GETTING THE DEAL THROUGH

Data Protection & Privacy

in 26 jurisdictions worldwide

2014

Contributing editor: Rosemary P Jay

Published by
Getting the Deal Through
in association with:

Adams & Adams

Arzinger

Coelho Ribeiro e Associados

Com advokatbyrå

Drew & Napier LLC

ELIG, Attorneys-at-Law

Gilbert + Tobin

Heenan Blaikie LLP

Hoffmann Liebs Fritsch & Partner

Hunton & Williams LLP

Ichay & Mullenex Avocats

Iriarte & Asociados

Jayaram & Jayaram

Laux Lawyers, Attorneys-at-Law

Lee and Li, Attorneys-at-Law

Lexing Spain

Lorenz International Lawyers

Matheson

MNKS

Nagashima Ohno & Tsunematsu

Olivares & Cia

Panetta & Associati Studio Legale

Pinheiro Neto Advogados

Preslmayr Rechtsanwälte OG

Yoon & Yang LLC

GETTING THE DEAL THROUGH

Data Protection & Privacy 2014

Contributing editor
Rosemary P Jay
Hunton & Williams

Publisher
Gideon Roberton

Business development managers
Alan Lee
George Ingledew
Dan White

Account manager
Megan Friedman

Trainee account managers
Cady Atkinson, Joseph Rush, Dominique Destrée and Emma Chowdhury

Media coordinator
Parween Bains

Administrative coordinator
Sophie Hickey

Trainee research coordinator
Robin Synnot

Marketing manager (subscriptions)
Rachel Nurse
subscriptions@gettingthedealthrough.com

Head of editorial production
Adam Myers

Production coordinator
Lydia Gerges

Senior production editor
Jonathan Cowie

Subeditor
Davet Hyland

Director
Callum Campbell

Managing director
Richard Davey

Data Protection & Privacy 2014
Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2012
Second edition

ISSN 2051-1280

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

Law Business Research

CONTENTS

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 Data Protection 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 also 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 on the Protection of Privacy and Transborder Flows 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 or upon the request of the government or the parliament;
- maintaining a public register with the notifications that PII-owners must submit prior to commencing any processing of PII (unless an exemption applies);
- reviewing all complaints that are submitted, 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, among other things:
  - communication of any document that may be of use for their investigation; and
  - access to premises where information processing is believed to take place.

The Privacy Commission has no power to impose mandatory orders on PII owners. However, 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 criminal penalties for breaches of the DPAct. The following criminal sanctions can be imposed:

- a fine ranging from €600 to €600,000;
- imprisonment for up to two years;
- publishing judgments in a newspaper;
- confiscation of filing systems;
- orders to erase data; and
- a prohibition on using 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:
  - the data subject made the PII public; or
  - 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;
- processing PII which is necessary to comply with the obligations under applicable money laundering legislation; and
- processing performed by 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, the following activities are subject to further specific regulations:

Interception of communication

- Articles 259-bis and 314-bis of the Belgian Criminal Code;
- Article 124 and following 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;
- Collective Labour Agreement No. 68 regarding the Protection of the Privacy with respect to Camera Surveillance at the Workplace of 16 June 1998; and
- Recommendation of the Privacy Commission regarding cyber-surveillance in the employment context (August 2012).

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 Law 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 set of PII, which is accessible according to specific criteria, such as an alphabetic 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 European Union that use equipment for PII processing located on Belgian territory, unless this equipment is only used to transfer the PII through Belgian territory. This may, for instance, be the case if an electronic system is used to receive orders for goods that are physically located in Belgium but administered from outside the European Union.

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 are 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. However, 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 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 and informed indication (defined broadly) 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 or trade-union membership, and data concerning an individual's 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, physically or legally incapable of giving his or her 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 non-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 defence 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; and
- necessary for the promotion and protection of public health.

Processing judicial PII is only permitted in the following cases:
- 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 individuals having access to it at the disposal of the Privacy Commission, and individuals having access to it 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?

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 purpose(s) 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, notice is not required if:
- the recording or communication of PII is required by law; or
- the requirement of 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 if based on a serious and legitimate ground. Data subjects do not have the possibility to object to processing 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;
- compliance with a legal obligation to which the PII owner is subject; or
- protecting the data subject's vital interests.

Furthermore, if the PII are 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 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, however, the DPAct only imposes a vague standard 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 which 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
- 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. This obligation is subject to a test of reasonableness.

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 in specific cases.

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 that 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. However, the guidance to the Privacy Commission's registration tool contains a lengthy list of processing purposes which it considers legitimate (including purposes such as 'sale of personal information' and other intensive 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 consistent with the purposes that were 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 for 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 risks on the other hand.

To clarify these obligations and as a consequence of recent data breach cases, the Privacy Commission has published a recommendation on security measures to be taken to avoid security breaches (January 2013) (www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf) and has developed a list of reference security measures (www.privacycommission.be/sites/privacycommission/files/documents/lignes_directrices_securite_de_l_information_0.pdf).

When implementing these measures, the PII owner must assess the needs 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 amount 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 data processors 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, in its recommendation on dealing with information security breaches (January 2013), the Privacy Commission insists that such breaches be notified within 48 hours to the Privacy Commission and that a public information campaign be undertaken within 24 to 48 hours thereafter. In such cases, lack of notification of individuals may trigger liability based on Belgian tort law.

In addition, the amended Act on Electronic Communication of 13 June 2005 introduces a data breach notification obligation for providers of public electronic communication services (ie, services that mainly consist of transferring signals over an electronic communication network). This implies that these providers are now required to immediately report any kind of security breach effecting PII to the Belgian Institute for Postal Services and Telecommunications (BIPT). Furthermore, if the data breach is likely to negatively affect personal data and the privacy of clients or other individuals, these individuals should also be informed without delay, unless the company can demonstrate to the BIPT that the affected PII is protected by information security measures, which render the data incomprehensible for unauthorised third parties (eg, encryption techniques). Data breach notices to individuals should contain information on the nature of the data breach, the persons or services that individuals can contact for more information, as well as the measures which individuals can take to mitigate the negative effects of the data breach. In addition, the data breach notification to the BIPT should contain a description of the consequences of the data breach and the actions which the company intends to take or has already taken to address the data breach. In practice, companies subject to the data breach notification obligations should anticipate potential data breaches, for example by preparing operating procedures and notification templates which are ready to use, since the BIPT and the concerned individuals should be notified without delay. Furthermore, it is also required to keep a register of the data breaches containing information on data breach facts and the consequences and the measures taken to address the incident.

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 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 a data protection officer tends to increase the credibility of an organisation in the Privacy Commission's eyes.

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 contain 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, if they are 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 (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.

The notification form should include:

- the PII owner, such as its name and corporate address;
- the purposes of the processing;
- the categories of PII which 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;
- information on the PII retention period;
- implemented information security and confidentiality measures;
- international data transfers; and
- a contact person for the Privacy Commission.

After completing the online notification procedure, the PII owner will receive an authentication form. This authentication 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 after receiving the written notification or the authentication form of the electronic notification. The notification will then be processed and published in the public register of the Privacy Commission. This normally occurs within 21 days after 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 requests additional information or raises 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; however it must be kept up to date. This implies that it must be amended in case 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 between three months and two years of 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 (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 provide that:

- the data processor can only act on behalf of the PII owner and pursuant to its instructions; and
- the data processor's liability is determined in case of failure to comply with its obligations (ie, implementation of information security measures and compliance with the DPAct).

Regardless, 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 DPAct 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. However, PII transfers outside of the EEA countries are subject to more stringent restrictions.

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 having an adequate level of protection (this list is available at http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm), which is followed 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 which can be consulted by anyone who can invoke 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 EU 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 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 other supervisory authority.

However, if PII transfers to third countries outside the exemptions on the general international data transfer prohibition (as mentioned in 'Transfers to non-adequate countries' in question 31), 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. This process has been confirmed by a Privacy Commission decision in July 2013.

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

Update and trends

The Privacy Commission recently published a non-binding recommendation regarding cyber-surveillance in the employment context (August 2012), which aims at clarifying the Belgian rules governing access to the content of e-communications at work. The most important trend from this recommendation is that the Privacy Commission opines that the Belgian framework provides a sufficient legal basis to access non-contested business-related e-communication content if the access is performed for legitimate purposes (eg, the employee is sick or on leave).

The Privacy Commission recently published a recommendation on security measures to be taken to avoid security breaches (January 2013), which offers general measures and guidelines on information security of PII. In addition, the recommendation insists that data breaches be notified to the Privacy Commission.

The Privacy Commission issued an updated recommendation on direct marketing (February 2013). The recommendation describes the procedure that companies should follow to perform direct marketing.

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 classes of recipients to whom the data are or may be disclosed; and
  - information about the origin of the data; and
- to receive the above-mentioned information in an intelligible form. According to the Privacy Commission, this does not imply that a copy of the processed PII, or the file of which the PII forms part should be provided.

Data subjects should address a dated and signed access request to the PII owner or processor together with proof of their identity. When receiving a valid access request, access must be provided free of charge, as soon as possible and at least within 45 days after receipt of the request.

The right to access does not apply if:

- PII is processed by public authorities in the fulfilment of the duties of the 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 which is processed in violation of the DPAct (see question 15 above). 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. However, 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 of between €600 and €600,000:

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

The following criminal offences are punishable by a fine of between €600 and €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 individual;
- failure to communicate the information requested by the individual 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 for between three months and two years, and a fine of between €600 and €600,000, or one of these sanctions alone.

41 Internet use

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

The use of cookies is regulated by article 129 of the Electronic Communication Act of 13 June 2005, which was recently amended. The amendment entered into force on 1 October 2012 and requires companies to obtain the user's opt-in consent and inform the data subject of the use of cookies, unless the cookie is strictly necessary to transmit communication over an electronic communication network or to provide services explicitly requested by the user. Furthermore, users must always have the opportunity to withdraw their consent easily and free of charge. In practice, this implies that companies using cookies will have to redesign their websites in a way that the user's consent can be obtained prior to installing any cookie – where the cookie use does not fall within one of the above-mentioned exemptions. This may be done, for example, by implementing a banner or pop-up message requiring users to tick a box to indicate their consent to the use of cookies. Furthermore, a practical procedure needs to be implemented for users who want to withdraw their consent.

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 e-mail address of a legal person (eg, info@company.be);
- a customer, provided that:
  - the marketer has collected the e-mail address in relation to the sale of products or services;
  - the marketing relates to similar products or services; and
  - 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 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 **j.dhont@lorenz-law.com**
David Dumont **d.dumont@lorenz-law.com**
Jonathan Guzy **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