV

13.1 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)?

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.

The Belgian legislator introduced a new administrative obligation in the Surveillance Camera Act as well as in the Police Service Act with regard to recording the use of cameras. This register forms an extensive logbook about the use of the cameras. Moreover, according to current Belgian legislation on surveillance cameras, installing CCTV in public areas is only permitted after positive advice from the communal or city council and the

chief of police, which requires a safety investigation. In addition, when installing CCTV in public areas, the controller must inform the local chief of police.

When installing CCTV, a sign must be placed to warn individuals that the area is under CCTV surveillance and to inform them of the identity and contact details of the controller.

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

CCTV for surveillance purposes can only be installed and used for the following purposes: (i) to prevent, record or detect offences; (ii) to prevent, record or detect disturbances; or (iii) to maintain public order.

CCTV can only be used in the workplace for the following purposes: (i) health and safety; (ii) protection of company property; (iii) surveillance of the production process; or (iv) monitoring of the work of employees. The employer must clearly and explicitly define the purposes of the CCTV system installed in the workplace.

14 Employee Monitoring

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

According to, amongst others, Collective Bargaining Agreement N° 68 (on the use of CCTV in the workplace) and Collective Bargaining Agreement N° 81 (on the monitoring of electronic communications in the workplace):

- the employer may monitor the hours worked through the use of a time registration system, but only if the employee has been informed of this use beforehand;
- the employer may consult the electronic agenda of an employee if it is necessary for the proper conduct of the business and there are no other, less intrusive, means to obtain the information;
- the employer may systematically monitor the professional telephone conversations in order to monitor the quality of the service, depending on the employee's function; call centres must always inform their employees that the conversations may be recorded and listened to;
- emails of a professional nature may be accessed by the employer in the absence of the employee, in order to ensure the continuity of service, provided the employer complies with the data protection legislation; the employer must inform the employee beforehand that such access may happen and only look at the emails which seem to be related to ongoing cases and are related to the period in which the employee was absent without the correspondent knowing it;
- monitoring of electronic communications in the workplace is permitted to the extent the data protection laws and Collective Bargaining Agreement N° 81 are complied with;
- the use of geo-localisation is permitted under strict conditions and only if there is no other, less intrusive, manner to monitor the employees; the data should not be kept longer than necessary; if the employer wishes to conduct an in-depth investigation, he must inform the employee and provide him the opportunity to be heard; and
- monitoring of employees through CCTV installed in the workplace is permitted to the extent the data protection laws and Collective Bargaining Agreement N° 68 are complied with; the employer must clearly define the purposes of such monitoring, and if it is only to monitor the employees, the use of the CCTV must be temporary.

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

Consent is not required as it would not be freely given, taking into account the imbalance of power between the employer and the employee. Fair processing notices are always required. Employers usually inform the workers of the monitoring via the Work Regulations, via a specific policy or, when it is punctual, before the monitoring activity.

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

Pursuant to Collective Bargaining Agreement N° 68 on the protection of privacy of workers with regard to CCTV in the workplace and Collective Bargaining Agreement N° 81 concerning the protection of workers' private lives in respect of the monitoring of electronic communications in the workplace, the Works Council or, in the absence of a Works Council, the Committee for Health and Safety or the employee representatives, must be informed of the use of CCTV in the workplace and the monitoring of electronic communications in the workplace.

15 Data Security and Data Breach

15.1 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 organisational measures for ensuring the security of processing.

15.2 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.

15.3 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).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of EUR 20,000,000 or 4% of worldwide turnover.

16 Enforcement and Sanctions

16.1 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 reviews 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.

(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).

(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.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The GDPR provides for administrative fines which can be EUR 20,000,000 or up to 4% of the business's worldwide annual turnover of the proceeding financial year.

(e) **Non-compliance with a data protection authority**: The GDPR provides for administrative fines which will be EUR 20,000,000 or up to 4% of the business's worldwide annual turnover of the proceeding financial year, whichever is higher.

16.2 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. Pursuant to the law of 3 December 2017 on the establishment of the Data Protection Authority, the inspection chamber of the Data Protection Authority can order, by way of a temporary measure, the suspension, limitation or freezing of the processing under review, if the data concerned could cause damage which is serious, immediate and difficult to repair. The litigation chamber can order the temporary or definitive freezing, restriction or prohibition of the processing.

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

Before the law of 3 December 2017 on the establishment of the Data Protection Authority, the Commission for the Protection of Privacy did not have the power to issue a ban on a particular processing activity. However, it could institute proceedings against the controller before the regular courts and tribunals in order to obtain such a ban or transfer the matter to the Public Prosecutor for criminal proceedings against the controller. In 2017, the Commission for the Protection of Privacy instituted proceedings against Facebook before the Court of First Instance in Brussels. On 16 February 2018, the Brussels Court of First Instance condemned Facebook for having tracked internet users without their knowledge or consent, and ordered the ceasing of the unlawful processing under penalty of a fine of EUR 250,000 per day with a maximum of EUR 100,000,000.

On 2 April 2019, the Data Protection Authority issued a ban on processing activities that were infringing data protection laws, which could not be rectified. The case involved the placement of cameras in the common areas of student rooms. The placement of such cameras was to be disproportionate to the objective of combatting vandalism, damage and nuisance. In other cases, it was ordered that a processing operation shall be made compliant with the GDPR.

16.4 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 indeed exercise its powers against businesses established in other jurisdictions. On 16 February 2018, the Brussels Court of First Instance condemned Facebook, including Facebook Ireland Limited and Facebook Inc., for having tracked internet users without their knowledge or consent. The court ordered the ceasing of the unlawful processing under the penalty of a fine of EUR 250,000 per day with a maximum of EUR 100,000,000. The judgment has, however, been appealed by Facebook and the matter will now be heard by the Court of Appeals of Brussels. The latter referred the case for a ruling to the European Court of Justice (C-645/19). The case concerns questions on the lead supervisory authority and the cooperation between authorities in cross-border

GDPR cases. The Advocate General states that the supervisory authority in the Member State where a data controller or processor (in this case Facebook) has its main EU establishment (which is Ireland for Facebook) has a general competence to start court proceedings for GDPR infringements in relation to cross-border data processing. The Advocate General emphasised the one-stop-shop nature of a 'lead' supervisory authority in cross-border data processing cases – a contrary situation meaning the coherence of the whole system would be impacted. However, such lead supervisory authority cannot be the sole enforcer of the GDPR in cross-border cases, and ought to closely cooperate with other relevant supervisory authorities. Moreover, the Advocate-General does not exclude the possibility that other national supervisory authorities can also commence proceedings in their respective Member States, if the GDPR expressly allows them to do so, for example, where national supervisory authorities:

- act outside the material scope of the GDPR;
- investigate into cross-border data processing carried out by public authorities, in the public interest, in the exercise of official authority or by controllers not established in the Union;
- adopt urgent measures; or
- intervene following the lead supervisory authority having decided not to handle a case.

In its decision of 15 June 2021, the Court of Justice considers that the GDPR authorises, under certain conditions, a non-lead supervisory authority of a Member State to exercise its power to bring any alleged infringement of the GDPR before a court of that State and to initiate or engage in legal proceedings in relation to an instance of cross-border data processing.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

Where 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 (i) agree on appropriate safeguards with the recipient (if and to the extent possible), (ii) seek the explicit consent of the data subjects for the disclosure and transfer, (iii) limit the disclosure to anonymous data, and/or (iv) provide a legal opinion from a reputable law firm to confirm that the disclosure and transfer is not permitted under applicable data protection laws.

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

The WP29 has issued an Opinion 1/2009 on pre-trial discovery for cross-border litigation, which provides guidance to controllers subject to EU law in dealing with requests to transfer personal data to another jurisdiction for use in civil litigation. The Data Protection Authority has not issued any specific opinions on the subject, but has indicated (amongst others, in an opinion of 2008 on the SWIFT case) that it follows the opinion of the WP29.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The Data Protection Authority's Litigation Chamber already announced a substantial number of decisions. The sanctions imposed are diverse, as are the subject matters involved. The Belgian Data Protection Authority has most definitely shown its teeth in the last years as the Litigation Chamber issued multiple fines. The highest fine was imposed on Google (EUR 600,000), other fines vary between EUR 1,000–100,000 depending on the severity of the infringements as well as the so-called 'exemplary role' of the defendant.

The most notable decisions contain the following learnings for undertakings operating in Belgium:

- undertakings should take note that, when opting for an internal Data Protection Officer, his/her position should be carefully assessed, including whether there are possible conflicts of interests and incompatibilities such as for Compliance Officers;
- undertakings should be aware that a notification of a data breach might be a trigger for the Belgian Data Protection Authority to look for other possible infringements and may therefore give rise to an in-depth inspection by the Belgian Data Protection Authority's Inspection Service;
- as regards compliance with data subject's requests, controllers should only request proof of identity where reasonable doubt exists as to the identity of the person exercising the data subject right; and
- as regards surveillance cameras, it should be noted that controllers should (i) carefully consider the purposes of the use of surveillance cameras, (ii) consider whether the placing of surveillance cameras is proportionate to such purposes, (iii) notify the placement of surveillance cameras to the police, and (iv) ensure the related processing is mentioned in their records of processing activities.

  The Litigation Chamber was somewhat tempered in its enthusiasm to sanction non-compliance controllers and processors by the Brussels Market Court, as it has already reversed a number of decisions of the Litigation Chamber.

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

In the 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.

Bastiaan Bruyndonckx is a Partner in LYDIAN's Commercial & Litigation department and heads the Information & Communications Technology (ICT) practice as well as the Information Governance & Data Protection (Privacy) practice.
Bastiaan has a particular focus on information governance, privacy, data protection and cybersecurity and advises businesses on a broad range of industry sectors.
Bastiaan is a fellow of the Belgian American Educational Foundation (BAEF) and is a member of the International Association of Privacy Professionals (IAPP).
Bastiaan is a regular speaker at seminars, workshops and conferences on privacy and data protection. He also regularly publishes in international legal reviews such as Computerrecht, Privacy & Informatie, DataGuidance, Tijdschrift voor Privacy en Persoonsgegevens and Bulletin des Assurances. Bastiaan also contributed to the book *Data Protection – The Impact of the GDPR in Insurance* with a chapter regarding the new rules on consent and the processing of special categories of data under the GDPR.

LYDIAN
Avenue du Port 86C b113
1000 Brussels
Belgium

Tel: +32 2 787 90 93
Email: bastiaan.bruyndonckx@lydian.be
URL: www.lydian.be

Olivia Santantonio is counsel in LYDIAN's Information Governance & Data Protection (Privacy) practice and IP and ICT practice.
Olivia frequently advises on data protection issues regarding, *inter alia*, the obligations and liability of the data controller and data processor, the transfer of data into and out of the EU and the processing of sensitive data. She also frequently assists clients to assess their level of compliance with the new legislation, and assists them in case of data subject requests, data breaches or Data Protection Authority requests. She also specialises in global privacy issues (GDPR compliance, contracts review, etc.).
Olivia is a member of the International Association of Privacy Professionals (IAPP) and an active member of the International Association for the Protection of Intellectual Property (AIPPI).

LYDIAN
Avenue du Port 86C b113
1000 Brussels
Belgium

Tel: +32 2 787 90 07
Email: olivia.santantonio@lydian.be
URL: www.lydian.be

Liese Kuyken is an associate in Lydian's Information & Communications Technology (ICT), Information Governance & Data Protection (Privacy) and Intellectual Property practices.
She frequently assists clients in data protection matters regarding, for instance, data processing agreements, privacy and cookie policies, and data subject rights. Liese is involved in several procedures regarding the processing of personal data, before the Belgian Data Protection Authority as well as the Belgian courts. She teaches Media Law in the journalism programme at KU Leuven, where she educates students on issues such as privacy and image rights. Furthermore, Liese is a member of the International Association of Privacy Professionals (IAPP) and has published in the legal review *Tijdschrift voor Privacy en Persoonsgegevens*.

LYDIAN
Avenue du Port 86C b113
1000 Brussels
Belgium

Tel: +32 2 787 91 34
Email: liese.kuyken@lydian.be
URL: www.lydian.be

LYDIAN is a full-service Belgian business law firm with an Anglo-Saxon approach to practising law. Through a fine blend of transactional law expertise and litigation skills, we deliver straight to-the-point solutions that add true value.
Our Information Governance & Data Protection (Privacy) team represents clients, large and small, from all industry sectors (including technology, retail, telecommunications, healthcare and life sciences, media, energy, insurance, banks and other financial institutions, as well as printing and publishing industries), on all aspects of information governance and data protection.
Our range of services includes corporate privacy risk management, GDPR compliance, international data transfers, records management, e-discovery, (direct) marketing, e-commerce, cybersecurity and cybercrime.
We provide assistance to our clients, from legal advice to integrated consulting on corporate privacy risk management, as well as legislative strategic policy advice and legal compliance. We also litigate on behalf of clients in data protection-related matters.
We advise clients on global data protection and privacy compliance challenges, including by taking into account data protection and privacy rules on a global basis. We frequently advise clients on multi-jurisdictional data protection (privacy) compliance projects, either dealing with the local Belgian aspects or leading the project for our clients with the support of local correspondent firms advising on local law issues.
LYDIAN is one of the few independent law firms in Belgium operating outside a US/UK law firm banner. We are a popular referral choice for foreign firms seeking a high-quality law firm in Belgium with recognised skills in information governance and data protection, such as Hogan Lovells, Luther, Norton Rose Fulbright, Taylor Wessing and Willkie Farr & Gallagher.

www.lydian.be

LYDIAN

ICLG.com

Other 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
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

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group