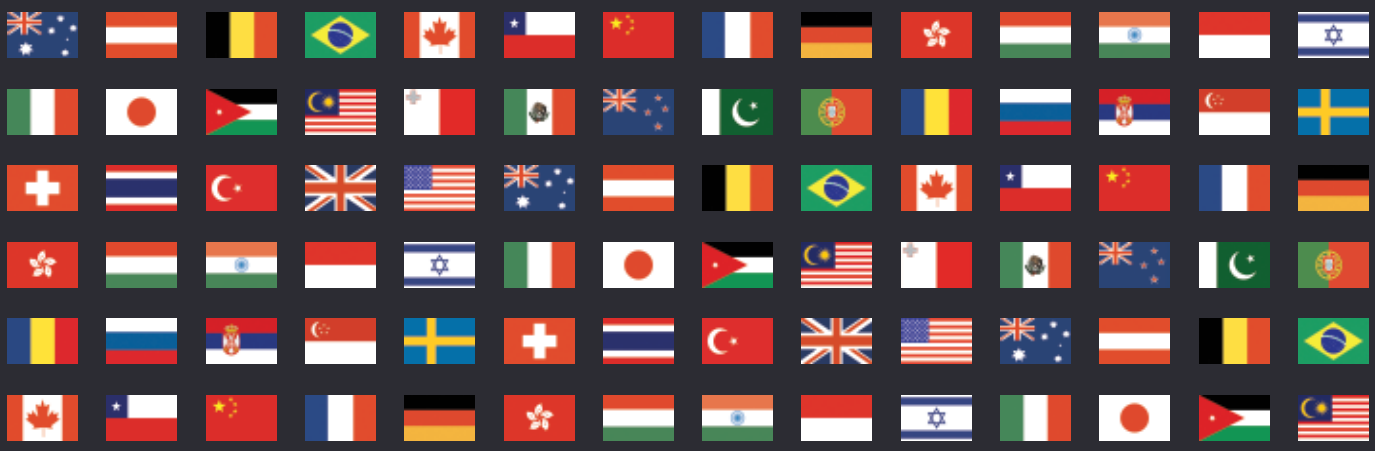
Data Protection & Privacy 2022

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

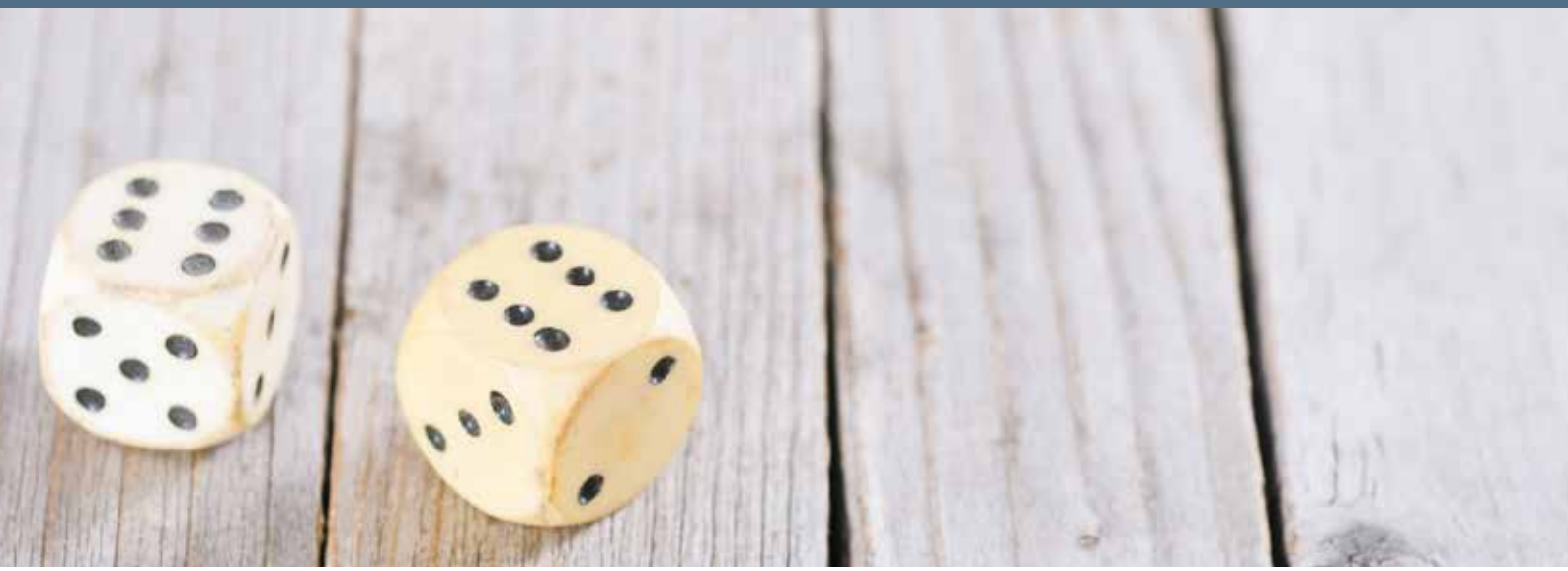


LEXOLOGY
Getting The Deal Through

HUNTON
ANDREWS KURTH

HUNTON
ANDREWS KURTH

Leaders in Handling High-Stakes Cybersecurity Events



Luck is not a strategy.

Increase your company's resilience and responsiveness to cyber attacks.

Hunton Andrews Kurth LLP's privacy and cybersecurity practice assists global organizations in managing data through every step of the information life cycle. We help businesses prepare for and respond to cybersecurity incidents all over the world. The firm is ranked as a top law firm globally for privacy and data security.

For more information, visit www.huntonprivacyblog.com.

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Tenth edition
ISBN 978-1-83862-644-0

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

Data Protection & Privacy

2022

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the tenth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Jordan, Pakistan and Thailand.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

Belgium

David Dumont and Laura Léonard

Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

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

Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) became directly applicable in Belgium on 25 May 2018.

In the context of this important evolution of the legal framework, the Belgian data protection supervisory authority (formerly called the Commission for the Protection of Privacy) was reformed by the Act of 3 December 2017 creating the Data Protection Authority (DPA). This reform was necessary to enable the DPA to fulfil the tasks and exercise the powers of a supervisory authority under the GDPR.

On 5 September 2018, the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act) was published in the Belgian Official Gazette. The Data Protection Act addresses the areas where the GDPR leaves room for EU member states to adopt country specific rules and implements Directive (EU) 2016/680 (the Law Enforcement Directive). The Data Protection Act replaced the Act on the Protection of Privacy concerning the Processing of Personal Data of 8 December 1992.

This chapter mainly focuses on the legislative data protection framework for private sector companies and does not address the specific regime for the processing of PII by police and criminal justice authorities in detail. The responses reflect the requirements set forth by the GDPR and the Data Protection Act.

In addition to the GDPR, several international instruments on privacy and data protection apply in Belgium, including:

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

There is also sector-specific legislation relevant to the protection of PII. The Electronic Communications Act of 13 June 2005 (the Electronic Communications Act), for instance, imposes specific privacy and data protection obligations on electronic communications service providers.

Data protection authority

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

The Belgian Data Protection Authority (DPA) is responsible for overseeing compliance with data protection law in Belgium. The DPA is headed by a chairperson and consists of five main departments, each headed by a director:

- a general secretariat that supports the operations of the DPA and has several executive tasks, including establishing the list of processing activities that require a data protection impact assessment, rendering opinions in the case of prior consultation by a data controller, and approving codes of conduct and certification criteria, as well as standard contractual clauses and binding corporate rules for cross-border data transfers;
- a front office service that is responsible for receiving complaints and requests, starting mediation procedures, raising awareness around data protection with the general public and informing organisations of their data protection obligations;
- a knowledge centre that issues advice on questions related to PII processing and recommendations regarding social, economic or technological developments that may have an impact on PII processing;
- an investigation service that is responsible for investigating data protection law infringements; and
- a litigation chamber that deals with administrative proceedings.

Together, the chairperson and the four directors form the executive committee that, among others, approves the DPA's annual budget and determines the strategy and management plan. The DPA's 2020–2025 Strategic Plan was published on 12 March 2020.

Also, there is an independent reflection board that provides non-binding advice to the DPA on all data-protection-related topics, upon request of the executive committee or the knowledge centre or on its own initiative.

To fulfil its role, the DPA is granted a wide variety of investigative, control and enforcement powers. The enforcement powers include the power to:

- issue a warning or a reprimand;
- order compliance with an individual's requests;
- order to inform affected individuals of a security incident;
- order to freeze or limit processing;
- temporarily or permanently prohibit processing;
- order to bring processing activities in compliance with the law;
- order the rectification, restriction or deletion of PII and the notification thereof to data recipients;
- order the withdrawal of a licence given to a certification body;
- impose penalty payments and administrative sanctions; and
- suspend data transfers.

Further, the DPA can transmit a case to the public prosecutor for criminal investigation and prosecution. The DPA can also publish the decisions it issues on its website. The investigation powers of the DPA include the power to:

- hear witnesses;
- perform identity checks;
- conduct written inquiries;
- conduct on-site inspections;
- access computer systems and copy all data such systems contain;
- access information electronically;
- seize or seal goods, documents and computer systems; and
- request the identification of the subscriber or regular user of an electronic communication service or electronic communication means.

The investigation service also has the power to take interim measures, including suspending, limiting or freezing PII processing activities.

In addition to the DPA, certain public bodies, such as police agencies, intelligence and security services and the Coordination Unit for Threat Analysis, have a specific authority overseeing their data protection compliance.

Cooperation with other data protection authorities

3 | Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The DPA is required to cooperate with all other Belgian public and private actors involved in the protection of individuals' rights and freedoms, particularly concerning the free flow of PII and customer protection. The DPA must also cooperate with the national data protection authorities of other countries. Such cooperation will focus on, inter alia, the creation of centres of expertise, the exchange of information, mutual assistance for controlling measures and the sharing of human and financial resources. The rules for ensuring a consistent application of the GDPR throughout the European Union outlined in the GDPR will apply in cross-border cases.

Breaches of data protection

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

The DPA has the power to impose the administrative sanctions outlined in the GDPR. Depending on the nature of the violation, these administrative sanctions can go up to €20 million or 4 per cent of an organisation's total worldwide annual turnover of the preceding financial year. Breaches of data protection law can also lead to criminal penalties, which can, depending on the nature of the violation, go up to €240,000. Also, violations of Belgian privacy and data protection law may result in a civil action for damages.

SCOPE

Exempt sectors and institutions

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

Belgian data protection law is generally intended to cover the processing of personally identifiable information (PII) by all types of organisations in all sectors. That said, certain types of PII processing are (partially) exempted or subject to specific rules, including the processing of PII:

- by a natural person in the course of a purely personal or household activity; for example, a private address file or a personal electronic diary;
- solely for journalism purposes, or purposes of academic, artistic or literary expression;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- by the intelligence and security services;
- by the armed forces;
- by competent authorities in the context of security classification, clearances, certificates and advice;
- by the Coordination Unit for Threat Assessment;
- by the Passenger Information Unit; and
- by certain public bodies that monitor the police, intelligence and security services (eg, the Standing Policy Monitoring Committee and the Standing Intelligence Agencies Review Committee).

Communications, marketing and surveillance laws

6 | 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.

Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act) generally apply to the processing of PII in connection with the interception of communications and electronic marketing, as well as monitoring and surveillance of individuals. Also, these topics are addressed by specific laws and regulations, including:

- the Belgian Criminal Code;
- the Electronic Communications Act of 13 June 2005;
- Collective Bargaining Agreement No. 81 of 26 April 2002 on the monitoring of employees' online communications (interception of communications);
- the Belgian Code of Economic Law;
- the Royal Decree of 4 April 2003 regarding spam (electronic marketing);
- the Belgian Act of 21 March 2007 on surveillance cameras (as amended by the Act of 21 March 2018);
- the Royal Decree of 10 February 2008 regarding the signalling of camera surveillance (as amended by the Royal Decree of 28 May 2018);
- the Royal Decree of 9 March 2014 appointing the categories of individuals authorised to watch real-time images of surveillance cameras in public spaces; and
- Collective Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance in the workplace (surveillance of individuals).

Other laws

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

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

- the Act of 21 August 2008 on the establishment and organisation of the e-Health Platform (e-health records);
- Book VII of the Belgian Code of Economic Law on payment and credit services containing data protection rules for the processing of consumer credit data (credit information);
- Collective Bargaining Agreement No. 81 of 26 April 2002 on the monitoring of employees' online communications and the Collective

Bargaining Agreement No. 68 of 16 June 1998 regarding camera surveillance in the workplace;
- the Passenger Data Processing Act of 25 December 2016; and
- the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and the restriction on the use of cash.

PII formats

8 | What forms of PII are covered by the law?

The GDPR and the Data Protection Act apply to the processing of PII, wholly or partly by automatic means, and to the processing other than by automatic means of PII that forms part of a filing system (or is intended to form part of a filing system). PII is broadly defined and includes any information relating to an identified or identifiable natural person.

Extraterritoriality

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

Belgian data protection law applies to the processing of PII carried out in the context of the activities of an establishment of a controller or processor in Belgium. Also, Belgian data protection law can apply to the processing of PII by organisations that are established outside the European Union. This is the case where such organisations process PII of individuals located in Belgium concerning offering goods or services to such individuals in Belgium or monitoring the behaviour of such individuals in Belgian territory.

Belgian data protection law will, however, not apply to the processing of PII by a processor established in Belgium on behalf of a controller established in another EU member state, to the extent that the processing takes place in the territory of the member state where the controller is located. In such a case, the data protection law of the member state where the controller is established will apply.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

In principle, all types of PII processing fall within the ambit of Belgian data protection law, regardless of who is controlling the processing or merely processing PII on behalf of a controller. The controller is any natural or legal person, public authority, agency or other body that alone or jointly with others determines the purposes and means of the processing of PII. Controllers can engage a processor to carry out PII processing activities on their behalf and under their instructions. Controllers are subject to the full spectrum of data protection obligations. Processors, on the other hand, are subject to a more limited set of direct obligations under Belgian data protection law (including the obligation to process PII only on the controller's instructions, keep internal records of PII processing activities, cooperate with the data protection supervisory authorities, implement appropriate information security measures, notify data breaches to the controller, appoint a data protection officer if certain conditions are met and ensure compliance with international data transfer restrictions). In addition to these direct legal obligations, certain data protection obligations will be imposed on processors through their mandatory contract with the controller.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

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

Controllers are required to have a legal basis for each PII processing activity. The exhaustive list of potential legal grounds for the processing of PII outlined in Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) will be available to controllers that are subject to Belgian data protection law:
- the data subject has unambiguously consented to the processing of his or her PII;
- the processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract;
- the processing is necessary for compliance with a legal obligation under EU or EU member state law to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another individual;
- the processing is necessary for the performance of a task carried out in the public interest or the exercise of the official authority vested in the controller; or
- the processing is necessary for the legitimate interests of the controller (or a third party to whom the PII is disclosed), provided that those interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

For certain types of PII, such as sensitive PII, more restrictive requirements in terms of legal bases apply. Further, controllers that rely on consent to legitimise the processing of PII that takes place in the context of offering information society services to children below the age of 13 years must obtain consent from the child's legal representative.

Legitimate processing – types of PII

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

The processing of sensitive PII revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data, health data or data concerning a person's sex life or sexual orientation, is prohibited in principle, and can only be carried out if:
- the data subject has given his or her explicit consent to such processing;
- the processing is necessary to carry out the specific obligations and rights of the controller or the data subject in the employment, social security or social protection law area;
- the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his or her consent;
- the processing is carried out by a foundation, association or any other non-profit organisation with political, philosophical, religious or trade union objectives in the course of its legitimate activities, and solely relates to the member or former members of the organisation or to persons that have regular contact with the organisation and the PII is not disclosed to third parties without the data subject's consent;
- the processing relates to PII that has been manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;

- the processing is necessary for reasons of substantial public interest recognised by EU or EU member state law;
- the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services based on EU or EU member state law or according to a contract with a health professional, subject to appropriate confidentiality obligations;
- the processing is necessary for reasons of public interest in the area of public health based on EU or EU member state law; or
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EU or EU member state law.

The Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act) explicitly lists several PII processing activities that (provided certain conditions are met) can be deemed as necessary for reasons of substantial public interest, including PII processing activities of human rights organisations, the Centre for Missing and Sexually Exploited Children (Child Focus), and organisations that assist sex offenders.

The GDPR prohibits the processing of PII relating to criminal convictions and offences or related security measures, except where the processing is carried out under the supervision of an official authority or when the processing is authorised by EU or EU member state law. The Data Protection Act allows the processing of PII relating to criminal convictions and offences:

- by natural persons, private or public legal persons for managing their own litigation;
- by lawyers or other legal advisors, to the extent that the processing is necessary for the protection of their clients' interests;
- by other persons, if the processing is necessary to perform duties of substantial public interest that are determined by EU or EU member state law;
- if the processing is required for scientific, historical or statistical research or archiving;
- if the data subject has given his or her explicit and written consent to the processing of PII relating to criminal convictions and offences for one or more purposes and the processing is limited to such purposes; or
- if the processing concerns PII made public by the data subject, on its own initiative, for one or more specific purposes and the processing is limited to such purposes.

The Data Protection Act also sets forth several specific measures that must be implemented when processing genetic, biometric, health data or PII relating to criminal convictions and offences. In such cases, a list of categories of individuals that will have access to the data, together with a description of those individuals' roles concerning the processing, must be maintained. This list must be made available to the Data Protection Authority upon request. Further, the controller or processor must ensure that the individuals who have access to such data are bound by legal, statutory or contractual confidentiality obligations.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

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

Controllers are required to provide notice to data subjects whose PII they process. If PII is obtained directly from the data subject, the notice must contain at least the following information and be provided no later than the moment the PII is obtained:

- the name and address of the controller (and of its representative, if any);
- the contact details of the data protection officer (if any);
- the purposes of and legal basis for the processing;
- where the legitimate interests' ground is relied upon, the interests in question;
- the existence of the right to object, free of charge, to the intended PII processing for direct marketing purposes;
- the (categories of) recipients of PII;
- details of transfers to third countries or international organisations, the relevant safeguards associated with such transfers (including the existence or absence of an adequacy decision of the European Commission) and how data subjects can obtain a copy of these safeguards or where they have been made available;
- the data retention period or criteria used to determine that period;
- the existence of the right to request access to and rectification or erasure of PII or the restriction of processing of PII or to object to the processing, as well as the right to data portability;
- the existence of the right to withdraw consent at any time if the controller relies on the data subject's consent for the processing of his or her PII;
- the right to lodge a complaint with a supervisory authority;
- whether providing the PII is a statutory or contractual requirement or a requirement to enter into a contract, as well as whether the data subject is obliged to provide the PII and the possible consequences of the failure to provide the PII; and
- information on automated individual decision-making (if any), including information on the logic involved in such decision-making, the significance and the envisaged consequences.

If PII is not obtained directly from the data subject, the controller must provide, in addition to the information listed above, the categories of PII concerned and the source from which the PII originates. This information must be provided within a reasonable period after obtaining the PII (within one month at the latest), or when PII is shared with a third party, at the very latest when the PII is first disclosed or when the PII is used to communicate with the data subject at the latest at the time of the first communication.

Exemption from notification

14 | When is notice not required?

Notice is not required if data subjects have already received the information concerning the processing of their personally identifiable information (PII) required under data protection law.

Also, in cases where PII is not collected directly from the data subject, the controller is exempt from the duty to provide notice if:

- informing the data subject proves impossible or would involve a disproportionate effort, in particular in the context of processing PII for archiving purposes in the public interest, statistical, historical or scientific research, or to the extent that providing notice would seriously impair or render the achievement of the purposes of the processing impossible; or

- PII must remain confidential subject to an obligation of professional secrecy regulated by EU or EU member state law.

Control of use

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

Belgian data protection law includes several rights aimed at enabling data subjects to exercise choice and control over the use of their PII. In particular, data subjects are entitled to:

- request the controller to provide information regarding the processing of their PII and a copy of the PII being processed;
- obtain the rectification of incorrect PII relating to them and to have incomplete PII completed;
- obtain the erasure of their PII;
- obtain the restriction of the processing of their PII;
- receive the PII they have provided to the controller in a structured, commonly used and machine-readable format and to have it transmitted directly to another controller where technically feasible;
- object to the processing of their PII, for reasons related to their particular situation, if such processing is based on the ground that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or based on the legitimate interests ground unless the controller demonstrates that it has compelling legitimate grounds that outweigh the interests, rights and freedoms of the data subject or the processing is necessary for the establishment, exercise or defence of legal claims;
- object to the processing of their PII for direct marketing purposes; and
- not be subject to decisions having legal effects or similarly significantly affecting them, which are taken purely based on automatic PII processing, including profiling.

The above-mentioned data protection rights are not absolute and typically subject to conditions and exemptions outlined in Regulation (EU) 2016/679 (the General Data Protection Regulation) and the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act).

Data accuracy

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

Controllers must ensure that the PII they process is accurate and take reasonable steps to ensure that inaccurate PII is rectified or erased without delay.

Amount and duration of data holding

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

Controllers are required to limit the processing of PII to what is strictly necessary for processing purposes. In terms of data retention requirements, PII must not be kept in an identifiable form for longer than necessary in light of the purposes for which the PII is collected or further processed. This means that, if a controller no longer needs to identify data subjects for the purposes for which the PII was initially collected or further processed, the PII should be erased or anonymised.

Finality principle

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

Belgian data protection law incorporates the 'finality principle' and, therefore, PII can only be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes.

Use for new purposes

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

PII can be processed for new purposes if these are not incompatible with the initial purposes for which the PII was collected, taking into account all relevant factors, especially the link between the purposes for which the PII was collected and the purposes of the intended further processing, the context in which the PII was collected, the relationship between the controller and the data subject, the nature of the concerned PII, the possible consequences of the further processing and the safeguards implemented by the controller (eg, pseudonymising or encrypting the PII). Further, the Data Protection Act sets forth specific rules for the further processing of PII for archiving in the public interest, scientific or historical research or statistical purposes.

SECURITY

Security obligations

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

Controllers and processors are required to implement appropriate technical and organisational measures to protect PII from accidental or unauthorised destruction, loss, alteration, disclosure, access and any other unauthorised processing.

These measures must ensure an appropriate level of security considering the condition, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity for the rights and freedoms of individuals.

These measures may include:

- the pseudonymisation and encryption of PII;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to PII promptly in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The more sensitive the PII and the higher the risks for the data subject, the more precautions have to be taken. The Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data, for instance, sets forth specific measures that controllers must implement when processing genetic and biometric data, health data and data relating to criminal convictions and offences, including measures to ensure that persons having access to such PII are under appropriate confidentiality obligations.

Notification of data breach

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

The Electronic Communications Act of 13 June 2005 imposes a duty on providers of publicly available electronic communications services to notify security breaches, under certain conditions, to the Data Protection Authority (DPA). The notification should contain the following information:

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

Where feasible, the notification should be done within 24 hours after detection of the breach. In case the controller does not have all the required information available within this time frame, it can complete the notification within 72 hours after the initial notification. The DPA has published a template form on its website to accommodate companies in complying with their data breach notification obligations. Also, data subjects must be informed without undue delay when the security breach is likely to adversely affect their privacy or PII.

Since Regulation (EU) 2016/679 (the General Data Protection Regulation) became applicable, mandatory data breach notification obligations are no longer limited to the telecom sector. Controllers in all sectors are now required to notify data breaches to the DPA unless the data breach is unlikely to result in a risk to the rights and freedoms of individuals. Such notification must be done without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. Where notifying the DPA within 72 hours is not possible, the controller must justify such delay. A data breach notification to the DPA must at least contain:

- the nature of the data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of PII records concerned;
- the name and contact details of the data protection officer (if any) or another contact point to obtain additional information regarding the data breach;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken to address the breach, including mitigation measures where appropriate.

In addition to notifying the DPA, controllers are required to notify data breaches to the affected data subjects where the breach is likely to result in a high risk to the rights and freedoms of natural persons. The notification to the affected individuals must contain at least:

- the name and contact details of the data protection officer or another contact person;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken to address the breach, including mitigation measures where appropriate.

Notifying the affected individuals is, however, not required if the controller has implemented measures that render the affected PII unintelligible to any person who is not authorised to access it (eg, encryption), subsequent measures have been taken to ensure that the high risk to the rights and freedoms of individuals is no longer likely to materialise or where notifying the affected individuals would involve a disproportionate effort. In the latter case, public communication or similar measure should be made to inform the affected individuals about the breach. If a processor suffers a data breach, it must notify the controller on whose behalf it processes PII without undue delay. In Belgium, data breaches can be notified to the DPA via an online form made available on the DPA's website.

INTERNAL CONTROLS

Data protection officer

22 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 mandatory where:

- the processing is carried out by a public authority or body;
- the core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or processor consist of processing sensitive PII on a large scale.

Also, the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act) provides that the appointment of a data protection officer is required for:

- private organisations that process PII on behalf of a public authority (as data processors) or that receive PII from a public authority and the processing of such PII is considered to present a high risk; and
- controllers processing PII for archiving purposes in the public interest or scientific, historical or statistical purposes.

The main tasks of the data protection officer are to:

- inform and advise the controller or processor of its data protection obligations;
- monitor compliance with data protection laws, Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and the controller's or processor's policies, including concerning the assignment of responsibilities, raising awareness and training the controller's or processor's personnel involved in the processing of PII;
- assist with data protection impact assessments;
- cooperate with the relevant supervisory authority; and
- act as a contact point for the data subjects and the relevant supervisory authorities regarding the processing activities, including prior consultation in the context of data protection impact assessments.

Although the obligation to maintain internal records of processing ultimately falls on the controller or processor, the data protection officer may also be assigned the task of maintaining such records.

Controllers and processors must communicate the identity and contact details of their data protection officer to the Data Protection Authority (DPA) via an online form available on the DPA's website.

Record keeping

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

Controllers and processors are required to maintain internal records of their processing activities. Such records should be in writing, including in electronic form, and should be made available to the DPA upon request.

Controllers' internal records should contain, at least:

- the name and contact details of the controller, joint controller or the controller's representative, if applicable, and the identity and contact details of the data protection officer (if any);
- the purposes of the processing;
- a description of the categories of data subjects and PII;
- the categories of data recipients, including recipients in third countries;
- transfers of PII to a third country, including the identification of such country and, where applicable, documentation of the safeguards that have been put in place to protect the PII transferred;
- the envisaged data retention period or the criteria used to determine the retention period; and
- a description of the technical and organisational security measures put in place, where possible.

Processors' records should contain, at least:

- the name and contact details of the processor and each controller on behalf of which the processor is acting and, where applicable, the controller's or processor's representative and data protection officers;
- the categories of processing carried out on behalf of the controller;
- transfers of PII to third countries, including the identification of such countries and, where applicable, documentation of the safeguards put in place to protect the PII transferred; and
- where possible, a description of the technical and organisational security measures that have been put in place.

Companies that employ fewer than 250 persons are exempted from the obligation to keep internal records of their PII processing activities unless their processing activities are likely to result in a risk to the rights and freedoms of individuals, are not occasional or include the processing of sensitive PII or PII relating to criminal convictions and offences.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

The GDPR introduces the principles of privacy by design and privacy by default. Privacy by design means that controllers are required to implement appropriate technical and organisational measures designed to implement the data protection principles effectively and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR. When doing so, controllers must consider the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing. Privacy by default means that controllers must implement appropriate technical and organisational measures to ensure that, by default, only PII that is strictly necessary for each processing purpose is processed.

When engaging in new PII processing activities or changing existing processing activities that are likely to result in a high risk to the rights and freedoms of individuals, controllers are also required to carry out a data protection impact assessment. High-risk PII processing activities triggering the requirement to conduct a data protection impact assessment include:

- automated individual decision-making;
- large-scale processing of sensitive PII or PII relating to criminal convictions and offences; and
- systematic monitoring of a publicly accessible area on a large scale.

Where a data protection impact assessment reveals that the processing would result in high risk and no measures are taken by the controller to mitigate such risk, the controller must consult the DPA before commencing the envisaged PII processing activity. The Data Protection Act excludes, under certain conditions, processing activities for journalistic, academic, artistic or literary purposes from such requirement.

The DPA issued a Recommendation 01/2018 on data protection impact assessments in which it provides guidance to controllers on when a data protection impact assessment is required and what the assessment should contain. Recommendation 01/2018 also includes a list of PII processing activities that require a data protection impact assessment (black list) and a list of PII processing activities that do not trigger the requirement to conduct a data protection impact assessment (white list). Also, the Belgian DPA issued a form that should be used in cases where prior consultation with the DPA is required. The form is available on the DPA's website.

REGISTRATION AND NOTIFICATION

Registration

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

Since 25 May 2018, the obligation for controllers to register their data processing activities with the Data Protection Authority (DPA) no longer exists. Instead, controllers and processors are required to maintain internal records of their processing activities. However, if a controller or processor appoints a data protection officer, such an appointment must be communicated to the DPA through a specific online form made available on the DPA's website.

Formalities

26 | What are the formalities for registration?

Not applicable. There is no obligation under the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data (the Data Protection Act) for controllers to register their data processing activities.

Penalties

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

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Refusal of registration

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

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Public access

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

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Effect of registration

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

Not applicable. There is no obligation under the Data Protection Act for controllers to register their data processing activities.

Other transparency duties

31 | Are there any other public transparency duties?

No.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

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

Under Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), when a controller outsources data processing activities to a third party (ie, a processor), it should put in place an agreement with the processor that sets out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of PII and categories of data subjects; and
- the obligations and rights of the controller.

Such agreement should stipulate that the processor:

- processes the PII only on documented instructions from the controller, unless otherwise required by EU or EU member state law. In that case, the processor must inform the controller of the legal requirement before processing, unless the law prohibits such information on important grounds of public interest. Also, if in the processor's opinion an instruction of the controller infringes the GDPR, it should immediately inform the controller thereof;
- ensures that persons authorised to process the PII have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all appropriate technical and organisational measures required under the GDPR to protect the PII;
- shall not engage sub-processors without the specific or general written authorisation of the controller. In the case of a general written authorisation, the processor must inform the controller of intended changes concerning the addition or replacement of sub-processors;
- assists the controller by appropriate technical and organisational measures, insofar as this is possible, with data subjects' rights requests;
- assists the controller in ensuring compliance with the security and data breach notification requirements, as well as the controller's obligation to conduct privacy impact assessments;
- at the end of the provision of the services to the controller, returns or deletes the PII, at the choice of the controller, and deletes existing copies unless further storage is required under EU or EU member state law; and
- makes available to the controller all information necessary to demonstrate compliance with the GDPR and contribute to audits.

On 12 November 2020, the European Commission adopted draft standard contractual clauses to be used between controllers and processors in the European Economic Area. The Controller-Processor standard contractual clauses are aimed at assisting organisations that rely on data processors in the European Economic Area to perform certain data processing activities on their behalf to comply with their obligation to put in place an appropriate data processing agreement, as described above. The final Controller-Processor standard contractual clauses have yet to be adopted and published.

Restrictions on disclosure

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

In general, there are no specific restrictions under the GDPR or the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal on the disclosure of PII other than the restrictions resulting from the general data protection principles (such as lawfulness, notice and purpose limitation).

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

PII can be transferred freely to other countries within the European Economic Area, as well as to countries recognised by the European Commission as providing an adequate level of data protection.

Transferring PII to countries outside the European Economic Area that are not recognised as providing an adequate level of data protection is prohibited unless:

- the data subject has explicitly given his or her consent to the proposed transfer after having been informed of the possible risks of such transfers;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject;
- the transfer is necessary for important reasons of public interest or the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or other persons; or
- the transfer is made from a register that is open to consultation either by the public in general or by any person that can demonstrate a legitimate interest.

If none of the above applies and no appropriate safeguards have been put in place, the transfer can take place if it is necessary for compelling legitimate interests pursued by the controller, but only if the transfer is not repetitive, concerns only a limited number of data subjects, and the controller has assessed all circumstances surrounding the data transfer and has provided suitable safeguards to protect the PII. In this case, the controller must inform the Data Protection Authority (DPA) and concerned data subjects of the transfer and the legitimate interests that justify such transfer.

In addition to the exemptions listed above (which should typically only be relied on in limited cases), cross-border transfers to non-adequate countries are allowed if the controller has implemented measures to ensure that the PII receives an adequate level of data protection and data subjects can exercise their rights after the PII has been transferred. Such measures include the execution of standard contractual clauses approved by the European Commission or adopted by a supervisory authority, an approved code of conduct or certification mechanism or implementation of binding corporate rules. When relying on such safeguards to legitimise data transfers, the exporting controller must conduct a transfer risk assessment to verify whether the level of protection for PII transferred is essentially equivalent to the level of protection in the European Union. Depending on the outcome of that assessment, additional safeguards may need to be put in place to ensure such a level of protection for the PII that is transferred. Also, transfers of PII can be legitimised by executing an ad hoc data transfer agreement. However, in such cases, the prior authorisation of the DPA must be obtained.

On 12 November 2020, the European Commission published a draft implementing decision on standard contractual clauses for the transfer of PII to third countries under the GDPR, along with its draft set of new standard contractual clauses. The new standard contractual clauses are aimed at replacing the previous version of the clauses that were published by the European Commission in 2001, 2004 and 2010 respectively. The new draft standard contractual clauses consider the complexity of modern processing chains by combining several general provisions with several modular provisions that should be selected based on the status of the parties under the GDPR, namely provisions for controller-to-controller transfers, controller-to-processor transfers, processor-to-processor transfers and processor-to-controller transfers. The final standard contractual clauses for the transfer of PII to third countries have yet to be adopted and published.

Notification of cross-border transfer

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

In general, cross-border data transfers do not need to be notified to the DPA.

Prior authorisation is required if the controller relies on an ad hoc data transfer agreement to legitimise the transfer of PII to non-adequate countries. Such authorisation is not required when the controller has guaranteed an adequate level of data protection by executing the standard contractual clauses approved by the European Commission.

Further transfer

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

The data transfer restrictions and authorisation requirements apply regardless of whether PII is transferred to a service provider (ie, processor) or another controller.

The restrictions and requirements applicable to onward PII transfers depend on the legal regime in the jurisdiction where the data importer is located and the data transfer mechanism relied upon to legitimise the initial data transfer outside the European Economic Area. For example, the standard contractual clauses contain specific requirements for onward data transfers.

RIGHTS OF INDIVIDUALS

Access

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

Data subjects have a right to access the PII that a controller holds about them. When a data subject exercises his or her right of access, the controller is required to provide the following information to the data subject:

- confirmation as to whether the controller processes the data subject's PII;
- the purposes for which his or her PII is processed;
- the categories of PII concerned;
- the recipients or categories of recipients to whom PII has been or will be disclosed, in particular, recipients in third countries, and in the case of transfers to third countries, the appropriate safeguards put into place by the controller to legitimise such transfers;
- where possible, the envisaged period for which the PII will be stored or, if not possible, the criteria used to determine such period;
- the existence of the right to request the rectification or erasure of PII or restriction of the processing or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- information regarding the source of the PII; and
- the existence of automated decision-making and information about the logic involved in any such automated decision-making (if any), as well as the significance and the envisaged consequences of such processing.

The controller should also provide a copy of the PII to the data subject in an intelligible form. For further copies requested by the data subjects, controllers may charge a reasonable fee to cover administrative costs.

The right to obtain a copy of PII may be subject to restrictions to the extent it adversely affects the rights and freedoms of others, and the controller may refuse to act on a request of access if the request is manifestly unfounded or excessive, in particular, because of its repetitive character.

Also, exemptions to the right of access apply to PII originating from certain public authorities, including the police and intelligence services and to PII processed for journalistic, academic, artistic or literary purposes.

Other rights

38 | Do individuals have other substantive rights?

Rectification

Data subjects are entitled to obtain, without undue delay, the rectification of inaccurate PII relating to them.

Erasure

Data subjects have the right to request the erasure (the right to be forgotten) of PII concerning them where:

- the PII is no longer necessary for the purposes for which it was collected or otherwise processed;
- the processing is based on consent and the data subject withdraws his or her consent and there is no other legal basis for the processing;
- the data subject objects to the processing of his or her PII based on the controller's legitimate interests and there are no overriding legitimate grounds for the processing;
- the data subject objects to the processing of his or her PII for direct marketing purposes;
- PII has been unlawfully processed;
- PII has to be erased for compliance with a legal obligation under EU or EU member state law; and
- PII has been collected concerning offering information society services to a child.

The right to be forgotten does not apply where the processing is necessary for:

- the exercise of the right to freedom of expression and information,
- compliance with a legal obligation under EU or EU member state law;
- the performance of a task carried out in the public interest or the exercise of official authority vested in the controller;
- reasons of public interest in the area of public health;
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- the establishment, exercise or defence of legal claims.

Restriction of processing

Data subjects are entitled to request that the processing of their PII is restricted by the controller, where one of the following conditions applies:

- the data subject is contesting the accuracy of his or her PII, in which case, the processing should be restricted for a period enabling the verification by the controller of the accuracy of the PII;
- the processing is unlawful and the data subject opposes the erasure of the PII and requests the restriction of its use instead;
- the controller no longer needs the PII, but the PII is required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to the processing of his or her PII for purposes other than direct marketing, based on grounds relating to his or her particular situation. In this case, the processing should be restricted, pending the verification by the controller as to whether the controller's legitimate interests override those of the data subject.

Objection to processing

Data subjects have the right to object at any time to the processing of their PII for substantial and legitimate reasons related to their particular situation, where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or where the controller processes the PII to pursue its legitimate interests. Also, data subjects are in any event (ie, without any specific justification) entitled to object, at any time, to the processing of their PII for direct marketing purposes.

Data portability

Data subjects are entitled to receive in a structured, commonly used and machine-readable format the PII they have provided directly to the controller and the PII they have provided indirectly by the use of the controller's services, websites or applications. Also, where technically feasible, data subjects have the right to have their PII transmitted by the controller to another controller. The right to data portability only applies if:

- the PII is processed based on the data subject's consent or the necessity of the processing for the performance of a contract; and
- the PII is processed by automated means.

The above-mentioned rights are subject to certain restrictions, in particular in the case of processing PII originating from certain public authorities, including the police and intelligence services, or processing of PII for journalistic, academic, artistic or literary purposes.

Complaint to relevant supervisory authorities and enforce rights in court

Data subjects are entitled to file a complaint with the DPA (which has been granted investigative, control and enforcement powers) to enforce their rights. Further, data subjects can initiate proceedings before the President of the Court of First Instance when their rights have not been respected by the controller.

Automated decision-making

Data subjects also have the right not to be subject to decisions having legal effects or significantly affecting them, including profiling, which are taken purely based on automatic data processing, unless the decision:

- is necessary to enter into or for the performance of a contract;
- is based on a legal provision under EU or EU member state law; or
- is based on the data subject's explicit consent.

Compensation

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

Data subjects are entitled to receive compensation from controllers if they have suffered material or non-material damages as a result of a violation of Belgian data protection law. Controllers will only be exempt from liability if they can prove that they are not responsible for the event giving rise to the damage. Individuals may choose to mandate an organ, organisation or non-profit organisation to lodge a complaint on their behalf before the Data Protection Authority (DPA) or the competent judicial body.

Enforcement

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

Enforcement of data subjects' rights is possible through legal action before the Belgian courts (ie, before the President of the Court of First Instance) and via the DPA.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

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

No.

SUPERVISION

Judicial review

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

Controllers can appeal against certain decisions of the inspection service of the Data Protection Authority (DPA) (including orders to freeze or limit processing activities, decisions to temporarily or permanently prohibit the processing or decisions to seize or seal goods or computer systems) in front of the DPA's Litigation Chamber. Also, controllers can appeal the decisions of the DPA's Litigation Chamber in front of a specific section of the Appeal Court of Brussels (ie, the Markets Court).

SPECIFIC DATA PROCESSING

Internet use

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

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

On 9 April 2020, the Data Protection Authority (DPA) updated its practical guidance on cookies intending to clarify how companies should inform individuals about and obtain their consent for the use of cookies, as well as the types of cookies that are exempted from the consent requirement.

The guidance provides that consent must be informed, unambiguous and provided through a clear affirmative action. Merely continuing to browse a website does not constitute valid consent. Users must have the possibility to provide granular consent per type of cookie, as well as, in a second stage, per cookie. Also, users must be provided with information regarding the use of cookies. The DPA suggests providing this information in two phases: first, a notice at the time the users' consent is obtained, and second, a more detailed notice in the form of a cookie policy.

According to the DPA, users must be provided with the following information upon consenting to the use of cookies:

- the entity responsible for the use of cookies;
- the purposes for which cookies are used;
- the data collected through the use of cookies;
- the cookies' expiry time; and
- the users' rights concerning cookies, including the right to withdraw their consent.

The DPA also clarifies that the lifespan of a cookie must be limited to what is necessary to achieve the cookie's purpose and cookies should not have an unlimited lifespan.

The cookie requirements under Belgian law result from the legal regime for the use of cookies set forth by Directive 2002/58/EC (the ePrivacy Directive), as transposed into EU member state law. The ePrivacy Directive is currently under review and will most likely be replaced by the ePrivacy Regulation in the future. The exact timing of the adoption of the ePrivacy Regulation has, however, not yet been determined.

Electronic communications marketing

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

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

Marketing by electronic post

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

Marketing by automated calling systems and fax

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

Marketing by telephone

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

As the rules on electronic communications marketing under Belgian law result from the ePrivacy Directive, these rules may change once the ePrivacy Directive is replaced by the ePrivacy Regulation (which has not been adopted yet). Also, on 10 February 2020, the DPA published Recommendation 1/2020 on data processing activities for direct marketing purposes, which aims at clarifying the complex rules relating to the processing of PII for direct marketing purposes and provides practical examples and guidelines around direct marketing.

Among others, Recommendation 1/2020 clarifies that:

- Determining and specifying the purposes for which PII will be processed is essential. In this respect, the DPA considers that merely stating that personal data will be processed for direct marketing purposes is not sufficient in light of the transparency requirements applicable under Regulation (EU) 2016/679 (the General Data Protection Regulation).
- To ensure data minimisation, companies should limit open fields in data collection forms, review their databases regularly to delete any unnecessary data, and implement processes to ensure that Do Not Call lists are considered when reviewing databases where marketing data is stored.
- Individuals must be offered a right to object at any time and easily, without having to take additional steps and free of charge, to the processing of their PII for direct marketing purposes. In this respect, the DPA considers that a simple unsubscribe button in small characters at the end of a marketing email is not sufficient. Also, where it is technically feasible, the DPA recommends allowing individuals to granularly select the marketing activities for which they want to object (eg, email marketing or text).
- Consent to direct marketing must be specific concerning the content of the marketing communication and the means used.
- Where an individual withdraws their consent to the processing of PII, there is no longer a valid legal ground unless PII must be kept to comply with a legal obligation. In practice, this means that if the individual withdraws their consent and there is no alternative legal ground, PII should be deleted (regardless of whether the individual exercises their deletion rights). The same applies where individuals object to the processing of their PII based on the legitimate interest ground.

Cloud services

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

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

Some of the risks identified by the DPA include:

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

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

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

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Data Protection Authority (DPA) published Recommendation 03/2020 on data sanitisation and data medium destruction techniques to assist companies with the secure disposal of data or data media.

Also, the DPA continues to publish new material and update its existing material regarding the processing of PII in the context of the coronavirus pandemic. Coronavirus-related content is available on the DPA's website.

Coronavirus

47 | What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

Belgium has worked on various laws and regulations to combat the spread of coronavirus, including the draft Pandemic Law that has not yet been adopted. The draft Pandemic Law is aimed at providing a legal framework for the interim measures taken as a response to the emergency.

The DPA has published various statements and opinions regarding coronavirus-related draft laws and regulations. Among others, the DPA asked the Belgian government to consider the data protection principles, including the principles of proportionality, purpose limitation and necessity, when adopting coronavirus-related measures and reminded the government that it should request the DPA's opinion on legislative initiatives that involve the processing of PII in the context of the pandemic.

There is currently no Belgian law or collective agreement allowing the collection by private companies of employees' health data (eg, temperature data or proof of vaccination). Further, employees' consent is typically not a valid legal basis for the processing of PII in the employment context as employees' consent is not considered freely given. In light of the above, there is generally no legal basis under Regulation (EU) 2016/679 (the General Data Protection Regulation) and the Act of 30 July 2018 on the protection of natural persons concerning the processing of personal data to process such health data regarding employees in the context of the pandemic. Specific exceptions may apply but their scope is limited and such exceptions must be applied restrictively. The DPA regularly updates its coronavirus-related guidance and it is, therefore, recommended to monitor such guidance continuously.

HUNTON ANDREWS KURTH

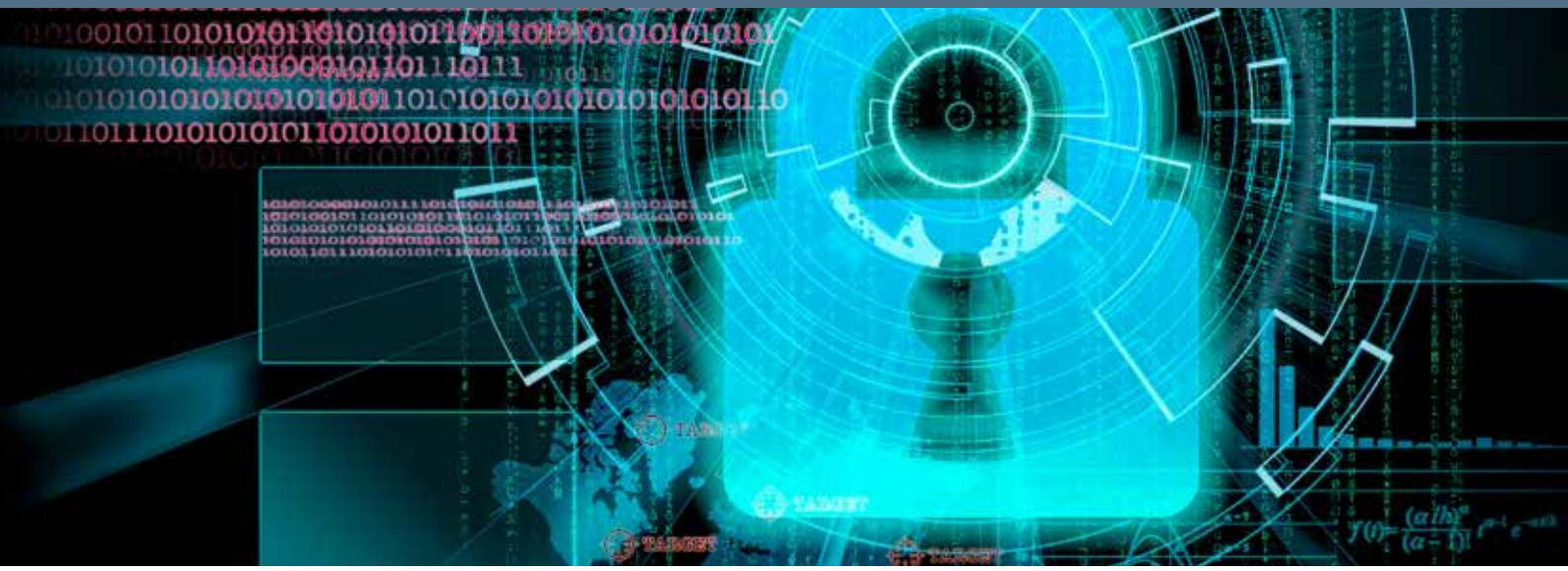
David Dumont
ddumont@huntonak.com

Laura Léonard
lleonard@huntonak.com

Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
Tel: +32 2643 5800
Fax: +32 2643 5822
www.huntonak.com

HUNTON
ANDREWS KURTH

Leaders in Privacy and Cybersecurity



Keep the trust you've earned.

Complying with global privacy, data protection and cybersecurity rules is challenging, especially for businesses that operate across borders. Our top-ranked privacy team, in combination with the firm's Centre for Information Policy Leadership, advises on all aspects of US and European data protection law and cybersecurity events. We help businesses develop global compliance frameworks addressing regulatory obligations in the US, the EU and across the world. The firm is widely recognized globally as a leading privacy and data security firm.

For more information, visit www.huntonprivacyblog.com.

Other titles available in this series

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

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-644-0