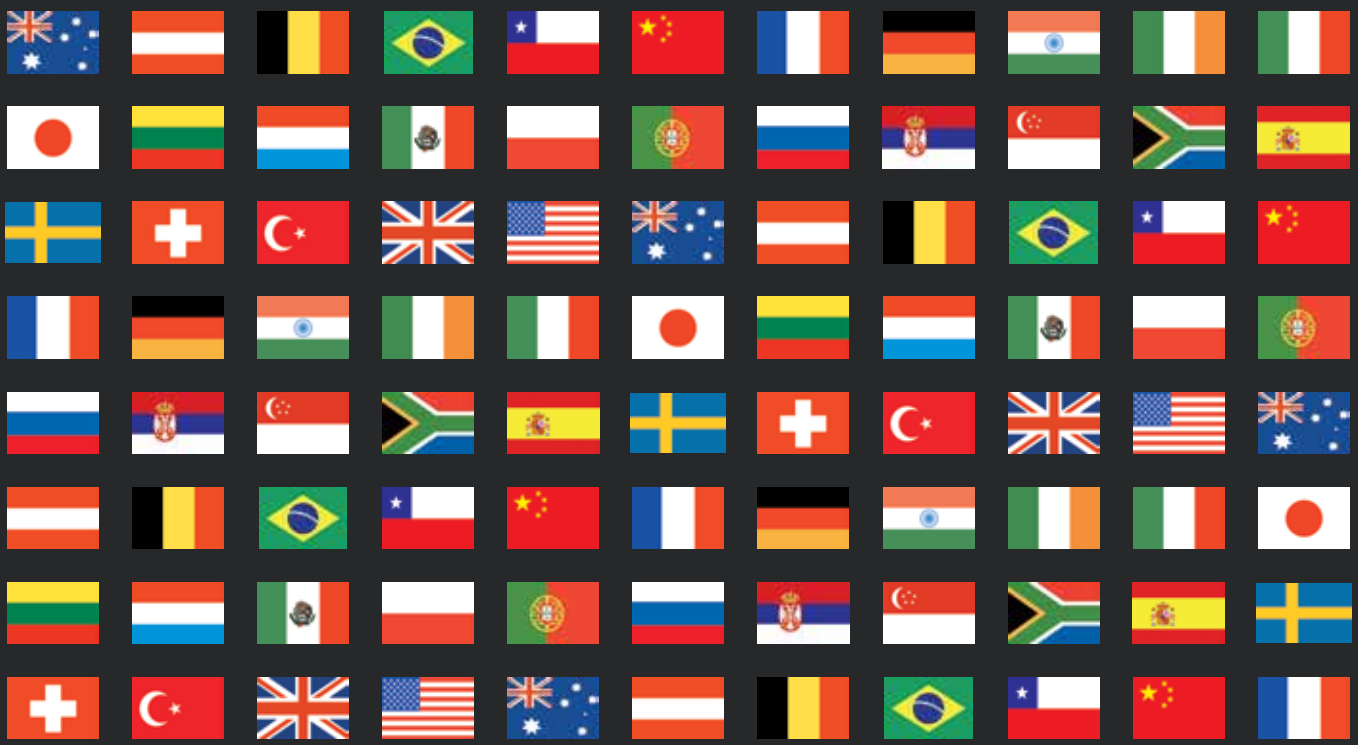
# Data Protection & Privacy



2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

# Data Protection & Privacy 2018

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910


First published 2012
Sixth edition
ISSN 2051-1280



Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

# Belgium

**Wim Nauwelaerts and David Dumont**
Hunton & Williams

## Law and the regulatory authority

### 1 Legislative framework

**Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?**

Until the EU General Data Protection Regulation (the GDPR) becomes applicable, the Act on the Protection of Privacy in relation to the Processing of Personal Data of 8 December 1992 (the Data Protection Act), as well as the Royal Decree of 13 February 2001 implementing the Data Protection Act (the Royal Decree), will continue to be the main data protection legislation in Belgium. The Data Protection Act, which has been significantly amended over time, transposes Data Protection Directive 95/46/EC into Belgian law.

Furthermore, the following international instruments on privacy and data protection also apply in Belgium:

- the Council of Europe Convention 108 on the Protection of Privacy and Trans-border Flows of Personal Data;
- the European Convention on Human Rights and Fundamental Freedoms (article 8 on the right to respect for private and family life); and
- the Charter for Fundamental Rights of the European Union (article 7 on the right to respect for private and family life and article 8 on the right to the protection of personal data).

In addition to the general legislative framework for data protection outlined above, there is also sector-specific legislation relevant to the protection of PII. The Electronic Communications Act of 13 June 2005 (the Electronic Communications Act), for instance, imposes specific privacy and data protection obligations on electronic communications service providers.

On 25 May 2018, the GDPR will become applicable in all EU member states, including Belgium. The Belgian Secretary of State for Privacy is preparing a draft bill to replace the current Data Protection Act with the GDPR, and implement Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

### 2 Data protection authority

**Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.**

The Belgian Commission for the Protection of Privacy, better known as the Privacy Commission, is responsible for overseeing compliance with privacy and data protection law in Belgium. Since 1 January 2004, the Privacy Commission has been an independent supervisory authority under the auspices of the Belgian House of Representatives. The Privacy Commission consists of 16 members, who are appointed for a renewable six-year mandate. The Privacy Commission's powers include:

- issuing opinions and recommendations on any matters relating to the application of the fundamental principles of data protection, on its own initiative or at the request of the different governments and legislators in Belgium;
- investigating privacy- and data-protection-related complaints. In this respect, the Privacy Commission mainly plays a mediating role. If an amicable settlement cannot be reached, the Privacy Commission can issue an opinion on the legitimacy of the complaints, as well as specific recommendations directed to the controller;
- organising on-site investigations into potential privacy and data protection violations. For that purpose, members of the Privacy Commission have the status of assistant officers of the Public Prosecutor, and they have access to all places that may reasonably be linked to activities covered by the Data Protection Act. They can demand, among other things, the disclosure of any documents that may be of use for their investigation; and
- receiving and keeping a record of notifications submitted by controllers (or their local representatives) with regard to wholly or partly automatic data processing operations carried out in Belgium.

The Privacy Commission itself cannot impose sanctions for privacy or data protection violations. Instead, it must inform the Public Prosecutor of such violations, and the Public Prosecutor can subsequently decide whether or not to press charges. However, in some cases the President of the Privacy Commission may submit privacy and data protection disputes to the Court of First Instance.

The role and powers of the Privacy Commission will significantly change once the GDPR becomes applicable. In light of this upcoming change, the Secretary of State for Privacy has prepared a draft bill to reform the Privacy Commission. However, the Privacy Commission has made substantial comments with respect to the draft bill and, therefore, it will most likely be amended before the Secretary of State submits the draft bill to the Parliament for approval.

### 3 Breaches of data protection

**Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?**

Breaches of data protection law can lead to civil or criminal penalties if the Privacy Commission decides to bring the case before the Court of First Instance or to refer it to the Public Prosecutor. Unlawful processing of PII is punishable with fines up to €800,000, confiscation of the media containing the PII, erasure of the data or a prohibition to manage any PII processing for a period of up to two years. The Belgian courts may also order the publication of their judgments 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 or fines of up to €800,000. In addition, violations of Belgian privacy and data protection law may result in civil action for damages.

## Scope

### 4 Exempt sectors and institutions

**Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?**

The Data Protection Act is intended to cover all sectors and all types of organisations, but the following types of PII processing fall (partly) outside of its scope:

- processing of PII by a natural person in the course of a purely personal or household activity, for example, a private address file, or a personal electronic diary;
- processing of PII solely for journalism purposes, or purposes of artistic or literary expression, if the processing relates to PII made public by the data subject or closely related to the public nature of the data subject or the facts in which the data subject is involved;
- processing of PII by the State Security Service, or the General Intelligence and Security Service of the Armed Forces;
- processing of PII managed by public authorities with a view to the fulfilment of their judicial police duties;
- processing of PII that is necessary to comply with anti-money laundering laws; and
- processing of PII managed by the European Centre for Missing and Sexually Exploited Children.

### 5 Communications, marketing and surveillance laws

**Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.**

The Data Protection Act generally applies to interception of communications and electronic marketing, as well as monitoring and surveillance of individuals. In addition, these topics are addressed by specific laws and regulations, including:

- the Belgian Criminal Code, the Electronic Communications Act and Collective Bargaining Agreement No. 81 of 26 April 2002 on the monitoring of employees' online communications (interception of communications);
- the Belgian Code of Economic Law, and the Royal Decree of 4 April 2003 regarding spam (electronic marketing); and
- the Belgian Act of 21 March 2007 on surveillance cameras, the Royal Decree of 10 February 2008 regarding the signalling of camera surveillance, the Royal Decree of 2 July 2008 regarding the registration of camera surveillance, the Royal Decree of 9 March 2014 appointing the categories of individuals authorised to watch real-time images of surveillance cameras in public spaces, and the Collective Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance at the workplace (surveillance of individuals).

### 6 Other laws

**Identify any further laws or regulations that provide specific data protection rules for related areas.**

A significant number of laws and regulations set forth specific data protection rules that are applicable in a certain area, for example:

- Belgian Act of 21 August 2008 on the establishment and organisation of the e-Health Platform (e-health records).
- Book VII of the Belgian Code of Economic Law on payment and credit services containing data protection rules for the processing of consumer credit data (credit information).

### 7 PII formats

**What forms of PII are covered by the law?**

The Data Protection Act applies to the processing of PII (ie, any information relating to an identified or identifiable natural person), wholly or partly by automatic means, and to the processing otherwise than by automatic means of PII that forms part of a filing system (or is intended to form part of a filing system). 'Filing system' refers to any structured set of PII that is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

### 8 Extraterritoriality

**Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?**

The Data Protection Act applies to processing of PII by a controller who is either established in Belgium (provided that the processing of PII is carried out in the context of the activities of the establishment) or not established in Belgium or another EU country, but who uses 'means' located on Belgian territory to process PII other than for transit purposes. 'Means' can refer to, for example, the use of service providers operating in Belgium.

### 9 Covered uses of PII

**Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?**

In principle, all types of PII processing fall within the ambit of the Data Protection Act, regardless of who is 'controlling' the processing or merely processing PII on behalf of a controller. The 'controller' is any natural or legal person, un-associated organisation or public authority that alone or jointly with others determines the purposes and means of the processing of PII. The obligations set forth in the Data Protection Act are mainly addressed to the controller. The concept of 'processor' refers to any natural person, legal person, un-associated organisation or public authority that processes PII on behalf of the controller, except for the persons who, under the direct authority of the controller, are authorised to process the data (eg, employees of the controller). Except for legal information security requirements, data protection obligations are imposed on processors through their mandatory contract with the controller.

## Legitimate processing of PII

### 10 Legitimate processing – grounds

**Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?**

Controllers are required to have a legal basis for each PII processing activity. The Data Protection Act includes the following, exhaustive list of potential legal grounds for processing of PII:

- the individual (data subject) has unambiguously consented to the processing of his or her PII;
- the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with an obligation to which the controller is subject under or by virtue of an act, decree or ordinance;
- the processing is necessary in order to protect the vital interests of the data subject;
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller or in a third party to whom the PII is disclosed; or
- the processing is necessary for the legitimate interests of the controller (or the third party to whom the data is disclosed), provided that those interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

For certain types of PII, more restrictive requirements in terms of legal basis apply (see question 11).

### 11 Legitimate processing – types of PII

**Does the law impose more stringent rules for specific types of PII?**

The processing of PII revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of PII concerning a person's sex life, is prohibited in principle, and can only be carried out if:

- the data subject has given his or her written consent to such processing;
- the processing is necessary to carry out the specific obligations and rights of the controller in the employment law area;
- the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his or her consent;
- the processing is carried out by a foundation, association or any other non-profit organisation with political, philosophical, religious, health insurance or trade union objectives, in the course of its legitimate activities;
- the processing relates to PII that has been made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for the purposes of scientific research (subject to certain conditions);
- the processing is necessary to comply with social security laws;
- the processing is carried out in accordance with the Act of 4 July 1962 on Public Statistics;
- the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment to the data subject or one of his or her relatives, or the management of healthcare services in the interest of the data subject, provided that the PII is processed under the supervision of a health professional;
- the processing is carried out by an association with legal personality or an organisation of public interest whose main objective is the protection and promotion of human rights and fundamental freedoms; or
- the processing of PII is authorised (by an act, decree or ordinance) for another reason of substantial public interest.

The processing of health-related PII is prohibited in principle, and can only be carried out if:

- the data subject has given his or her written consent to such processing;
- the processing is necessary to carry out the specific obligations and rights of the controller in the employment law area;
- the processing is necessary to comply with social security laws;
- the processing is necessary for the promotion and protection of public health, including medical examination of the population;
- the processing is required (by an act, decree or ordinance) for reasons of substantial public interest;
- the processing is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving his or her consent;
- the processing is necessary for the prevention of imminent danger or the mitigation of a specific criminal offence;
- the processing relates to PII that has been made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment to the data subject or to one of his or her relatives, or the management of healthcare services in the interest of the data subject, provided that the PII is processed under the supervision of a health professional; or
- the processing is required for the purposes of scientific research (and carried out under certain conditions).

The processing of litigation-related PII (including PII relating to suspicions, prosecutions or convictions in criminal matters or administrative sanctions) is prohibited in principle and can only be carried out if the PII is processed:

- under the supervision of a public authority or ministerial civil servant, provided the processing is necessary for the fulfilment of duties;
- by other persons, if the processing is necessary to achieve purposes that have been established by law;
- by natural persons, private or public legal persons, to the extent that the processing is necessary to manage their own litigation;
- by lawyers or other legal advisors, to the extent that the processing is necessary for the protection of their clients' interests; or
- because the processing is required for scientific research and carried out under specific conditions established by law.

## Data handling responsibilities of owners of PII

### 12 Notification

**Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?**

Controllers are required to provide notice to data subjects whose PII is processed. The Data Protection Act lists the information that must be provided to data subjects. If PII is obtained directly from the data subject, the controller (or its representative) must provide at least the following information no later than the moment the PII is obtained:

- the name and address of the controller (and of its representative, if any);
- the purposes of the processing;
- the existence of the right to object, free of charge, to the intended PII processing for direct marketing purposes;
- the (categories of) recipients of PII;
- whether it is compulsory to reply to requests for information and what the possible consequences of the failure to reply are;
- the existence of the right to access and rectify his or her PII; and
- other information dependent on the specific nature of the processing as specified by law (additional notice obligations apply, eg, when processing health data).

If PII is not obtained directly from the data subject, the controller (or its representative) must provide, in addition to the information listed above, the categories of PII concerned. This information must be provided when collecting PII or, when PII is shared with a third party, at the very latest when the PII is first disclosed.

### 13 Exemption from notification

**When is notice not required?**

Notice is not required if data subjects have already received the information mentioned in question 12. In addition, in cases where PII is not collected directly from the data subject, the controller is exempt from the duty to provide notice if:

- informing the data subject proves impossible or would involve a disproportionate effort, in particular in the context of statistical, historical or scientific research, or for the purpose of medical examination of the population with a view to protecting and promoting public health; or
- PII is recorded or provided to comply with legal provisions.

### 14 Control of use

**Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?**

The Data Protection Act includes a number of rights aimed at enabling data subjects to exercise choice and control over the use of their PII. In particular, data subjects are entitled to:

- request the controller to provide information regarding the processing of their PII and communication of the PII in an intelligible form;
- obtain, free of charge, the rectification of incorrect PII relating to them;
- object to the processing of their PII, for substantial and legitimate reasons related to their particular situation, unless the processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract with the data subject or when the processing is necessary for compliance with a legal obligation;
- obtain, free of charge, the erasure of or the prohibition to use PII 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 PII is prohibited, or where it has been stored for longer than the authorised period of time;
- object to the intended processing of their PII, free of charge and without reason, if PII is obtained for direct marketing purposes;

- complain to the Privacy Commission, free of charge, and request that the Privacy Commission exercises their rights on their behalf;
- not 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 decision is taken in the context of an agreement or if it is based on a legal provision; and
- receive compensation from controllers for damage incurred as a result of a violation of the Data Protection Act, unless the controllers can prove that the facts that caused the damage cannot be ascribed to them.

### 15 Data accuracy

**Does the law impose standards in relation to the quality, currency and accuracy of PII?**

Under the Data Protection Act, controllers must ensure that the PII they collect and further process is adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed. Furthermore, PII must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that PII that is inaccurate or incomplete, with respect to the purposes for which it is collected or for which it is further processed, is erased or rectified.

### 16 Amount and duration of data holding

**Does the law restrict the amount of PII that may be held or the length of time it may be held?**

Controllers are required to limit the processing of PII to what is strictly necessary for processing purposes. Pursuant to the data minimisation principle, PII collected and processed must be proportionate to the processing purposes. In terms of data retention requirements, PII 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 PII is collected or further processed. This means that, if a controller no longer has a need to identify data subjects for the purposes for which the PII was initially collected or further processed, the PII should be erased or anonymised.

### 17 Finality principle

**Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?**

The Data Protection Act incorporates the 'finality principle' and, therefore, PII can only be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes. In its guidance concerning the registration of processing activities (see question 23), the Privacy Commission has identified a list of purposes that are considered legitimate.

### 18 Use for new purposes

**If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?**

PII can be processed for new purposes as long as these are not incompatible with the initial purposes for which the PII was collected, taking into account all relevant factors, especially the reasonable expectations of the data subject and any applicable legal and regulatory provisions. Under specific conditions established by the Royal Decree, further processing of PII for historical, statistical or scientific purposes is not considered incompatible.

## Security

### 19 Security obligations

**What security obligations are imposed on PII owners and service providers that process PII on their behalf?**

Controllers and their processors are required to implement appropriate technical and organisational measures to protect PII 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 PII to be protected and the potential risks related to the processing on the other hand. The more sensitive the PII and the higher the risks for the data subject are, the more precautions have to be taken. For example, the processing of health-related PII outside a medical context (eg, by a life insurance company) should be subject to stricter security measures.

In 2013, the Privacy Commission issued non-binding guidance by means of a 'Recommendation' on information security. The Recommendation supplements and builds on two previously issued guidance documents from the Privacy Commission: the 2012 Reference Measures for the Security of Any Personal Data Processing Operation and the 2012 Guidelines Relating to Information Security of Personal Data. Jointly, these three guidance documents are intended to assist controllers and processors in their efforts to implement suitable security measures in compliance with the Data Protection Act.

### 20 Notification of data breach

**Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?**

The Electronic Communications Act imposes a duty on providers of publicly available electronic communications services to notify security breaches, under certain conditions, to the Privacy Commission. The notification should contain the following information:

- the nature of the security breach;
- the consequences of the breach;
- details of the person or persons who can be contacted for more information concerning the breach;
- measures suggested or implemented by the controller to address the breach; and
- measures recommended to mitigate the negative effects of the security breach.

Where feasible, the notification should be done within 24 hours after detection of the breach. In case the controller does not have all required information available within this time frame, 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. In addition, data subjects must be informed without undue delay when the security breach is likely to adversely affect their privacy or PII.

Except for the notification duty in the Electronic Communications Act, there is currently no general breach notification obligation. However, the Privacy Commission strongly recommends all types of controllers to notify security breaches. It has published a separate template form on its website to be used by controllers other than providers of electronic communication services for purposes of notifying security breaches. The Privacy Commission expects controllers to report a breach incident within 48 hours of discovery and, in some cases, to notify affected individuals as well. Failure to notify in the event of a security incident could trigger liability under Belgian data protection law. Upon notification, the Privacy Commission will generally conduct a formal investigation into the security incident, and examine how PII was processed and protected prior to the incident.

Although the Privacy Commission has taken the position that notifying security incidents is strongly recommended, the Privacy Commission acknowledges that notification is not necessary if: it is clear from the circumstances that the incident will not affect the privacy or PII of the individuals concerned; the controller can demonstrate that the PII was encrypted or otherwise protected so that the PII is not 'useful' in the hands of third parties; or affected individuals have been informed immediately of the scope and consequences of the security incident, provided that only a limited number of individuals were affected (not more than 100) and no 'sensitive' PII (eg, health-related PII) or financial data (eg, combination of an individual's name and bank account number) was involved.

## Internal controls

### 21 Data protection officer

**Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?**

The appointment of a data protection officer is not mandatory except in limited cases where a prior authorisation of the Privacy Commission is required for the data processing activity (eg, for processing PII from certain government databases).

Nevertheless, the Privacy Commission recommends controllers to appoint a person responsible for the implementation of the organisation's information security policy where the nature of the personal data processed justifies such information security measure. The main task of this person is to ensure that the various responsibilities with regard to information security (prevention, supervision, detection and processing) have been clearly defined and that the individuals in charge of information security within the organisation can operate autonomously and independently.

### 22 Record keeping

**Are owners of PII required to maintain any internal records or establish internal processes or documentation?**

The Data Protection Act does not provide any explicit obligations to maintain internal records or establish internal processes or documentation, unless sensitive PII is processed. In the latter case, the controller or processor must keep a list of categories of individuals having access to such PII with a precise description of their function with respect to the data processing activity. This list should be available to the Privacy Commission.

Furthermore, the Privacy Commission's recommendations on information security provide that controllers should have complete and centralised documentation relating to information security within their organisation, which is updated on a regular basis and contains at least the following information:

- the identity of the data protection officer (if any);
- an information security policy;
- an overview of the implemented security measures;
- an inventory of the PII being processed, its location and the operations performed on it;
- a list with the names of the bodies or designated individuals having access to the PII;
- a description of the system and network configuration;
- technical documentation about the security controls that are implemented;
- a schedule of planned operations;
- an intrusion detection policy;
- security control test plans;
- incident reports; and
- audit reports, if any.

## Registration and notification

### 23 Registration

**Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?**

As a general rule, controllers (as opposed to processors) are required to register their data processing activities with the Privacy Commission. A number of data processing activities are, however, exempted from the general registration obligation provided that certain conditions are met. For example, PII processing for the following purposes may not require registration: payroll management, employee administration, accounting, administration of shareholders and partners, customer and supplier management, communication purposes and access control. Furthermore, exemptions to the general registration obligation exist for certain data processing activities of non-profit organisations, educational organisations and public authorities.

### 24 Formalities

**What are the formalities for registration?**

Controllers can register their data processing activities by completing an online registration form on the Privacy Commission's website or by submitting a paper registration form (which can be downloaded from the Privacy Commission's website).

The following information needs to be provided in the registration form:

- identification details of the controller (such as name, corporate address, legal form, etc);
- name of the data processing;
- purposes of the data processing;
- categories of PII processed;
- legal basis for the data processing;
- categories of data recipients and measures implemented to secure the disclosure of PII to these data recipients;
- means of informing the data subjects about the processing of their PII;
- a person or department that data subjects can contact to exercise their rights and measures implemented by the controller to facilitate data subjects in exercising their rights;
- retention period of each category of PII;
- description of the information security measures implemented by the controller;
- international data transfers (including legal basis – eg, EU Model Contracts – for international data transfers to non-adequate countries outside the EU); and
- details of the contact person and signatory of the registration form.

After submitting the registration form, the controller is required to pay a registration fee of €25 for online registrations or €125 for paper registrations.

Registrations do not need to be renewed periodically, but they must be updated if their content is no longer accurate.

### 25 Penalties

**What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?**

Not complying with the registration obligation may lead to criminal fines ranging between €800 and €800,000. In case of recidivism, the controller may, in addition to a fine, be convicted to imprisonment of up to two years. The courts can also order the publication of their judgment in one or more newspapers, the confiscation of data storage media and the erasure of PII. In addition, the courts can prohibit the convicted person from managing any processing of PII for a period of up to two years.

### 26 Refusal of registration

**On what grounds may the supervisory authority refuse to allow an entry on the register?**

The Privacy Commission may refuse a registration if the information provided in the registration form is not complete or the registration fee has not been paid.

### 27 Public access

**Is the register publicly available? How can it be accessed?**

A public register is available online on the Privacy Commission's website (https://eloket.privacycommission.be/elg/searchPR.htm?eraseResults=true&siteLanguage=nl). This register is also available at the offices of the Privacy Commission and individuals can request an extract from the public register by letter.

### 28 Effect of registration

**Does an entry on the register have any specific legal effect?**

Controllers may initiate their PII processing activities as soon as the required registrations have been completed. Registrations as such do not exempt a controller from any of its other obligations under the Data Protection Act. Controllers need to ensure that their processing activities are in line with the submitted registrations (eg, only process

PII for the purposes identified in the registration) and should inform the Privacy Commission of any changes to the registered processing activities.

## Transfer and disclosure of PII

### 29 Transfer of PII

**How does the law regulate the transfer of PII to entities that provide outsourced processing services?**

When a controller outsources data processing activities to a third party (ie, a processor), it should put in place a (written or electronic) agreement with the processor that specifies:

- the technical and organisational information security measures to be implemented by the processor;
- the processor's liability towards the controller; and
- the processor's obligation to only process the PII in accordance with the controller's instructions.

### 30 Restrictions on disclosure

**Describe any specific restrictions on the disclosure of PII to other recipients.**

In general, there are no specific restrictions on the disclosure of PII other than the restrictions resulting from the general data protection principles (such as notice and purpose limitation). Health-related PII can, however, only be disclosed to health professionals (and their agents and assignees) bound by a secrecy obligation, unless the data subject has given his or her written consent for the disclosure or if the disclosure is necessary to prevent an imminent danger or to suppress a specific criminal offence. Furthermore, data subjects may submit a request to the President of the Court of First Instance to issue an injunction prohibiting the disclosure of PII.

### 31 Cross-border transfer

**Is the transfer of PII outside the jurisdiction restricted?**

PII can be transferred freely to other countries within the EEA, as well as to countries recognised by the European Commission as providing an 'adequate level of data protection' (see http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm for a list of countries deemed to be providing an adequate level of data protection).

Transferring PII to countries outside the EEA that are not recognised as providing an 'adequate level of data protection' is prohibited, unless:

- the data subject has unambiguously given his or her consent to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject;
- the transfer is necessary or legally required in light of the public interest, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is made from a register that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

In addition to the exemptions listed above, cross-border transfers to non-adequate countries can be authorised by the Minister of Justice (via Royal Decree) if the controller has implemented measures to ensure that the PII receives an adequate level of data protection and data subjects are able to exercise their rights after the PII has been transferred. Such measures include the execution of a data transfer agreement or implementation of binding corporate rules. Prior authorisation by the Minister of Justice is, however, not required if the controller has executed the standard contractual clauses approved by the European Commission.

### 32 Notification of cross-border transfer

**Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?**

In general, cross-border data transfers do not need to be notified to the Privacy Commission. However, if the controller is required to register its data processing activities with the Privacy Commission, any cross-border data transfers, as well as the legal grounds for transfers to countries not providing an adequate level of data protection, must be indicated in the registration.

As mentioned in question 31, prior authorisation by the Minister of Justice is required if the controller relies on binding corporate rules or an ad hoc data transfer agreement to legitimise the transfer of PII to non-adequate countries. Such authorisation is not required when the controller has guaranteed an adequate level of data protection by executing the standard contractual clauses approved by the European Commission. In the latter case, a copy of the executed standard contractual clauses must be submitted to the Privacy Commission for review.

### 33 Further transfer

**If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?**

The restrictions and authorisation requirements described in questions 31 and 32 apply regardless of whether PII is transferred to a service provider (ie, processor) or another controller.

The restrictions and requirements applicable to onward PII transfers depend on the legal regime in the jurisdiction where the data importer is located, unless the PII is transferred on the basis of the standard contractual clauses (which contain specific requirements for onward data transfers).

## Rights of individuals

### 34 Access

**Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.**

Data subjects have a right to 'access' the PII that a controller holds about them.

When a data subject exercises his or her right of access (by sending a signed and dated access request together with proof of his or her identity), the controller is required to provide the following information to the data subject:

- confirmation as to whether the controller processes the data subject's PII;
- the purposes for which his or her PII is processed;
- the nature and origin of the PII processed;
- the categories of individuals to whom his or her PII is or has been provided;
- the logic involved in any automated decision making (if any); and
- the existence of the right to object to the processing or request rectification or deleting of his or her PII, as well as the possibility to initiate a proceeding before the President of the Court of First Instance and to consult the public register of the Privacy Commission.

The controller should also provide the PII to the data subject in an intelligible form. This does not necessarily imply that the data subject is entitled to receive a copy of his or her PII or to have direct access to the file that contains his or her PII. Controllers can freely choose how they provide this information to the data subject.

Limitations to the right of access exist for PII processed:

- by certain public authorities, including police services and tax authorities;
- in the context of the application of anti-money laundering legislation;
- for journalistic, artistic or literary purposes, where providing access would compromise the intended publication or reveal information sources;
- in the medical file of a patient; and
- in the context of medical scientific research.

**Update and trends**

Both industry and the Privacy Commission are fully focused on preparing for the GDPR. Over the past year, the Privacy Commission has issued several guidance documents (including guidance on data inventories, Data Protection Officer designation and when to conduct Data Protection Impact Assessments), as well as a practical GDPR step plan and FAQs to help companies gear up for the GDPR.

The Privacy Commission is also in the process of being overhauled to ensure that in its new configuration it is properly equipped to take on its expanded role and powers under the GDPR.

### 35 Other rights

**Do individuals have other substantive rights?**

In addition to the right of access described above, data subjects have the following rights.

**Correction and deletion**
Data subjects are entitled to obtain, free of charge, the rectification of incorrect PII relating to them. Furthermore, data subjects have the right to request the erasure of or the prohibition to use all PII that is incomplete or irrelevant with a view to the purpose of the processing, or where the recording, disclosure or storage of the PII is prohibited, or where it has been stored for longer than the authorised period of time.

**Objection to processing**
Individuals have the right to object to the processing of their PII for substantial and legitimate reasons related to their particular situation, unless the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract, or compliance with a legal obligation to which the controller is subject. Data subjects are in any event (ie, without any specific justification) entitled to object to the processing of their PII for direct marketing purposes.

**Complaint to relevant supervisory authorities and enforce rights in court**
Data subjects are entitled to request the Privacy Commission to exercise their rights on their behalf. Furthermore, they can initiate proceedings before the President of the Court of First Instance when their rights have not been respected by the controller.

**Automated decision making**
Data subjects also 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 decision is taken in the context of an agreement or if it is based on a legal provision.

### 36 Compensation

**Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?**

Data subjects are entitled to receive compensation from controllers if they have suffered damages (including injury to feelings) as a result of a violation of the Data Protection Act. Controllers will only be exempt from liability under the Data Protection Act if they are able to prove that the facts that caused the damage cannot be ascribed to them.

### 37 Enforcement

**Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?**

The Privacy Commission can act as mediator between data subjects and controllers, and can address recommendations to controllers (with a view to ensuring the latter's compliance with the Data Protection Act), but it has no actual enforcement power. Enforcement of data subjects' rights is only possible through legal action before the courts.

## Exemptions, derogations and restrictions

### 38 Further exemptions and restrictions

**Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.**

No.

## Supervision

### 39 Judicial review

**Can PII owners appeal against orders of the supervisory authority to the courts?**

Controllers cannot appeal against the decisions of the Privacy Commission, as these are not legally binding.

## Specific data processing

### 40 Internet use

**Describe any rules on the use of 'cookies' or equivalent technology.**

In general, cookies or any other type of information can only be stored or accessed on individuals' equipment provided that the individuals have consented after having been informed about the purposes of such storage or access and their rights with regard to the processing of their PII. However, individuals' opt-in consent is not required if the access to or storage of information on their equipment is for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or strictly necessary to provide a service explicitly requested by the individual.

On 4 February 2015, the Privacy Commission issued practical guidance on the cookie consent requirements, which clarifies how companies should inform individuals about and obtain their consent for the use of cookies, as well as the types of cookies that are exempted from the consent requirement.

### 41 Electronic communications marketing

**Describe any rules on marketing by email, fax or telephone.**

Apart from the general rules on marketing practices and specific rules on marketing for certain products or services (eg, medicines and financial services), there are specific rules for marketing by email, fax and telephone.

**Marketing by electronic post**
Sending marketing messages by electronic post (eg, email or SMS) is only allowed with the prior, specific, free and informed consent of the addressee. However, provided that certain conditions are fulfilled, electronic marketing to legal persons and existing customers is exempt from the opt-in consent requirement. In any event, electronic marketing messages should inform the addressee about his or her right to opt out from receiving future electronic marketing and provide an appropriate means to exercise this right electronically. In addition to the consent requirement, Belgian law sets out specific requirements concerning the content of electronic marketing messages, such as the requirement that electronic marketing should be easily recognisable as such and should clearly identify the person on whose behalf it is sent.

**Marketing by automated calling systems and fax**
Direct marketing by automated calling systems (without human intervention) and fax also requires the addressees' prior, specific, free and informed consent. Furthermore, the addressee should be able to withdraw his or her consent at any time, free of charge and without any justification.

**Marketing by telephone**
Belgian law explicitly prohibits direct marketing by telephone to individuals who have registered their telephone number with the Do Not Call register.

**42 Cloud services**

**Describe any rules or regulator guidance on the use of cloud computing services.**

There are no specific rules on the use of cloud computing services under Belgian law. However, the Privacy Commission has issued advice (Advice No. 10/2016 of 24 February 2016 on the Use of Cloud Computing by Data Controllers) that identifies the privacy risks related to cloud computing services and provides guidelines for data controllers on how to comply with the Data Protection Act when relying on providers of cloud computing services.

Some of the risks identified by the Privacy Commission include:

- loss of control over the data owing to physical fragmentation;
- increased risk for access by foreign authorities;
- vendor lock-in;
- inadequate management of access rights;
- risks associated with the use of sub-processors;
- non-compliance with data retention restrictions;
- difficulties with accommodating data subjects' rights;
- unavailability of the services;
- difficulties with recovering data in case of termination of cloud provider's business or the service contract; and
- violations of data transfer restrictions.

To address these risks, the Privacy Commission has issued a number of guidelines for data controllers that want to migrate data to a cloud environment. The Privacy Commission recommends data controllers, among others, to:

- clearly identify data and data processing activities before migrating them to the cloud environment, taking into account the nature and sensitivity of the data;
- impose appropriate contractual and technical requirements on cloud providers (eg, not allowing cloud providers to alter terms and conditions unilaterally, requiring cloud providers to inform about the use of sub-processors and including exhaustive lists of physical locations where data can be stored);
- identify the most suitable cloud solution;
- perform a risk analysis (ideally by an independent body specialised in information security);
- select the appropriate cloud provider taking into account the risk analysis;
- inform data subjects about the migration of their PII to the cloud; and
- monitor changes to cloud services over time and update the risk analysis in light of such changes.

HUNTON& WILLIAMS

**Wim Nauwelaerts** **wnauwelaerts@hunton.com**
**David Dumont** **ddumont@hunton.com**

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 00
Fax: +32 2 643 58 22
www.hunton.com

*Getting the Deal Through*

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

*Also available digitally*

**Online**

www.gettingthedealthrough.com

Law Business Research

*Data Protection & Privacy*
*ISSN 2051-1280*

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

*Official Partner of the Latin American Corporate Counsel Association*

ABA Section of International Law
*Your Gateway to International Practice*

*Strategic Research Sponsor of the ABA Section of International Law*