



Data Protection & Privacy

in 21 jurisdictions worldwide

2013

Contributing editor: Rosemary P Jay



Published by *Getting the Deal Through*
in association with:

Adams & Adams

Arzinger

Bogsch & Partners Law Firm

Coelho Ribeiro e Associados

ELIG, Attorneys-at-Law

Foley & Lardner LLP

Gianni, Origoni, Grippo, Cappelli & Partners

Gilbert + Tobin Lawyers

Heenan Blaikie

Hoffmann Liebs Fritsch & Partner

Hogan Lovells (CIS)

Hunton & Williams

Ichay & Mullenex Avocats

Jayaram & Jayaram

Laux Lawyers, Attorneys-at-Law

Lorenz International Lawyers

MNKS

Nestor Nestor Diculescu Kingston Petersen

Attorneys & Counsellors

Olivares & Compañía SC

Preslmayr Rechtsanwälte

Yoon & Yang LLC



Data Protection & Privacy 2013

Contributing editor
Rosemary P Jay
Hunton & Williams

Business development managers
Alan Lee
George Ingledew
Robyn Hetherington
Dan White

Marketing manager
Alice Hazard

Marketing assistants
William Bentley
Zosia Demkowicz
Megan Friedman

Admin assistant
Cady Atkinson

Marketing manager (subscriptions)
Rachel Nurse
Subscriptions@
GettingTheDealThrough.com

Assistant editor
Adam Myers

Editorial assistant
Lydia Gerges

Senior production editor
Jonathan Cowie

Chief subeditor
Jonathan Allen

Subeditors
Joanne Morley
Charlotte Stretch

Editor-in-chief
Callum Campbell

Publisher
Richard Davey

Data Protection & Privacy 2013
Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910
© Law Business Research Ltd 2012
No photocopying: copyright licences
do not apply.
ISSN 2051-1280

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of September 2012, be advised that this is a developing area.

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

Law
Business
Research



Overview Rosemary P Jay <i>Hunton & Williams</i>	3
Australia Peter Leonard, Michael Burnett and Les Gray <i>Gilbert + Tobin Lawyers</i>	6
Austria Rainer Knyrim <i>Preslmayr Rechtsanwälte</i>	14
Belgium Jan Dhont, David Dumont and Jonathan Guzy <i>Lorenz International Lawyers</i>	20
Canada Adam Kardash, Joanna Fine and Bridget McIlveen <i>Heenan Blaikie</i>	28
France Annabelle Richard and Diane Mullenex <i>Ichay & Mullenex Avocats</i>	35
Germany Peter Huppertz <i>Hoffmann Liebs Fritsch & Partner</i>	42
Hungary Tamás Gödölle and Ádám Liber <i>Bogsch & Partners Law Firm</i>	49
India Malavika Jayaram <i>Jayaram & Jayaram</i>	57
Italy Daniele Vecchi and Melissa Marchese <i>Gianni, Origoni, Grippo, Cappelli & Partners</i>	68
Korea Wonil Kim and Kwang-Wook Lee <i>Yoon & Yang LLC</i>	75
Luxembourg Gary Cywie and Agnès Mongin-Weiss <i>MNKS</i>	81
Mexico Gustavo A Alcocer, Ricardo M Cadena and María Velasco <i>Olivares & Compañía SC</i>	88
Portugal Mónica Oliveira Costa <i>Coelho Ribeiro e Associados</i>	93
Romania Roxana Ionescu and Iurie Cojocar <i>Nestor Nestor Diculescu Kingston Petersen Attorneys & Counsellors</i>	100
Russia Ksenia Andreeva <i>Hogan Lovells (CIS)</i>	107
South Africa Danie Strachan and André Visser <i>Adams & Adams</i>	114
Switzerland Christian Laux <i>Laux Lawyers, Attorneys-at-Law</i>	122
Turkey Gönenç Gürkaynak, İlay Yılmaz, Gökhan Aydoğan <i>ELİG, Attorneys-at-Law</i>	129
Ukraine Oleksander Plotnikov and Oleksander Zadorozhnyy <i>Arzinger</i>	136
United Kingdom Rosemary P Jay, Tim Hickman and Naomi McBride <i>Hunton & Williams</i>	142
United States Peter F McLaughlin <i>Foley & Lardner LLP</i>	149

Belgium

Jan Dhont, David Dumont and Jonathan Guzy

Lorenz International Lawyers

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The Belgian Act of 8 December 1992 regarding the Protection of Privacy in relation to the Processing of Personal Data (the DPAct) and the Royal Decree of 13 February 2001 that executes the DPAct (the Royal Decree) constitute the primary legislative framework for data protection in Belgium. The DPAct implements Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data. Additionally, certain other laws provide provisions touching upon PII processing, such as the Electronic Communication Act of 13 June 2005 and the Act concerning Patients' Rights of 22 August 2002.

In addition to the national legal framework, the following international instruments apply in Belgium:

- article 8 of the European Convention on Human Rights and Fundamental Freedoms on the right to respect for private and family life, home and correspondence;
- article 8 of the Charter for Fundamental Rights of the European Union on the protection of personal data; and
- the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

2 Data protection authority

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

The Belgian Privacy Commission is responsible for ensuring compliance with the DPAct and any other applicable law relating to PII processing. The Privacy Commission is entrusted with the following primary tasks:

- issuing non-binding recommendations either on its own initiative or upon the request of the government or the parliament;
- maintaining a public register of notifications;
- handling complaints that are submitted to it, mediating between relevant parties and formulating non-binding recommendations; and
- instructing investigations and identifying breaches of the law for which it has wide powers, such as requiring: (i) communication of any document that may be of use to their investigation; and (ii) access to premises where information processing is believed to take place.

The Privacy Commission has no power to impose mandatory orders on PII owners, but it can submit a criminal complaint to the Public Prosecutor's Office for criminal breaches of the DPAct. Furthermore, the President of the Privacy Commission can also file a civil action before the Tribunal of First Instance for any dispute relating to the application of the DPAct.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

Criminal courts can impose penalties for breaches of the DPAct. The following criminal sanctions can be imposed: (i) a fine ranging from €600 to €600,000, (ii) imprisonment of up to two years, (iii) publishing of judgments in one or more newspapers, (iv) confiscation of filing systems, (v) orders to erase data, and (vi) a prohibition on processing any personal data for up to two years. In practice, the Privacy Commission will conduct investigations and if no settlement is obtained, the matter will be handed over to the Public Prosecutor's Office.

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 DPAct applies to all processing of PII, regardless of the sector or type of organisation; however, individuals processing data exclusively for private or household purposes (eg, keeping a personal address book) are excluded from the scope.

Furthermore, the DPAct contains partial exemptions for certain types of processing or organisations:

- organisations or individuals processing PII exclusively for journalistic, artistic or literary purposes, provided that (i) the data subject made the PII public, or (ii) the PII relates to the public character of the data subject or the fact in which the data subject is involved (eg, journalists collecting PII regarding public figures to write an article);
- certain public bodies, such as the state security service and the intelligence service;
- police authorities or other public authorities;
- PII processing that is necessary to comply with the obligations under applicable money laundering legislation; and
- processing performed by the European Centre for Missing and Sexually Abused 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 DPAct applies to the processing of PII resulting from the interception of communications, electronic marketing and the monitoring and surveillance of individuals.

Additionally, these activities are subject to specific regulations.

Interception of communication

- Articles 259-bis and 314-bis of the Belgian Criminal Code;
- article 124 et seq of the Electronic Communication Act of 13 June 2005;
- Act on the Methods of Data Collection of Intelligence and Security Services of 4 February 2010; and
- Collective Labour Agreement No. 81 on the Protection of Employees' Privacy in relation to the Monitoring of Electronic Online Communication Data of 26 April 2002.

Electronic marketing

- Article 100 of the Act on Market Practices and Consumer Protection of 6 April 2010;
- articles 13–15 of the Act on Certain Legal Aspects of Information Society Services of 11 March 2003; and
- Royal Decree regulating Advertising by Electronic Communications of 4 April 2003.

Monitoring and surveillance of individuals

- Act on the Installation and Use of Surveillance Cameras of 21 March 2007;
- Act concerning Special Tracing Methods and Any Other Investigation Methods of 6 January 2003; and
- Collective Labour Agreement No. 68 regarding the Protection of the Privacy with respect to Camera Surveillance at the Workplace of 16 June 1998.

6 Other laws

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

Credit information

- Act on Consumer Credit of 12 June 1991;
- Royal Decree on Processing of Personal Data on Consumer Credit of 20 November 1992; and
- Act concerning the Central of Credits to Individuals of 10 August 2001.

Health information

- Patient Rights Act of 22 August 2002.

7 PII formats

What forms of PII are covered by the law?

The DPAct covers all PII that is processed in an electronic record as well as in certain manual records (ie, structured sets of PII, accessible according to specific criteria, such as an alphabetical contact list in writing).

8 Extraterritoriality

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

No, the DPAct also applies to PII owners established outside the EU, using equipment for PII processing that is located on the Belgian ter-

ritory, unless such equipment is only used to transfer the PII through Belgian territory. This may, for instance, be the case if an electronic system physically located in Belgium is used to receive orders for goods, which is administered from outside the EU.

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 services to owners?

Yes, in principle, all processing or use of PII is covered by the DPAct (ie, all operations performed upon PII 'from cradle to grave' such as the creation, collection, recording, organisation, storage, alteration or destruction of PII).

The obligations that weigh on PII owners are of a different order than those weighing on data processing service providers. The DPAct imposes primarily obligations on PII owners, but the Act requires that service providers implement appropriate technical and organisational information security measures. In addition, PII owners are required to bind service providers, by means of a written agreement, to provide adequate information security and to ensure that the information is not processed outside the PII owner's control.

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? Give details.

Yes, any processing of PII must be legitimised on one of the following grounds:

- the data subject's unambiguous consent (ie, any freely, specific and informed indication of the data subject's agreement that its PII may be processed);
- for the performance of a contract to which the data subject is a party or for pre-contractual measures taken at his or her request;
- to comply with a legal obligation to which the PII owner is subject;
- to protect a vital interest of the data subject;
- for the performance of a task carried out in the public interest or in order to exercise an official authority vested in the PII owner or in a third party to whom the PII is disclosed; and
- to preserve the legitimate interests of the PII owner or a third party to whom the PII is disclosed, except where the interests or fundamental rights and freedoms of the data subject prevail.

However, the processing of certain specific types of PII is subject to more stringent requirements (see question 11).

11 Legitimate processing – types of data

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

Yes, the law imposes more stringent rules for specific types of PII.

The DPAct stipulates more stringent conditions for the processing of the following specific types of PII:

- sensitive PII (ie, PII revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning sex life);
- health-related PII; and
- PII relating to litigations submitted to civil, criminal and administrative courts, relating to suspicions, prosecutions or convictions in matters of criminal offences, administrative sanctions or security measures (judicial PII).

The processing of sensitive and health-related PII can take place if:

- the data subjects have given their written consent;
- it is necessary to comply with labour or social security law;
- the processing is necessary to protect the vital interests of the data subject or of another person, provided he or she is physically or legally incapable of giving consent;
- the PII has been manifestly made public by the data subject;
- it is necessary for the establishment, exercise or defence of a legal claim;
- it is done for the purpose of scientific research provided that certain conditions are satisfied;
- it is necessary for medical purposes provided that the PII is processed under the supervision of a health professional; and
- it is permitted by law for reasons of an important public interest.

In addition, sensitive PII may be processed:

- by a not-for-profit organisation in the course of its legitimate activities, provided strict conditions are met;
- for the purpose of public statistics; and
- by an organisation promoting the protection of human rights.

Moreover, health-related PII may also be processed if the processing is necessary for the prevention of a specific danger or the punishment of a particular criminal offence, or for the promotion and protection of public health.

Processing judicial PII is only permitted when performed:

- under the supervision of a public authority if the processing is necessary for the fulfilment of its duties;
- by other persons if the processing of PII is necessary for the achievement of objectives that have been laid down by the law;
- by legal or natural persons for the management of their own litigations;
- by legal counsel, if necessary for the defence of their clients; and
- for the purpose of scientific research provided that certain conditions are met.

When processing sensitive, health-related or judicial PII, the PII owner must keep a list of categories of individuals having access to it at the disposal of the Privacy Commission, and individuals with access must be bound by a legal, statutory or contractual confidentiality obligation.

Data handling responsibilities of owners of PII

12 Notification

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

Yes, PII owners are required to notify data subjects whose PII they process. If PII is obtained directly from a data subject, the following information should be provided to the data subject no later than the moment the PII is collected:

- the name and address of the PII owner;
- the purposes of the PII processing;
- the existence of a right to object if the PII is processed for direct marketing;
- categories of recipients of the PII;
- whether replies to the questions are obligatory and possible consequences of a failure to reply; and
- the existence of the right of access and rectification of PII.

If PII is not obtained directly from the data subject, the aforementioned information must be provided either at the time of the recording of the PII or, if the PII is intended to be disclosed to a third party, no later than the moment of such disclosure.

13 Exemption from notification

When is notice not required (for example, where to give notice would be disproportionate or would undermine another public interest)?

The PII owner is not required to give notice to data subjects who are already aware of the information contained in the notice.

If PII is not obtained directly from the data subject, the PII owner is not required to give notice if the recording or communication of PII is required by law, or if such notification appears to be impossible or involves a disproportionate effort.

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?

Yes, the DPAct requires PII owners to provide data subjects a certain degree of choice and control over the PII processing.

Right to object

Data subjects must be offered the possibility to object to the processing of their PII for serious and legitimate reasons relating to his or her particular situation. Data subjects are not able to object to PII processing necessary for:

- the performance of a contract to which the data subject is a party or for pre-contractual measures taken at the request of the data subject; or
- compliance with a legal obligation to which the PII owner is subject.

Furthermore, if the PII is processed for direct marketing purposes, the data subject always has the right to object to such processing (opt out).

Automated decision-making

Data subjects have the right not to be subject to an automated decision-making process that has legal effects (or affects them seriously) and which is aimed at the evaluation of certain aspects of their personality, such as professional performance, credit reliability, etc. However, this prohibition does not apply if the automated decision is taken in the context of an agreement or if it is necessary to comply with a legal obligation.

15 Data accuracy

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

Yes, but the DPAct only imposes vague standards for the quality, currency and accuracy of PII.

Generally, a PII owner is required to ensure that the PII is accurate and kept up to date. Therefore, the PII owner must:

- take all reasonable steps to ensure that inaccurate or incomplete PII is erased or rectified; and
- implement technical and organisational measures that prevent any unauthorised alteration of PII.

Furthermore, the data subject has the right to request the rectification or deletion of inaccurate PII. The PII will only be erased or corrected to the extent that:

- the PII is incomplete, not necessary or irrelevant in view of the purpose of the processing;
- the recording, communication or storage is prohibited; or
- the PII has been stored for longer than the authorised retention period.

The PII owner has one month to rectify or erase the PII on receipt of the data subject's request.

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?

Yes, the PII owner may only process PII that is adequate, relevant and not excessive in light of the processing purposes. Furthermore, PII can only be kept in an identifiable format as long as needed for such purposes.

The statute of limitation periods for civil (up to 30 years) or criminal (up to 10 years) claims are relevant indicators to determine retention practices.

17 Finality principle

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

Yes, the DPAct has adopted the finality principle, which implies that PII may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The DPAct does not further specify what specific data processing purposes are deemed legitimate. The guidance to the Privacy Commission's registration tool, however, contains a lengthy list of processing purposes that it considers legitimate (including purposes such as 'sales of personal information' and other privacy-invasive data processing practices) (see www.privacycommission.be/sites/privacycommission/files/documents/01.01.03.22-notice_decl_ordinaire_0.pdf).

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?

The DPAct allows PII owners to use PII for new (different) purposes as long as the new processing remains compatible with the purposes originally specified. All relevant factors should be taken into account, in particular the reasonable expectations of the data subject and the applicable legal and regulatory provisions to assess whether processing for a new processing purpose is acceptable.

It should be noted that further processing of PII for historical, statistical or scientific purposes is allowed under the conditions stipulated in the Royal Decree (primarily, providing for de-identification).

Security obligations

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

The DPAct imposes obligations on the PII owner to implement appropriate, organisational and technical information security measures to protect PII against accidental or unlawful destruction, accidental loss, and unauthorised amendment or access. These measures must guarantee an adequate security level taking into account the costs for implementing the measures and the current state of the art in the field of information security on the one hand, and the nature of the PII and the potential privacy risks on the other hand.

To clarify these obligations, the Privacy Commission elaborated a list of reference security measures (see www.privacycommission.be/sites/privacycommission/files/documents/01.01.04.06-mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf).

When implementing these measures, the PII owner must assess the need for information security, taking into account:

- the nature of the PII and the processing activities, as well as the integrity, confidentiality and the availability of the PII;
- the applicable legal and regulatory requirements;
- the size of the entity (including the number of individuals having access to the PII);
- the significance and complexity of the IT-systems and software;
- the level of external access;
- the privacy risks; and
- the state of the art of information security technologies.

Furthermore, a PII owner is also required to carefully select and supervise providers that process PII on their behalf.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

There are no specific security breach requirements in the DPAct. However, prudence requires that notification be considered if potential harm will result to data subjects' privacy if notification was not made. In such cases, lack of notification of individuals may trigger liability based on Belgian tort law.

Under the recently amended Act on Electronic Communication of 13 June 2005, telecom operators are required to inform the Belgian Institute for Postal Services and Telecommunications (Telecom Regulator) of security breaches that affect PII. If the security breach is likely to negatively affect PII and the privacy of the concerned users, telecom operators are also required to inform these users, unless the PII owner can demonstrate to the Telecom Regulator that the affected PII is sufficiently protected by information security measures that make the PII unreadable for unauthorised individuals. The information security breach notification to users must contain at least the following information: (i) the nature of the security breach; (ii) contact information for individuals who want to obtain more information regarding the breach; and (iii) recommended measures that individuals can take to limit the negative consequences of the breach. Furthermore, the information security breach notification towards the Telecom Regulator should also contain a description of the consequences of such breach and the measures that the company took or is planning to take to address it.

Internal controls

21 Data protection officer

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

No, the appointment of a data protection officer is not mandatory under Belgian law nor is it contemplated in the DPAct. There are no specific legal advantages (eg, an exemption on the notification obligation) related to the appointment of a data protection officer. Nevertheless, the internal appointment of such officer tends to increase the credibility of an organisation in the eyes of the Privacy Commission.

22 Record keeping

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

There is no specific legal obligation to keep internal records or documentation regarding PII processing; however, in case a PII owner is processing sensitive PII, it should keep a list of all the categories of individuals who are authorised to access this data. The list must con-

tain a specific description of the functions of these individuals with regard to the processing of PII and should be kept at the disposal of the Privacy Commission.

Registration and notification

23 Registration

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

Yes. PII owners are required to notify the processing of PII to the Privacy Commission by default. Entities that are only processing PII on behalf of another entity (ie, data processors) are not subject to this obligation.

The Royal Decree provides exemptions to the general notification obligation. It exempts PII processing performed for certain specific purposes, such as payroll, HR, client and supplier management, accounting, management of shareholder and partners, enabling communication, and visitor registration in relation to access control. Also, the Royal Decree exempts certain types of PII owners from the obligation to notify, such as non-profit organisations for processing PII of their members and benefactors, educational institutions (for processing PII of their students), municipalities processing PII in order to maintain the register of the population and identity cards, and administrative bodies processing PII in accordance with a specific act or regulation.

All these exemptions are conditioned and should be interpreted strictly, since the general rule is notification.

24 Formalities

What are the formalities for registration?

PII owners can register by:

- completing the online notification form on the website of the Privacy Commission (see <https://www.privacycommission.be/elg/main.htm?siteLanguage=nl>); or
- sending a written notification form (available at www.privacycommission.be/nl/static/pdf/gewone_aangifte_form.pdf) to the Privacy Commission (Rue de la Presse, 35/Drukpersstraat 35, 1000 Brussels, Belgium).

The notification form should include information on:

- the PII owner (name and corporate address);
- the purposes of the processing;
- the types of PII that are being processed;
- the legal basis for the processing;
- data recipients and the measures implemented to secure the disclosure of PII to these third parties;
- how the concerned data subjects are being informed about the PII processing;
- the person or department that data subjects can contact to exercise their rights;
- the PII retention period;
- implemented information security and confidentiality measures;
- international data transfers; and
- the contact person for the Privacy Commission.

After completing the online notification procedure, the PII owner will receive an authentication form. This form should be printed, signed and sent by (registered) mail to the Privacy Commission. It is only after receiving this authentication form that the Privacy Commission will consider the notification as officially submitted.

The Privacy Commission will send a confirmation letter within three working days of receipt of the written notification or the authentication form. The notification will then be processed and published in the public register of the Privacy Commission. This

normally occurs within 21 days of completing the notification procedure. The PII owner can start its processing activities once the notification is submitted and does not have to wait until its notification has been published; however, it is possible that the Privacy Commission may request additional information or raise concerns regarding the intended processing when reviewing the notification form.

The PII owner must pay a fee of €125 (if the notification is sent in writing) or €25 (in case the notification is submitted online).

The registration does not have to be renewed periodically, but it must be kept up to date. This implies that it must be amended where the notified information is no longer accurate. Amendments can be done in writing or online and are subject to a fee of €20.

25 Penalties

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

A PII owner who does not comply with its notification obligation can be convicted by a court to criminal fines ranging from €600 to €600,000. Furthermore, the court can order the publication of the decision in one or more newspapers, the confiscation of the data storage media, or the erasure of PII. The court can also prohibit the convicted person to process any PII for a maximum period of two years. In addition, in case of recidivism, the court can impose a sentence of three months up to two years' imprisonment or a criminal fine of between €600 and €600,000, or both.

26 Refusal of registration

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

The Privacy Commission may refuse entry in the public register if the notification is incomplete or if the PII owner fails to pay the notification fee; however, the Privacy Commission may not refuse an entry to its public register based on the notified processing activities of the PII owner.

27 Public access

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

The register is publicly available free of charge and can be accessed online on the website of the Privacy Commission (see <https://eloket.privacycommission.be/elg/searchPR.htm?eraseResults=true&siteLanguage=nl>), at the Privacy Commission's Office, or by sending a written access request to the Privacy Commission.

28 Effect of registration

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

The notification of PII processing and the registration in the public register do not exempt the PII owner from its other obligations under the DPAct. It is important that notice provided to individuals is in line with the registration. Also, changes in the information practices should be reflected in the public register.

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?

A written (or electronic) agreement should be concluded between the PII owner and the data processor. The agreement should determine:

- that the data processor can only act on behalf of the PII owner

- and pursuant to its instructions; and
- the data processor's liability in case of failure to comply with its obligations (ie, implementation of information security measures and compliance with the DPAAct).

In any event, the PII owner remains liable for the PII processing performed by a data processor and is required to carefully select its data processor.

30 Restrictions on disclosure

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

It is the PII owner's responsibility to ensure that the disclosure is consistent with the initial purpose of processing and notice is provided to the data subjects. The DPAAct does not further restrict the communication of PII to third parties.

However, the disclosure of health-related PII is restricted. Health-related PII can only be disclosed to another health-care professional bound by professional secrecy, unless the data subject gives his or her written consent, or if the processing is necessary for the prevention of an imminent danger or for the suppression of a criminal offence.

Furthermore, a data subject may ask the president of the Tribunal of First Instance to issue an injunction prohibiting the disclosure of PII where disclosure is not permitted.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Transfers of PII outside Belgium to other EEA countries are not restricted, but PII transfers outside the EEA are.

Transfers to adequate countries

Transfers of PII to EEA countries and countries that the European Commission has found to provide an 'adequate level of protection' are not restricted. The European Commission has adopted a white list of countries with an adequate level of protection (see http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm), which is recognised by the Belgian Privacy Commission.

Transfers to non-adequate countries

Transfers to countries outside the EEA not providing an adequate level of protection are prohibited unless the international data transfer is:

- based on the data subject's unambiguous consent;
- necessary for the execution of a contract between the data subject and the PII owner, or for actions necessary to implement pre-contractual measures at the data subject's request;
- necessary for the conclusion or execution of a contract between a PII owner and a third party in the data subject's interests;
- necessary for an important public interest, or for the establishment, exercise or defence of legal claims;
- necessary to protect a vital interest of the data subject; and
- carried out from a public register set up by law or from a register that can be consulted by anyone invoking a legitimate interest, provided that the legal requirements for consultation are met.

Furthermore, specific PII transfers to non-adequate countries can be authorised by the minister of justice, provided that the PII owner ensures 'sufficient guarantees' for the protection (eg, by concluding a data transfer agreement with appropriate clauses or adopting binding corporate rules (BCRs)); the authorisation will be given in the form of a Royal Decree. If the European Commission-approved model clauses are used, such an authorisation is not required in practice.

Belgium recognises the mutual recognition procedure for the approval of BCRs. The procedure provides that a lead data protection authority will review a company's BCRs. If the lead authority accepts the BCRs, the Privacy Commission will advise the minister of justice to authorise the BCRs.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

No, generally the international transfer of PII does not require specific notification or authorisation from the Privacy Commission or another supervisory authority.

However, if PII transfers to third countries fall outside the exemptions on the previously mentioned general international data transfer prohibition, the PII owner must apply for an authorisation from the minister of justice.

If a PII owner executes a data transfer agreement to a non-adequate country based on the European Commission's standard contractual clauses, such an agreement is automatically considered to provide a sufficient guarantee by the Privacy Commission. Therefore, in practice, prior authorisation by the minister of justice is not required in this case; however, a copy of this data transfer agreement must be sent to the Privacy Commission for review.

In any event, international transfers (and the legal basis for transfer) must be indicated on the mandatory notification which must be submitted to the Privacy Commission prior to the PII processing.

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?

In those exceptional cases where an authorisation of the Ministry of Justice is required (typically, in case of ad hoc data transfer agreements), onward transfers must be included in the transfer permit application if they take place on the initiative of the Belgium-based data exporter. International transfers that are initiated by the third country-based data importer (without involvement of the Belgium-based data exporter) are not subject to the authorisation process.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

Yes, data subjects have the right to access their PII. This right of access implies that the data subject is entitled:

- to be informed whether his or her PII are being processed;
- if PII is being processed, to receive a description of the:
 - PII of which the data subject is the subject;
 - processing purposes;
 - data categories to which the processing relates;
 - recipients or categories of recipients to whom the data are or may be disclosed; and
 - information about the origin of the data; and
- to receive the aforementioned information in an intelligible form. According to the Privacy Commission, this does not imply that a copy of the processed PII, or that the file of which the PII forms part should be provided to the data subject.

Data subjects should address a dated and signed access request to the PII owner or processor together with proof of their identity.

Update and trends

The Privacy Commission recently published a non-binding recommendation regarding cyber surveillance in the employment context. The most important point from this recommendation is that the Privacy Commission allows employers to access the content of employees' non-contested business-related e-mails if access is required for legitimate purposes (eg, the employee is ill or on leave).

The Belgian parliament recently adopted the Law with Various Provisions regarding Electronic Communications (the Law), which implements Directive 2009/136/EC (amending the E-Privacy Directive

2002/58/EC). The Law contains several provisions concerning the protection of PII, which include, most notably, the introduction of an opt-in consent requirement for cookies and the introduction of a specific data breach notification obligation for telecom operators.

The Privacy Commission recently released a protocol with the Ministry of Justice which simplifies, under Belgian law, the authorisation procedure for BCRs. While a Royal decree will still be required to authorise BCRs, the protocol facilitates the procedure for having BCRs approved under Belgian law.

When receiving a valid access request, access must be provided free of charge, as soon as possible and at least within 45 days of receipt of the request.

The right to access does not apply if:

- PII is processed by public authorities in the fulfilment of their duties of judicial police;
- PII is processed by certain police services;
- processing is necessary for the application of the law on the prevention of money laundering; and
- PII is processed exclusively for journalistic, artistic or literary purposes, provided that the execution of this right would compromise a publication or reveal information sources.

In this case, data subjects cannot request access directly from the PII owner, but can obtain access via a request addressed to the Privacy Commission.

The DPAct and the Act on Patients' Rights of 22 August 2002 contain a specific regime for access to medical data.

35 Other rights

Do individuals have other substantive rights?

In addition to the right of access, data subjects have the right to request the rectification, erasure or blocking of inaccurate PII or PII that is processed in violation of the DPAct (see question 15). Further, individuals also have the right to object to the processing of their PII (see question 14).

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 compensation from the PII owner if they suffer damages resulting from a violation of the DPAct. The PII owner will only be exempted from this liability when it proves that it cannot be held accountable for the violation of the DPAct.

37 Enforcement

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

The Privacy Commission has a mediating role regarding the enforcement of these rights, but actual enforcement is only possible through the judicial system. For more information on the Privacy Commission's powers please see question 2.

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 data owners appeal against orders of the supervisory authority to the courts?

It is not possible to appeal against a decision of the Privacy Commission since it cannot impose binding decisions.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

The processing of PII in violation of the DPAct may constitute a criminal offence subject to criminal sanctions.

The following criminal offences are punishable by a fine ranging from €600 to €120,000:

- failure to comply with a valid request for rectification, blocking or erasure of PII; and
- failure to comply with implementing adequate technical and organisational measures.

The following criminal offences are punishable by a fine ranging from €600 to €600,000:

- failure to comply with the general data protection principles;
- failure to comply with the rules on legitimate PII processing;
- failure to comply with the rules on the processing of sensitive PII;
- failure to comply with rules regarding the information to be provided to the data subject;
- failure to communicate the information requested by the data subject within 45 days of receipt of the request, or knowingly communicating inaccurate or incomplete data;
- providing incomplete or inaccurate information in the notification of a data processing operation to the Privacy Commission (or generally abstaining from notifying the Privacy Commission);
- failure to comply with a request for information of the Privacy Commission; and
- transferring PII to a country outside the EEA contrary to the applicable rules.

In addition, the following measures can be imposed by court order:

- confiscation of the carriers of PII to which the offence relates;
- erasure of the PII; and
- prohibition of the management of any processing of PII, directly or through an agent, for a period of up to two years.

Recidivism is punishable by imprisonment from three months up to two years, a fine ranging from €600 to €600,000, or both.

41 Internet use

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

The use of cookies is regulated by article 129 of Electronic Communication Act of 13 June 2005, which was recently amended.

This law requires:

- consent to be obtained from users prior to the placing or use of cookies;
- data subjects to be informed of the use of cookies; and
- data subjects to be offered the chance to withdraw consent in a clear and unambiguous way.

These conditions do not apply if the cookie is strictly necessary:

- for the provision of a service explicitly requested by the user; and
- for the transmission of a communication over an electronic communication network.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Marketing by e-mail

The consent of the addressee is required before sending marketing by e-mail, unless if the marketing is sent to:

- a generic email address of a legal person (eg, info@company.be);
- a customer, provided that (i) the marketer has collected the email address in relation the sale of products or services, (ii) the marketing relates to similar products or services, and (iii) the customer is offered an easy way to opt out.

Marketing by telephone

Marketing calls to individuals who opted out of these calls are prohibited.

The Belgian Direct Marketing Association has established a list ('the Robinson list') to enable individuals to exercise their rights of objection.

Marketing by facsimile

The consent of the addressee is required prior to sending direct marketing by facsimile.

LORENZ

International Lawyers

Jan Dhont
David Dumont
Jonathan Guzy

j.dhont@lorenz-law.com
d.dumont@lorenz-law.com
j.guzy@lorenz-law.com

Regentlaan 37-40 Bld du Régent
1000 Brussels
Belgium

Tel: +32 239 2000
Fax: +32 2 239 2002
www.lorenz-law.com

GETTING THE DEAL THROUGH

Annual volumes published on:

Air Transport	Licensing
Anti-Corruption Regulation	Life Sciences
Anti-Money Laundering	Merger Control
Arbitration	Mergers & Acquisitions
Banking Regulation	Mining
Cartel Regulation	Oil Regulation
Climate Regulation	Patents
Construction	Pharmaceutical Antitrust
Copyright	Private Antitrust Litigation
Corporate Governance	Private Equity
Corporate Immigration	Product Liability
Dispute Resolution	Product Recall
Dominance	Project Finance
e-Commerce	Public Procurement
Electricity Regulation	Real Estate
Enforcement of Foreign Judgments	Restructuring & Insolvency
Environment	Right of Publicity
Foreign Investment Review	Securities Finance
Franchise	Shipbuilding
Gas Regulation	Shipping
Insurance & Reinsurance	Tax on Inbound Investment
Intellectual Property & Antitrust	Telecoms and Media
Labour & Employment	Trademarks
	Vertical Agreements



For more information or to purchase books, please visit:
www.GettingTheDealThrough.com



Strategic research partners of
the ABA International section



THE QUEEN'S AWARDS
FOR ENTERPRISE:
2012



The Official Research Partner of
the International Bar Association