ICLG

The International Comparative Legal Guide to:

Data Protection 2016

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bagus Enrico & Partners
Cuatrecasas, Gonçalves Pereira
Deloitte Albania Sh.p.k.
Dittmar & Indrenius
ECIJA ABOGADOS
Eversheds SA
Gilbert + Tobin
GRATA International Law Firm
Hamdan AlShamsi Lawyers & Legal Consultants
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Rossi Asociados
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

global legal group

global legal group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
April 2016

ISBN 978-1-910083-93-2
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Belgium

Wim Nauwelaerts

Hunton & Williams

David Dumont

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Act on the Protection of Privacy in Relation to the Processing of Personal Data of December 8, 1992 (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*) (the "Data Protection Act") (as amended) and the Royal Decree of February 13, 2001 implementing the Data Protection Act (the "Royal Decree").

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

The Electronic Communications Act of June 13, 2005 (*Wet betreffende de elektronische communicatie/Loi relative aux communications électroniques*) (the "Electronic Communications Act") (as amended) contains provisions regarding the confidentiality of electronic communications and the use of cookies and similar technologies.

In addition, the processing of personal data for electronic marketing purposes is regulated in the Belgian Code on Economic Law of February 28, 2013.

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

The Electronic Communications Act imposes requirements on providers of telecommunication and internet services regarding data retention, the use of location data and the notification of data security breaches. There is also specific legislation on the processing of personal data in the financial sector.

1.4 What is the relevant data protection regulatory authority(ies)?

The Belgian Privacy Commission (*Commissie voor de bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée*) oversees compliance with Belgian privacy and data protection law.

2 Definitions

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

- **"Personal Data"**

  Personal data is "any information relating to an identified or identifiable natural person".
- **"Sensitive Personal Data"**

  The Data Protection Act identifies three types of sensitive personal data:
  - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership as well as the processing of data concerning sex life;
  - health-related personal data; and
  - personal data relating to litigation that has been submitted to Courts and Tribunals as well as to administrative judicial bodies, relating to suspicions, prosecutions or convictions in matters of crime, administrative sanctions or security measures.
- **"Processing"**

  Processing is "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by means of transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data".
- **"Data Controller"**

  The data controller is "any natural or legal person, un-associated organisation or public authority which alone or jointly with others determines the purposes and means of the processing of personal data".
- **"Data Processor"**

  The data processor is "any natural person, legal person, un-associated organisation or public authority which processes personal data on behalf of the controller, except for the persons who, under the direct authority of the controller, are authorised to process the data".
- **"Data Subject"**

  The data subject is "an identified or identifiable natural person". An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Pseudonymous Data"**

    Belgian data protection law does not contain a definition of "pseudonymous data". However, the Royal Decree defines encoded data as "personal data which can only be linked to an identified or identifiable individual by way of a code".
  - **"Direct Personal Data"**

    "Direct personal data" is not defined or used in Belgian data protection law.
  - **"Indirect Personal Data"**

    "Indirect personal data" is not defined or used in Belgian data protection law.

3 Key Principles

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

- **Transparency**

  Data controllers are required to inform data subjects of the processing of their personal data. The Data Protection Act lists the information that must be provided to data subjects (e.g., processing purposes, data subjects' rights, etc.).
- **Lawful basis for processing**

  Data controllers must have a legal basis for each data processing activity. The Data Protection Act includes an exhaustive list of the legal grounds for processing of (sensitive) personal data (e.g., data subjects' consent).
- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes.
- **Data minimisation**

  Personal data must be accurate, relevant and not excessive in relation to the purposes for which they were collected and processed. Data controllers are required to limit the data processing to what is strictly necessary for the processing purpose.
- **Proportionality**

  As part of the data minimisation principle, personal data collected and processed must be proportionate to the processing purposes.
- **Retention**

  Personal data must be kept in a form that allows for the identification of data subjects for no longer than necessary in light of the purposes for which the data are collected or further processed.
- *Other key principles – please specify*

  There are no other key principles in particular.

4 Individual Rights

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

- **Access to data**

  Data subjects are entitled to request that the data controller provides information regarding the processing of their personal data and communicates the data in an intelligible form. This does not necessarily entail that data subjects should have direct access to data files or have the right to obtain a copy of their personal data.
- **Correction and deletion**

  Data subjects are entitled to obtain, free of charge, the rectification of incorrect personal data relating to them. Data subjects are also entitled to obtain, free of charge, the erasure of or the prohibition to use all personal data relating to them that is incomplete or irrelevant with a view to the purpose of the processing, or where the recording, disclosure or storage of the data is prohibited, or where it has been stored for longer than the authorised period of time.
- **Objection to processing**

  Under certain conditions, data subjects are entitled to object to the processing of personal data relating to them.
- **Objection to marketing**

  If personal data are obtained for direct marketing purposes, data subjects may object to the intended processing of their personal data, free of charge and without reason.

  Data subjects must be informed of this right to object when their personal data are collected for direct marketing purposes.
- **Complaint to relevant data protection authority(ies)**

  Data subjects are entitled to request the Privacy Commission, free of charge, to exercise their rights on their behalf.
- *Other key rights – please specify*
  - **Automated decision-making**

    Data subjects have the right not to be subject to decisions having legal effects or significantly affecting them, which are taken purely on the basis of automatic data processing aimed at assessing certain aspects of their personality, unless the decisions are taken in the context of an agreement or if they are based on a legal provision.
  - **Right to compensation**

    Data subjects have the right to receive compensation from data controllers for damage incurred as a result of a violation of the Data Protection Act, unless the data controllers can prove that the facts which caused the damage cannot be ascribed to them.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

In Belgium, there is a general obligation for data controllers to notify their data processing activities to the Privacy Commission. Exemptions from this notification obligation exist for standard data processing activities (e.g., standard payroll administration), provided certain conditions are met (e.g., conditions concerning types of data and data subjects, data retention, disclosure to third parties, etc.).

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

Notifications are made per processing purpose or set of related purposes.

5.3 Who must register with/notify the relevant data protection authority(ies)? (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.)

Data controllers must notify their data processing activities (falling within the scope of the Data Protection Act) to the Privacy Commission unless an exemption applies. This includes data processing activities performed in the context of the effective and actual activities of a data controller permanently established on Belgian territory or in a place where Belgian law applies by virtue of international public law, as well as data processing activities of data controllers established outside the EU, using means for processing personal data located on Belgian territory (unless the means are only used for the purposes of transit of personal data through Belgian territory). In the latter case, the data controller established outside the EU is required to appoint a representative in Belgium.

Furthermore, joint data controllers may file a common notification.

5.4 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.)

The notification should describe the data processing operation(s). In particular, the notification should include the name, address and contact details of the data controller (and, if applicable, his representative), the name of the processing activity, the purpose or set of related purposes of the data processing, the categories of personal data being processed (including a detailed description of sensitive data, if any), the categories of data recipients (including the safeguards linked to the disclosure of data to these third parties), the manner in which data subjects are informed of the data processing and how they can exercise their rights, the applicable data retention periods, the security measures implemented to protect the personal data and the countries to which personal data may be transferred (including the legal basis for transfers to non-EEA countries).

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

Failure to notify can be sanctioned with fines of up to EUR 600,000.

5.6 What is the fee per registration (if applicable)?

The fee for notification is:

- EUR 25 for notifications submitted online;
- EUR 125 for notifications submitted via paper forms; and
- EUR 20 for amending existing notifications.

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

Notifications should be updated when the information provided therein is no longer accurate.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

In general, prior approval from the Privacy Commission is not required to carry out data processing activities. However, specific authorisation requirements may apply in certain exceptional cases (e.g., for the processing of data from the national register or for data processing for historical, statistical or scientific purposes).

International data transfers on the basis of *ad hoc* international data transfer agreements or Binding Corporate Rules ("BCR") also require prior approval (see section 8 below).

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

Several sector committees are established within the Privacy Commission which are responsible for granting prior approval for certain specific types of data processing. The procedure differs depending on the sector committee.

The procedure for prior approval of *ad hoc* international data transfer agreements or BCRs is described in section 8 below.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The appointment of a Data Protection Officer is optional (except for certain public bodies). The Privacy Commission has indicated that it supports the appointment of Data Protection Officers and that these appointments should be seen as an accountability measure which the data controller should be able to take freely, considering the processing operations carried out, the actual risks, the existence of other protection mechanisms and the actual benefits the appointment of a Data Protection Officer would offer in terms of increased data protection.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Office where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

There are no specific legal advantages (such as exemption from notification obligation). Nevertheless, the appointment of a Data Protection Officer is one of the information security measures recommended by the Privacy Commission.

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

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

Typically, a Data Protection Officer is responsible for the execution of the data controller's information security policy.

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

No, this is not the case in Belgium (unless in limited cases where prior approval of one of the sector committees of the Privacy Commission is required).

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

The automated sending of marketing communications by telephone without human intervention or by fax requires prior opt-in consent. The sending of marketing communications by SMS or by email also requires prior consent, unless the recipients are existing customers or legal entities and specific conditions are met. Direct marketing via other techniques to individuals who opted out of receiving such marketing communications is prohibited.

In addition, the Data Protection Act contains a general obligation for data controllers to provide data subjects with a right to opt-out of the processing of their personal data for direct marketing purposes.

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

The Privacy Commission has indicated that it considers direct marketing to be an important issue. However, it is unclear whether the Privacy Commission is actively enforcing marketing rules since the Privacy Commission rarely publishes information on its enforcement actions.

7.3 Are companies required to screen against any "do not contact" list or registry?

Before contacting individuals by phone for marketing purposes, companies are required to verify whether or not the concerned individuals have registered their name on the "do not call me anymore" list ("*bel-me-niet-meer-lijst*"), which is kept by non-profit organisation DNCM. Telecom operators are required to inform their users about this list and individuals can register online (www.bel-me-niet-meer.be). Contacting individuals registered on the list is prohibited, unless the company has obtained the specific consent of the individuals.

The Belgian Direct Marketing Association maintains a similar list for marketing by post, called the "Robinson" list. However, this list only imposes obligations on members of the Belgian Direct Marketing Association.

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

The use of automated calling systems without human intervention (automatic calling machines) or fax machines for sending marketing without prior opt-in consent may lead to fines of up to EUR 60,000. Sending marketing by SMS or email without prior opt-in consent may result in fines of up to EUR 150,000.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

The use of cookies requires opt-in consent, unless the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or if the cookie is strictly necessary to provide a service requested by the subscriber or user.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

The cookie rules imposed by EU Directive 2009/136/EC have been transposed in Article 129 of the Electronic Communications Act. Article 129 contains the same language as the cookie clause in EU Directive 2009/136/EC and it does not provide guidance as to how to obtain consent to the use of cookies. According to the Privacy Commission's Recommendation (nr. 01/2015) on the Use of Cookies, consent requires a clear action from the user (e.g., ticking a box or browsing to another webpage provided that the cookie notice is displayed until the user makes an explicit choice). Implied consent for the use of cookies is generally not considered acceptable.

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

In June 2015, the Privacy Commission initiated legal proceedings against Facebook for tracking individuals' browsing behaviour through cookies and social plug-ins without obtaining their consent. The Brussels Court of First Instance ordered Facebook to stop this practice. If Facebook does not comply with the Court's decision, it will have to pay a fine of EUR 250,000 per day of non-compliance.

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

Certain sanctions provided in the Belgian Criminal Code and the Data Protection Act could be imposed in the case of violation of the Belgian cookie rules. Possible sanctions include fines of up to EUR 600,000.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

In principle, the transfer of personal data to a country outside the EEA that does not provide an "adequate level of protection" is prohibited. The Privacy Commission follows the European Commission's decisions as regards those countries that are considered to provide such adequate level of protection.

The Data Protection Act provides a limited list of exceptions to this general prohibition. For instance, data transfers are permitted if the data subject has unambiguously given his/her consent to the proposed data transfer. The Data Protection Act also provides a derogation from the general prohibition if the data controller "ensures adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, and regarding the exercise of the corresponding rights; such safeguards can result from appropriate contractual clauses in particular".

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Companies typically put in place data transfer agreements based on the European Commission's Standard Contractual Clauses. More and more companies are also starting to use BCRs.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Each notification with the Privacy Commission contains a section on international data transfers that must be completed in cases where personal data are transferred abroad.

International data transfers to non-EEA countries that provide an adequate level of data protection, or that are based on one of the statutory exemptions listed in the Data Protection Act, do not require authorisation. However, in the case of data transfers based on a data transfer agreement, the agreement must be submitted to the Privacy Commission for approval, even if the agreement is based on one of the European Commission's Standard Contractual Clauses. In accordance with the Protocol of June 25, 2013 between the Privacy Commission and the Belgian Ministry of Justice, if the Privacy Commission concludes that the data transfer agreement incorporates the European Commission's Standard Contractual Clauses, the Privacy Commission will simply inform the data controller that the proposed international data transfers are permitted. In the case of a non-standardised data transfer agreement, the Privacy Commission will examine whether the data transfer agreement provides adequate safeguards for the international data transfer. If the Privacy Commission determines that the safeguards are adequate, the Ministry of Justice will verify that the entity complied with the applicable procedural rules and, if so, approve the agreement by Royal Decree.

In cases of data transfers based on a BCR, the BCR also needs to be sent to the Privacy Commission for approval. The Privacy Commission will review the BCR and send its opinion to the Ministry of Justice. In accordance with the Protocol of July 13, 2011 between the Privacy Commission and the Ministry of Justice, if the Privacy Commission's opinion is favourable, the Ministry of Justice will verify that the process specified in the Protocol has been followed and, if so, automatically approve the BCR by Royal Decree.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

In accordance with the Privacy Commission's Recommendation on the implementation of whistle-blowing schemes (Recommendation 01/2006 of November 29, 2006), the scope of corporate whistle-blower hotlines under Belgian data protection law does not need to be limited to certain issues. However, the Privacy Commission recommends that whistle-blower hotlines should only be used for reporting very serious issues that should be reported in the general interest or for the proper governance of the company (e.g., violations of financial, accounting or criminal law) and which, in the opinion of the whistle-blower, cannot be reported through the company's normal reporting channels (for example, the whistle-blower's first-line manager).

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

Anonymous reporting is not prohibited, but it should not be encouraged. The Privacy Commission follows the Article 29 Working Party Opinion 1/2006 (WP 117) on this point, which provides that anonymous reporting should only be allowed as an exception to the rule and under the following conditions:

- anonymous reporting is not encouraged; and
- whistle-blowers are informed, when submitting a report, that their identity will be kept confidential at all the stages of the process and in particular will not be disclosed to third parties, either to the incriminated person or to the whistle-blower'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.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Prior to implementation, the whistle-blower hotline must be notified to the Privacy Commission. The notification will typically be processed and published within 21 days after completion of the notification procedure. Prior approval is not required.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

There is no explicit requirement to have a separate notice for a whistle-blower hotline. However, as the information that needs to be provided to individuals about the whistle-blower hotline is rather specific (e.g., description of the procedure for submitting and handling reports, possible consequences of unfounded reports, etc.), in practice companies tend to implement a separate privacy notice for their whistle-blower hotline.

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

Works councils/trade unions/employee representatives must be informed prior to implementing a whistle-blower hotline in the company.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

In accordance with the Camera Surveillance Act of March 21, 2007, the use of CCTV requires a separate notification with the Privacy Commission. In the case of CCTV surveillance at the workplace, an additional notification with the Privacy Commission is required in accordance with Collective Labour Agreement no. 68 concerning camera surveillance at the workplace.

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

Employers may monitor employees' use of the company's email and internet system, in accordance with the procedures set out in Collective Labour Agreement no. 81 concerning the monitoring of electronic online communications of employees. Collective Labour Agreement no. 81 limits the monitoring to the following purposes:

1. the prevention of any unwanted, improper or defamatory activities or facts, or activities or facts that are against the public decency or may harm the dignity of other persons;
2. the protection of confidential economic, commercial and financial interests of the company, and to act against any practices inconsistent with the preservation of these interests;
3. the preservation of the security and/or the good technical functioning of the company's IT network systems, including monitoring the costs associated with it and the physical protection on the company's facilities; and
4. compliance in good faith with the company's policies and any other applicable principles and rules on the use of online technologies.

On May 2, 2012, the Privacy Commission issued a Recommendation on workplace cyber-surveillance (Recommendation 08/2012). In this Recommendation, the Privacy Commission explains via practical examples how employers can comply with Belgian privacy and data protection law when monitoring employees' use of the company's IT system. For instance, the Privacy Commission strongly recommends employers to encourage employees to label their private emails as "personal" and/or to store them in a folder marked as private. The Privacy Commission also recommends companies to appoint a neutral, trusted individual who will be authorised to review an absent/dismissed employee's emails and determine which emails are of a professional nature and need to be read by the employer (e.g., to pass on an urgent matter to a colleague while an employee is absent).

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

Employees should be informed of any monitoring. This is typically done via a HR privacy policy, an IT acceptable use policy or a specific monitoring policy. It is not required, nor is it advisable, to obtain their consent. The Privacy Commission takes the view that an employee's consent is, in principle, not considered to be freely given, because of his/her subordinate position.

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

Employee representative bodies such as works councils must be informed of the introduction of employee monitoring systems and should evaluate the systems on a regular basis.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Employee monitoring can be notified to the Privacy Commission as part of a general HR management registration.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

To date, the Privacy Commission has not issued specific guidance on processing of personal data in the cloud. However, it has announced that it is currently preparing such guidance. In the meantime, the Privacy Commission is likely to expect that data controllers and processors follow the guidelines issued by the Article 29 Working Party on this topic (in particular, Opinion 05/2012). In addition, the Data Protection Act imposes a general obligation on data controllers to: a) select processors providing sufficient safeguards in respect of the technical and organisational measures for the intended processing; and b) ensure compliance with these measures, in particular by contractual stipulations. This general obligation also applies in a cloud computing context.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

In the absence of specific guidance on processing of personal data in the cloud, the contract with a processor providing cloud-based services must contain at least the following elements:

- an obligation for the data processor to implement technical and organisational security measures for the intended processing;

- the data processor's liability towards the data controller; and
- the requirement that the data processor shall only act on behalf of the data controller and that it is bound by the same data security duties as the data controller.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

To date, the Privacy Commission has not issued specific guidance on the utilisation of big data and analytics. However, Royal Decree of February 13, 2001 contains specific rules on further processing of personal data for historical, statistical or scientific purposes, which may be relevant to certain big data applications or analytics. Pursuant to the Royal Decree, further processing of personal data for historical, statistical or scientific purposes must in principle take place using anonymous data. If it is impossible to achieve the historical, statistical or scientific purposes using anonymous data for the further processing, the data controller of the further processing for historical, statistical or scientific purposes may process encoded data and, in exceptional circumstances, non-encoded personal data.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Data controllers and processors are required to implement appropriate technical and organisational measures to protect personal data from accidental or unauthorised destruction, accidental loss, as well as from alteration, access and any other unauthorised processing. These measures must ensure an appropriate level of security taking into account the state of technological development in this field and the cost of implementing the measures on the one hand, and the nature of the personal data to be protected and the potential risks related to the processing on the other hand.

The Privacy Commission has issued non-binding guidance as to the type of security measures (e.g., encryption) that should be implemented (*Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens/Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* and *Aanbeveling uit eigen beweging betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken/ Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*).

13.2 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) expects voluntary breach reporting.

The Electronic Communications Act imposes a duty on providers of publicly available electronic communications services to notify data breaches, under certain conditions, to the Privacy Commission. The notification should contain the following information: (i) the nature of the data breach; (ii) consequences of the data breach; (iii) details of person which can be contacted for more information concerning the breach; (iv) measures suggested or implemented to address the data breach; and (v) measures recommended to mitigate the negative effects of the data breach. Where feasible, the notification should be completed within 24 hours after detection of the breach. In cases where the company does not have all required information within this timeframe, it can complete the notification within 72 hours after the initial notification. The Privacy Commission has published a template form on its website to accommodate companies in complying with their data breach notification obligations.

Except for the notification duty in the Electronic Communications Act, there is currently no general data breach notification obligation. However, the Privacy Commission strongly recommends all types of data controllers to notify data breaches. It has published a separate template form on its website to be used by data controllers that are not electronic communication providers for the purposes of notifying data breaches.

13.3 Is there a legal requirement to report data breaches to individuals? 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) expects voluntary breach reporting.

Unless a specific exemption applies, providers of publicly available electronic communications services should report data breaches to the affected individuals immediately after detection of the breach in cases where the breach is likely to negatively impact their privacy. This notification should contain the following information: (i) name of the company; (ii) contact person; (iii) description of the data breach; (iv) date of the data breach; (v) the data affected by the breach; (vi) possible consequences for the privacy of the concerned individual; (vii) circumstances of the data breach; (viii) measures implemented by the company to remedy the data breach; and (ix) recommended measures for the affected individuals to mitigate the negative effects of the breach. The Privacy Commission also recommends data controllers that do not qualify as electronic communication providers to notify the affected individuals in the event of a data breach.

13.4 What are the maximum penalties for security breaches?

Belgian data protection law does not provide specific penalties for security breaches.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
The Privacy Commission has the power to investigate possible violations of Belgian privacy and data protection law, at its own initiative or following complaints from individuals.	The Privacy Commission cannot impose sanctions. If it determines that Belgian privacy and data protection law may have been violated, it can bring the case before the Court of First Instance or refer it to the Public Prosecutor. In addition, a violation of Belgian privacy and data protection law may lead to civil action for damages.	Unlawfully processing personal data is punishable with fines of up to EUR 600,000, confiscation of the media containing the personal data to which the offence relates, the erasure of the data or the prohibition to manage any processing of personal data, directly or through an agent, for a period of up to two years. A Court may also order the publication of the judgment in one or more newspapers. Any repeated violation of the Data Protection Act is punishable by a term of imprisonment of up to two years, and/or fines of up to EUR 600,000.

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

The Privacy Commission does not publish statistics on its enforcement actions, but criminal proceedings will typically only be initiated in cases of severe violations.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

As a matter of best practice, companies within Belgium should attempt to comply with the recommendations in Working Document 1/2009 of the Article 29 Working Party when responding to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies.

15.2 What guidance has the data protection authority(ies) issued?

To date, the Privacy Commission has not issued specific guidance on the processing of personal data in the context of e-discovery requests. However, the Privacy Commission is likely to expect that data controllers and processors follow the guidelines issued by the Article 29 Working Party on this topic (in particular, Working Document 1/2009), as representatives of the Privacy Commission participated in the sub-group of the Article 29 Working Party that drafted the Working Document.

16 Trends and Developments

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

In 2015, the Privacy Commission has taken a number of enforcement initiatives related to the protection of individuals' privacy online.

The Privacy Commission has, for example, participated in the Internet Sweep Day organised by the Global Privacy Enforcement Network ("GPEN"), during which a number of data protection authorities performed a coordinated audit of approximately 1,500 websites and apps intended for, or popular with, children. The Privacy Commission has announced that it will reach out to a number of website and app developers with the findings of the audit. In cases where the audit revealed serious violations of the Data Protection Act, the Privacy Commission may issue a formal warning and, where necessary, forward the case to the competent authorities for further investigation and/or prosecution (e.g., to the Public Prosecutor).

The Privacy Commission's focus on online privacy was further demonstrated by its enforcement actions against Facebook for tracking online behaviour of non-members through cookies and social plug-ins. After issuing a formal Recommendation to Facebook, the Privacy Commission initiated legal proceedings before the Brussels Court of First Instance in June 2015. In November 2015, the Brussels Court ordered Facebook to stop tracking non-users. If Facebook does not comply with the Court's decision, it faces a fine of EUR 250,000 per day.

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

Similar to other data protection authorities throughout the EU, the Privacy Commission will most likely focus on preparing for its new role and tasks under the upcoming General Data Protection Regulation.

International data transfers and the mechanisms available to companies to legitimise such transfers will probably also remain a "hot topic" for the Privacy Commission following the invalidation of Safe Harbour and the introduction of the alternative EU-US Privacy Shield for transatlantic data flows.

Wim Nauwelaerts
Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 14
Fax: +32 2 643 58 22
Email: wnauwelaerts@hunton.com
URL: www.hunton.com

Wim Nauwelaerts is the managing partner of the firm's Brussels office and leads the Privacy and Cybersecurity team there. Wim advises companies on all aspects of EU and international data protection and privacy compliance, including data protection notifications, implementation of data security measures, compliance training, data transfer strategies, privacy implications of cross-border M&A transactions and representations before data protection authorities. Wim has been recognised as a leading privacy practitioner by *Chambers Global*, *Chambers Europe*, *The Legal 500* (Belgium), the *International Who's Who of Technology Lawyers*, and by *Global Law Experts*. He has written and spoken widely on privacy-related topics, such as cloud computing, interest-based advertising, cross-border discovery and privacy compliance in pharmaceutical research.

David Dumont
Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 18
Fax: +32 2 643 58 22
Email: ddumont@hunton.com
URL: www.hunton.com

David Dumont assists a broad range of clients with all aspects of Belgian and EU data protection law, including HR and customer data privacy issues, implementation of cross-border data transfer strategies and completing registrations with national data protection authorities.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal*'s "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

This article appeared in the 2016 edition of The International Comparative Legal Guide to: Data Protection published by Global Legal Group Ltd, London. www.iclg.co.uk

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk