THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FOURTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE Privacy, Data Protection and Cybersecurity Law Review

Fourth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2017
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LawReviews

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

ACCOUNT MANAGERS
Pere Aspinall, Sophie Emberson,
Laura Lynas, Jack Bagnall

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Arthur Hunter

EDITORIAL COORDINATOR
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Caroline Fewkes

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-89-8

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2017 Law Business Research Ltd

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC–PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW

THE CONSUMER FINANCE LAW REVIEW

THE INITIAL PUBLIC OFFERINGS REVIEW

THE CLASS ACTIONS LAW REVIEW

THE TRANSFER PRICING LAW REVIEW

THE BANKING LITIGATION LAW REVIEW

THE HEALTHCARE LAW REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BAKER & MCKENZIE – CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

DUCLOS, THORNE, MOLLET-VIÉVILLE & ASSOCIÉS (DTMV)

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

LEE & KO

M&M BOMCHIL

NNOVATION LLP

PERCHSTONE & GRAEYS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VDA VIEIRA DE ALMEIDA

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 6

BELGIUM

Steven De Schrijver[1]

I OVERVIEW

The Belgian legislative and regulatory approach to privacy, data protection and cybersecurity is quite comprehensive. The most important legal provisions can be found in the following:

a Article 22 of the Belgian Constitution, which provides that everyone is entitled to the protection of his or her private and family life;

b the Act of 8 December 1992 on Privacy Protection in Relation to the Processing of Personal Data (the Data Protection Act), further implemented by the Royal Decree of 13 February 2001;

c Book XII (Law of the Electronic Economy) of the Code of Economic Law, as adopted by the Act of 15 December 2013;

d the Act of 13 June 2005 on Electronic Communications (the Electronic Communications Act); and

e the Act of 28 November 2000 on Cybercrime.

Because of a series of cybersecurity attacks on a number of banks and private companies in the past few years, cybersecurity has increasingly received more and more attention in Belgium in recent years. One of Belgium's most notable cybersecurity incidents, however, was the lightning strike in 2015 at the Google data centre in Mons, which was struck four times during a summer storm, resulting in permanent data loss on a tiny fraction (0.000001 per cent) of the total disk space.

Since presenting its national cybersecurity strategy in 2012, Belgium has made substantial efforts to enhance cybersecurity. For instance, a secret Belgian operation in 2016 prevented the worldwide cyberattacks by the WannaCry ransomware virus from causing large-scale damage in Belgium in 2017. The Centre for Cybersecurity Belgium (CCB) had collected data from the global IT security company Rapid7 on Belgian companies' cybersecurity in 2016 after the country scored badly in Rapid7's National Exposure Index report that year, and used this information to warn companies. In 2017, Belgium is now ranked as the 179th most exposed country of 183 countries, in comparison with 2016, when it was ranked first, and therefore the most exposed country.

Furthermore, while the NotPetya ransomware virus did cause some damage within multinationals in Belgium, the federal cyber-emergency team (CERT) reports that efforts made after the WannaCry ransomware attack have paid off, as the damage in Belgium was limited. The responsibilities of the CCB and CERT are discussed further in Section IX.

1 Steven De Schrijver is a partner at Astrea.

Belgium is now looking to also improve cybersecurity in the military field, with the Belgian army recruiting 92 computer experts in 2017, and planning to recruit up to 200, to form a 'cyber-army' responsible for protecting possible military targets.

II THE YEAR IN REVIEW

Last year's most heated debate concerned the case against Facebook initiated by the Belgian Privacy Commission (Belgium's data protection authority (DPA)) in relation to Facebook's use of 'social plug-ins' to track the internet behaviour of not only its users, but also internet users without a Facebook account at all. The case still continues, although the interim measures imposed on Facebook by the President of the Court of First Instance have been overruled at appeal on jurisdictional grounds and, because of a lack of urgency, we are still awaiting a final ruling on the merits of the case, which is expected to be delivered at the end of 2017. This year, however, the focus has been on the ongoing discussion about whether foreign internet service providers, such as Yahoo! or peer-to-peer internet software providers such as Skype, are to be considered electronic communications service providers under Belgian law and subject to the jurisdiction of the Belgian courts.

After the final judgment in the *Yahoo!* saga on 1 December 2015, in which the Belgian Supreme Court dismissed an appeal lodged by Yahoo! against the ruling of the Court of Appeal of Antwerp obliging Yahoo! to disclose to the Belgian judicial authorities (despite the fact that Yahoo! had no establishment or personnel in Belgium) the identity of persons who committed fraud via its email service, the Court of First Instance of Mechelen had to rule on Skype's duty not only to disclose certain information, but also to provide technical assistance for the interception of the content of 'live' voice communications. Whereas the obligation to disclose information (and thus jurisdiction) could be located in Belgium in the *Yahoo!* case on the grounds of the 'portability' of information, this reasoning was difficult to apply by analogy to technical assistance that had to be provided in Luxembourg because Skype is a Luxembourg company and has no infrastructure in Belgium, and this would require material acts abroad. Nonetheless, the Court of First Instance imposed a fine of €30,000 on Skype for its refusal to cooperate in setting up a wiretap ordered by the Mechelen investigative judge. The Court ruled that the technical assistance required of Skype was to be extended in Belgium and the technical impossibility of Skype cooperating was irrelevant because Skype itself had created this impossibility by organising its operations in the way it did. Skype lodged an appeal against this judgment with the Court of Appeal of Antwerp, which is expected to deliver its judgment by the end of 2017 (see Section VI).

Another judgment that caused considerably controversy in the past year was the ruling of the Belgian Supreme Court of 13 December 2016, which declared unlawful all speeding tickets issued by the police solely on the basis of number plate identification (using roadside cameras). The Supreme Court found that the police had never been granted formal authorisation to retrieve personal information of the alleged traffic offenders from the database of the Vehicle Registration Service (DIV), where the names and addresses of all car owners are collated with the record of their number plates. The Supreme Court concluded that the police were therefore in violation of the Data Protection Act and fines imposed illegally through the use of unlawfully obtained personal data could be challenged and reviewed in court. However, the police authorities solved this illegality issue very quickly by applying for and being granted a formal authorisation from the DPA to consult the DIV database for identification purposes. This case clearly demonstrates that the Belgian

judiciary acknowledges the importance of privacy legislation in modern-day life and that even government bodies have to face the consequences of any non-compliance with privacy and data protection legislation.

Privacy-related concerns also arose with respect to the implementation of the low-emission zone (LEZ) in Antwerp, prohibiting polluting vehicles from entering the city centre, to improve the air quality of the city. The City of Antwerp placed smart cameras equipped with an automated number plate recognition system at the boundaries of the LEZ and a LEZ database was created, the data in which were mainly retrieved from the DIV, including a whitelist of compliant vehicles. Initially, the DPA considered that, by duplicating the entire DIV database in the LEZ database, the City of Antwerp was violating the proportionality principle set out in the Data Protection Act as the personal data of all vehicle owners registered in Belgium would be duplicated, while only a limited number of these vehicles would enter the LEZ zone. Subsequently, in June 2016, an adapted version of the project was submitted and accepted by the DPA, because it had limited the content of the LEZ database and put extra security measures in place.

Lastly, on 22 December 2016, the Court of Justice of the EU (CJEU) ruled that the statutory retention period of one year for metadata held by telecom operators and electronic communication service providers laid down in the recently amended Act of 13 June 2005 on Electronic Communications (amended by the Act on Data Retention of 29 May 2016) is incompatible with the right to privacy of individuals. The retention obligation should be limited to what is strictly necessary for the purposes the authorities want to achieve. The CJEU held that in the fight against 'serious crime', EU Member States are allowed to retain data in a targeted manner and only after review by a court or independent body, except in very urgent cases. We will have to wait and see what effect the CJEU ruling will have on this new Belgian data retention legislation.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The Belgian privacy and data protection legislation is set forth in the Act of 8 December 1992 on privacy protection in relation to the processing of personal data (the Data Protection Act). This Act was amended by the Act of 11 December 1998 with a view to implementing the provisions of the EU Data Protection Directive (which will of course be replaced by the new EU General Data Protection Regulation (GDPR), which entered into force on 24 May 2016 and will apply as of 25 May 2018).

Belgium has transposed the EU Data Protection Directive quite literally, so the definitions of the different concepts, such as personal data, sensitive personal data and data controllers, are identical or very similar to the definitions used in EU law. As such, 'personal data' means any information relating to an identified or identifiable natural person whereby an 'identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her identity. 'Sensitive personal data' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health, sex life or judicial information.

The data controller is the person who alone or jointly with others determines the purposes and means of the processing of personal data, and data processors are persons that process personal data on behalf of a data controller. Under Belgian law, it is also possible for different persons or entities to act as data controller in respect of the same personal data.

The Belgian enforcement agency with responsibility for privacy and data protection is the DPA. The DPA's mission includes monitoring compliance with the provisions of the Data Protection Act, but it cannot impose any administrative penalties upon individuals or organisations. However, the GDPR has broadened the powers of the DPA. As of mid-2018, the DPA will have increased investigative powers, the right to initiate legal proceedings as well as the right to impose interim measures and administrative fines.

The Data Protection Act provides for criminal sanctions for most provisions, including the duty to inform the data subject and the duty to file a prior notification of processing operations to the DPA. Penalties range from €600 to €600,000 and include, in specific cases, imprisonment of up to two years. The publication of a judgment may also be ordered, together with other measures that may constitute a serious threat to the data controller, such as confiscation of the support media, an order to erase the data or a prohibition on using the personal data for up to two years. There is no requirement to establish any harm or injury as a result of a breach of the Data Protection Act for the sanctions to apply, but obviously the existence of such harm or injury may have an impact on the judicial authorities' decision whether to prosecute.

ii General obligations for data handlers

Data controllers must notify the DPA of any automated data processing operation. Such a notification is a mere filing and can be done by filling in an online form and submitting a signed copy to the DPA. Any changes to the data processing operation must also be notified. Notification is only required for automated processing (and not for manual files) with certain limited exemptions (e.g., payroll and personnel administration, accounting and client or supplier administration).

Non-sensitive personal data may be processed if the processing is:

a carried out with the data subject's consent;
b necessary for the performance of a contract with the data subject;
c necessary for compliance with a legal obligation;
d necessary to protect the vital interests of the data subject;
e necessary for the public interest or in the exercise of official authority; or
f necessary for the data controller's or recipient's legitimate interests, except where overridden by the interests of the data subject.

In addition, the processing must comply with the general principles of data processing, which implies that personal data is to be:

a processed fairly and lawfully;
b collected for specific, explicit and legitimate purposes, and not processed in a manner incompatible with those purposes;
c adequate, relevant and not excessive;
d accurate and, where necessary, up to date; and
e kept in an identifiable form for no longer than necessary.

Sensitive personal data (i.e., personal data related to racial or ethnic origin, sexual orientation, religious or political beliefs, union membership, or health or judicial information) may only be processed if the processing:

a is carried out with the data subject's explicit written consent;
b is necessary for a legal obligation in the field of employment law;
c is necessary to protect the vital interests of the data subject where the data subject is unable to give consent;
d is carried out by a non-profit body and relates to members of that body or persons who have regular contact with it;
e relates to data made public by the data subject;
f is necessary for legal claims; or
g is necessary for medical reasons.

In practice, the legitimate interest condition is frequently relied upon as a ground for processing non-sensitive personal data. It should be noted, however, that the DPA finds that obtaining the unambiguous consent of the data subject is best practice and that the legitimate interest condition is only a residual ground for processing.

Except with respect to the processing of sensitive personal data, where consent of the data subject must be provided in writing, Belgian law does not impose any formalities regarding obtaining consent to process personal data. Such consent may be express or implied, written or oral, provided it is freely given, specific and informed. However, as consent should be unambiguous as well, it is recommended to obtain express and written consent for evidential purposes.

With respect to the processing of employees' personal data, the DPA finds that such processing should be based on legal grounds other than consent, in particular the performance of a contract with the data subject, since obtaining valid consent from employees is considered difficult (if not impossible) given their subordinate relationship with the employer.

As far as the data subjects' right of access, correction and removal is concerned, Belgian law provides that a data controller must provide a data subject access to his or her data upon request and free of charge. The data subject has the right to have inaccurate data corrected or deleted and, in certain cases, he or she may object to decisions being made about him or her based solely on automatic processing. To exercise this right, the data subject must send a dated and signed request to the data controller, who must confirm the amendment or deletion within one month to the data subject and, where possible, to the third parties to whom the incorrect data was communicated. If the data are to be used for direct marketing purposes, the data subject also has the right to object, free of charge, to the processing and the data controller must inform the data subjects of this right.

iii Specific regulatory areas

Although Belgium has not adopted a sectoral approach towards data protection legislation, there are nevertheless separate regulations in place for certain industries and special (more vulnerable) data subjects. In addition to the Data Protection Act and the Royal Decree of 13 February 2001, specific laws have been adopted to provide additional protection for data subjects in the following sectors:

a camera surveillance: the installation and use of surveillance cameras is governed by the Camera Surveillance Law of 21 March 2007;

b workplace privacy: the installation and use of surveillance cameras for the specific purpose of monitoring employees is subject to Collective Bargaining Agreement No. 68 of 16 June 1998 concerning the camera surveillance of employees. In addition, the monitoring of employees' online communication is subject to the rules laid down in Collective Bargaining Agreement No. 81 of 26 April 2002 concerning the monitoring of electronic communications of employees.

c electronic communications: the Electronic Communications Act of 13 June 2005 contains provisions on the secrecy of electronic communications and the protection of privacy in relation to such communications. Furthermore, the Electronic Communications Act imposes requirements on providers of telecommunication and internet services regarding data retention, the use of location data and the notification of data security breaches;

d medical privacy: the Patient Rights Act of 22 August 2002 governs, *inter alia*, the use of patients' data and the information that patients need to receive in this respect; and

e financial privacy: the financial sector is heavily regulated. For instance, the use of credit card information for profiling violates consumer credit legislation, which clearly states that (1) personal data collected by financial institutions can only be processed for specific purposes, (2) only some data can be collected, and (3) it is prohibited to use the data collected within the credit relationship for direct marketing or prospection purposes. Belgian legislation also requires that information be deleted when its retention is no longer justified.

Noteworthy in an EU context is the fact that jointly with the entry into force of the GDRP, the Network and Information Security Directive (the NIS Directive) should be transposed into national law by the EU Member States by 25 May 2018. In addition to the specific data protection rules above, the NIS Directive will add a legal basis for higher cybersecurity standards in respect of certain 'essential' services.

The NIS Directive applies in particular to operators of essential services (OESs). OESs can be found in the following industries:

a energy (electricity, oil and gas);

b transportation (air, rail, water and road);

c banking and financial market infrastructure;

d health and drinking water supply and distribution; and

e digital infrastructure.

To ensure an adequate level of network and information security in these sectors and to prevent, handle and respond to incidents affecting networks and information systems, the NIS Directive sets out the following obligations for these OESs:

a the obligation to take appropriate technical and organisational measures to manage the risks posed to their network and information systems, and to prevent or minimise the impact in the event of a data breach; and

b the obligation to notify the competent authority, without undue delay, of all incidents with a 'significant impact' on the security of the core services provided by these operators. To assess the impact of an incident, the following criteria should be taken into account: (1) the number of users affected; (2) the duration of the incident; (3) the

geographical spread with regard to the area affected by the incident; and (4) in relation to certain OESs, the disruption of the functioning of the service and the extent of the impact on economic and societal activities.

The notification obligations, preventive actions and sanctions under the NIS Directive should increase transparency regarding network and information security and heighten awareness of cybersecurity risks in the above-mentioned essential services.

iv Technological innovation and privacy law

Cloud computing

In February 2016, the DPA issued advice on the use of cloud computing services (Advice No. 10/2016 of 24 February 2016 on the Use of Cloud Computing by Data Controllers), which set out a number of key principles to be guaranteed in the contractual relationship between data subjects and cloud service providers, *inter alia*, pertaining to legal certainty, confidentiality, data subjects' rights, data localisation, international data transfer restrictions, data breach notification, government access, technical and organisational information security measures.

Furthermore, the DPA also set out certain guidelines for cloud service providers in their capacity as data controllers, such as: (1) the clear identification of data and data processing activities before migrating the data to the cloud environment, thereby giving due consideration to the nature and sensitivity of the data; (2) contractual and technical requirements for the provision of cloud services; (3) the obligation to identify the most suitable cloud solution; (4) the performance of a risk analysis; and (5) the extension of information to the data subjects about the storage of their personal data in a cloud.

Big-data analytics

The DPA released in March 2017 a report on the use of big data, on which stakeholders could comment until 11 April 2017.

The report aims to reconcile the need for legal certainty with the application of big data in current and future applications, especially in the light of the forthcoming GDPR. The recommendations made in the report cover various aspects, such as data protection compliance and respect for data subjects' rights. It is not the intention of the DPA to curtail unnecessarily the use of big-data applications as they are often very useful to society. Given that the deadline for comments expired in April, the DPA is expected to take a position and issue a statement on the use of big data soon.

Automated profiling

The DPA has not yet issued any recommendation or opinion on automated profiling. It can be expected, however, that it will take a position similar to the position of the Article 29 Working Party. The Working Party adopted an advice paper on profiling on 13 May 2013, in which it stated that Article 20 of the Data Protection Regulation should be improved by including additional elements to provide for a balanced approach on profiling and mitigate the risks for data subjects. This implies:

a more transparency;

b an increase of the data subjects' control;

c more responsibility and accountability of data controllers; and
d a 'balanced' and case-by-case approach taking into account the degree of intrusiveness of a specific processing type or measures on data subjects.

Cookies

The use of cookies is regulated by Article 129 of the Electronic Communications Act, as amended by the Act of 10 July 2012. The latest amendment provides that cookies may only be used with the prior consent of the data subject (i.e., opt-in rather than opt-out consent), who must be informed of the purposes of the use of the cookies as well as his or her rights under the Data Protection Act. The consent requirement does not apply to cookies that are strictly necessary for a service requested by an individual. The user must be allowed to withdraw consent free of charge.

On 4 February 2015, the DPA issued an additional draft recommendation on the use of cookies in which it provided further guidance regarding the type of information that needs to be provided and the manner in which consent should be obtained. This requires an affirmative action by the user, who must have a chance to review the cookie policy beforehand. This policy must detail each category of cookie with their purposes, the categories of information stored, the retention period, how to delete them and any disclosure of information to third parties.

According to the DPA, consent cannot be considered validly given by ticking a box in the browser settings.

In January 2017, the European Commission published the draft text of the new e-Privacy Regulation, which will become directly applicable in Belgium and replace all the current national rules relating to, *inter alia*, cookies after its adoption in May 2018 (together with the entry into force of the GDPR). The current draft Regulation allows consent to be given through browser settings provided that this consent entails a clear affirmative action from the end user of terminal equipment to signify his or her freely given, specific, informed and unambiguous consent to the storage and access of third-party tracking cookies in and from the terminal equipment. This entails that internet browser providers will have to significantly change the way their browsers function for consent to be validly given via browser settings.

In addition, the proposal clarifies that no consent has to be obtained for non-privacy-intrusive cookies that improve the internet experience (e.g., shopping-cart history) or cookies used by a website to count the number of visitors. Note, however, that this is still a draft text, so it remains to be seen which text will eventually be adopted.

Electronic marketing

Electronic marketing and advertising is regulated by the provisions of Book XII (Law of the Electronic Economy) of the Code of Economic Law, as adopted by the Act of 15 December 2013.

The automated sending of marketing communications by telephone without human intervention or by fax is prohibited without prior consent.

When a company wants to contact an individual personally by phone (i.e., in a non-automated manner) for marketing purposes, it should first check whether the individual is on the 'do-not-call-me' list of the non-profit organisation DNCM. Telecom operators

should inform their users about this list and the option to register online. If the individual is registered on the list, the company should obtain the individual's specific consent before contacting him or her.

Furthermore, the proposal for the new e-Privacy Regulation (already touched on in the context of cookie rules) obliges marketing callers to always display their phone number or use a special prefix that indicates a marketing call. Again, as this is only a draft text, it is not certain that this obligation will effectively be imposed on marketing callers.

Likewise, the use of emails for advertising purposes is prohibited without the prior, free, specific and informed consent of the addressee pursuant to Section XII.13 of the Code of Economic Law. This consent can be revoked at any time, without any justification or any cost for the addressee. The sender must clearly inform the addressee of its right to refuse the receipt of any future email advertisements and on how to exercise this right using electronic means. The sender must also be able to prove that the addressee requested the receipt of electronic advertising. The sending of direct marketing emails does not require consent if they are sent to a legal entity using 'impersonal' electronic contact details (e.g., info@company.be). The use of addresses such as john.doe@company.be, however, remains subject to the requirement for prior consent.

Unless individuals have opted out, direct marketing communications through alternative means are allowed. Nonetheless, the Data Protection Act prescribes a general obligation for data controllers to offer data subjects the right to opt out of the processing of their personal data for direct marketing purposes.

Employee monitoring

Employee monitoring is strictly regulated under Belgian law. Apart from the rules embedded in the Camera Surveillance Act of 21 March 2007, which provide that the use of CCTV requires a separate registration with the DPA, the monitoring of employees by means of surveillance cameras in particular is subject to the provisions of Collective Bargaining Agreement No. 68 of 16 June 1998. Pursuant to this Agreement, surveillance cameras are only allowed in the workplace for specific purposes:

a the protection of health and safety;
b the protection of the company's assets;
c control of the production process; and
d control of the work performed by employees.

In the latter case, monitoring may only be on a temporary basis. Employees must also be adequately informed of the purposes and the timing of the monitoring.

With respect to monitoring of emails and internet use, Collective Bargaining Agreement No. 81 of 26 April 2002 imposes strict conditions. Monitoring cannot be carried out systematically and on an individual basis. A monitoring system of emails and internet use should be general and collective, which means that it may not enable the identification of individual employees. The employer is only allowed to proceed with the identification of the employees concerned if the collective monitoring has unveiled an issue that could bring damage to the company or threaten the company's interests or the security of its IT infrastructure. If the issue only relates to a violation of the internal (internet) policies or the code of conduct, identification is only allowed after the employees have been informed of the fact that irregularities have been uncovered and that identification will take place if irregularities occur again in the future. In 2012, the DPA issued a specific recommendation

on workplace cyber-surveillance. In this regard, the DPA advises employers to encourage employees to label their private emails as 'personal' or to save their personal emails in a folder marked as private. Furthermore, companies should appoint a neutral party to review a former or absent employee's emails and assess whether certain emails are of a professional nature and should be communicated to the employer.

Finally, GPS monitoring in company cars is only allowed under Belgian law with respect to the use of the company car for professional reasons. Private use of the company car (i.e., journeys to and from the workplace and use during private time) cannot be monitored.

Right to be forgotten

In a judgment issued on 12 May 2016, the Belgian Supreme Court ruled that the right to be forgotten also applies to electronic archives of newspapers. The Supreme Court argued that the online publication of a case from over 20 years ago (a traffic accident reported in *Le Soir* in 1994), was likely to cause damage to the individual in the present. According to the Supreme Court, this would affect the individual's right to privacy in a disproportionate manner, notwithstanding the interests of the newspaper and its freedom of expression (see Section VII).

The right to be forgotten, or the right to erasure (i.e., an individual's right to have once public data about oneself removed from public access or to have private information erased) will also be buttressed by the GDPR. Pursuant to Article 17 of the GDPR, an individual has the right to demand that a data controller erase all personal data, without undue delay, on a number of occasions (e.g., no longer necessary for its purpose and unlawfully processed).

Although the right to be forgotten or to have data erased is not an absolute right and there are some limitations to it (e.g., freedom of expression and information, and reasons of public interest or public health), this right belongs to the individual. As such, a data controller cannot waive or opt out of compliance. If none of the exceptions of Article 17 apply, compliance with this right is mandatory. In making compliance mandatory, the GDPR will shift to the data controller the burden of proving that it falls under an exception of Article 17.

IV INTERNATIONAL DATA TRANSFER

Cross-border data transfers within the EEA or to countries that are considered to provide adequate data protection in accordance with EU and Belgian law are permitted. Transfers to other countries are only allowed if the transferor enters into a model data transfer agreement (based on the EU standard contractual clauses) with the recipient or if the transfer is subject to binding corporate rules (BCRs).

If an international data transfer is concluded under the EU standard contract clauses, a copy of these must be submitted to the DPA for information. The DPA will check their compliance with the standard contractual clauses and will subsequently inform the data controller whether the transfer is permitted. Data controllers need to wait for this confirmation from the DPA before initiating their international data transfer.

In the case of non-standard *ad hoc* data transfer agreements, the DPA will examine whether the data transfer agreement provides adequate safeguards for the international data transfer. If the DPA believes that the safeguards are adequate, the Ministry of Justice will, on verifying the entity's compliance with the applicable procedural rules, approve the agreement by Royal Decree.

If a data controller gives 'sufficient guarantees' for adequate data protection by adopting BCRs, a copy of the BCRs also needs to be sent to the DPA for approval. Pursuant to the Protocol of 13 July 2011 between the DPA and the Ministry of Justice, if the DPA's opinion is favourable, the Ministry of Justice will, on verifying that the process specified in the Protocol has been followed, approve the BCRs by Royal Decree.

Data transfers to the United States also used to be allowed if the recipient had committed to the Safe Harbor Principles. In its ruling of 6 October 2015, however, the CJEU concluded that the Safe Harbor regime is invalid and does not prevent national data protection authorities from assessing the adequacy of the protection granted by US recipients that are Safe Harbor-certified, and from prohibiting transfers to the United States (or imposing stricter conditions). This gave rise to negotiations between the EU and the United States regarding the legal framework for the data transfers. On 12 July 2016, the European Commission adopted the EU–US Privacy Shield, which meets the requirements as set by the CJEU (i.e., adequate protection of personal data and clear safeguard and transparency obligations).

After approximately a year of the EU–US Privacy Shield being in place, at the end of September 2017, officials from the US government, the European Commission and EU data protection authorities gathered in Washington to review it for the first time. They examined the administration and enforcement of the Privacy Shield, including commercial and national security-related matters, as well as broader US legal developments. The conclusion was that the Privacy Shield continues to ensure an adequate level of data protection, but that there is room for improvement. To achieve this, the European Commission has drawn up a list of recommendations on the functions of the Privacy Shield that need to be improved by the US authorities. The United States and the EU continue to collaborate and remain committed to ensuring the Privacy Shield functions as intended.

As an exemption to the above, transfers to countries not providing adequate protection are also allowed if the transfer:

a is made with the data subject's consent;
b is necessary for the performance of a contract with, or in the interests of, the data subject;
c is necessary or legally required on important public interest grounds or for legal claims;
d is necessary to protect the vital interests of the data subject; or
e is made from a public register.

V COMPANY POLICIES AND PRACTICES

Although companies are not explicitly required under Belgian law to have online privacy policies and internal employee privacy policies, in practice they need to have such policies in place. This results from the obligation, under Belgian data protection law, for data controllers to inform data subjects of the processing of their personal data (including the types of data processed, the purposes of the processing, the recipients of the data, the retention term, information on any data transfers abroad, etc.). As a result, nearly all company websites contain the required information in the form of an online privacy policy.

Likewise, companies often have a separate internal privacy policy for their employees, informing the latter of the processing of their personal data for HR or other purposes. Such a policy sometimes also includes rules on email and internet use. Some companies include the privacy and data protection information in their work regulations. This is the document

that each company must have by law and that sets out the respective rights and obligations of workers and employers. The work regulations also provide workers with information about how the company or institution employing them works and how work is organised.

The appointment of a chief privacy officer is not very common in Belgium, except within large (and mostly multinational) corporations. Such corporations often also have regional privacy officers. In smaller companies, the appointment of a chief privacy officer is rare. However, given the increasing importance of privacy and data security, even smaller companies often have employees at management level in charge of data privacy compliance (often combined with other tasks).

In this respect, it should be noted that in Belgium, unlike some other European countries, the appointment of an independent data protection officer, who is responsible for compliance and acts as the go-to person for the authorities, is not required by law.

Although it is only considered best practice at present, the upcoming GDPR contains an obligation to conduct a data protection impact assessment (DPIA) for high-risk data processing activities. The DPA has taken the liberty of issuing recommendations on the DPIA requirement of the GDPR. In addition to the non-exhaustive list of processing activities as envisaged by the GDPR (i.e., any processing that entails a systematic and extensive evaluation of personal aspects that produce legal effects; any processing on a large scale of special categories of data; and any systematic monitoring of a publicly accessible area on a large scale), the DPA clarifies its position on what qualifies as high risk, when a DPIA must be conducted, what it should entail and when it should be notified of the results of a DPIA. The main takeaway of the DPA's statement is that it should only be notified of processing activities where the residual risk (i.e., the risk after mitigating measures have been taken by the controller) remains high. Whether the DPA's position will be supported at EU level remains to be seen, since the interpretation of DPIA methodologies is in principle an EU-level matter.

A substantial number of companies have conducted privacy audits in the past decade to get a clear view on their data flows and security measures. These audits have often resulted in the implementation of overall privacy compliance projects, including the review and update of IT infrastructure, the conclusion of data transfer agreements or adoption of BCRs and the review and update of existing data processing agreements with third parties.

In large organisations, it is considered best practice to have written information security plans. Although this is also not required by law, it proves very useful, as companies are required to present a list of existing security measures when they notify their data processing operations to the DPA. The DPA has also recommended that companies have appropriate information security policies to avoid or address data security incidents.

On 14 June 2017, the DPA published a recommendation on processing-activity record-keeping. As from the entry into force of the GDPR in 2018, organisations processing personal data within the EU must maintain records of their processing activities. Organisations with fewer than 250 employees are exempted from keeping such records, unless their processing activities:

a are likely to result in a risk to the rights and freedoms of data subjects (e.g., automated decision-making);

b are not occasional; or

c include sensitive data.

On the basis of the above-mentioned non-cumulative conditions, it may be expected that basically all organisations processing personal data will have to maintain records of their processing activities in practice, even if they employ fewer than 250 people.

In substance, these records should contain information on who processes personal data, what data is processed and why, where, how and for how long data is processed.

VI DISCOVERY AND DISCLOSURE

Pursuant to the Belgian Code of Criminal Procedure, the public prosecutors and the examining magistrates have the power to request the disclosure of personal data of users of electronic communications services (including telephone, email and internet) in the context of criminal investigations. Examining magistrates may also request technical cooperation of providers of electronic communications service providers and network operators in connection with wiretaps.

The personal and territorial scope of application of these powers is currently the subject of a heated debate before the Belgian Supreme Court and criminal courts. In 2009, Yahoo! was prosecuted for non-compliance with the provisions of the Code of Criminal Procedure, as it had refused to disclose certain personal data related to a Yahoo! account that had been used in connection with a drug-related criminal offence. In addition, last year, Skype was charged with non-compliance as a result of its alleged lack of technical cooperation in connection with a wiretap on the communication of one of its Belgian users (see also Section II). The discussion in both cases deals with two issues: first, can Yahoo!, Skype and similar service or software providers be considered as providers of electronic communications services under Belgian law; and second, does the duty of cooperation set forth in the Belgian Code of Criminal Procedure apply to foreign entities that have no physical presence (no offices, infrastructure, servers, etc.) in Belgium – and if so, can it be enforced against them by the Belgian courts?

A detailed discussion of both questions is beyond the scope of this chapter, but it is interesting to note that the Supreme Court has already issued two surprising decisions in the *Yahoo!* case that may have far-reaching consequences. In its first decision, the Court has extended the scope of the definition of providers of electronic communications services, so that it includes not only service providers that take care of the transmission of signals and data over the electronic communications networks, but also 'anyone offering a service that allows its customers to obtain, receive or spread information via an electronic communications network'. This new definition seems problematic for multiple reasons. First, the Supreme Court disregards the very clear definition of 'providers of electronic communications services' set forth in the Act of 13 June 2005 on electronic communications. Second, its own definition is very vague and gives courts a great margin of appreciation, which goes against the principle of legal certainty (in particular in criminal matters). However, it can be expected that in the future, the duty to disclose personal data will apply not only to traditional internet access providers and telephone companies, but also to a wide variety of online software or service providers. Currently, the Belgian parliament is debating a draft proposal of the law that intends to extend the scope of application of the cooperation duty to all service providers meeting the definition offered by the Supreme Court.

The second decision of the Supreme Court in the *Yahoo!* case is even more important from an international perspective: the Court ruled that even though Yahoo! had no physical presence in Belgium, the provisions of the Code of Criminal Procedure applied to it, as the

'service' it offers can be used in Belgium via the internet. It also stated that the fact that the public prosecutor sent the request to disclose personal data directly to Yahoo! in the United States (without making use of the procedures set out in the applicable treaties regarding mutual legal assistance in criminal matters) did not make the request invalid or unenforceable.

This latter decision essentially implies that foreign entities offering an online service (or software) are subject to Belgian criminal law as soon as the software service can be used in Belgium, and that the Belgian public prosecutor has the power to enforce Belgian criminal law against such foreign entities without the intervention or assistance of the judicial authorities of the state of residence of these entities. Obviously, this position taken by the Supreme Court would also imply that foreign judicial authorities could enforce their national criminal law against service providers located in Belgium and do so without assistance from the Belgian courts.

Finally, on 1 December 2015, the Supreme Court put an end to the legal proceedings by rejecting the appeal, thereby confirming the Court of Appeal's decision, which has caused important implications for the international system of mutual legal assistance in criminal matters.

Analogously, the Court of First Instance of Mechelen condemned Skype Communications SARL, a Luxembourg-based entity, for refusing to set up a wiretap in Mechelen in its ruling of 27 October 2016. The wiretap concerned was ordered by the Mechelen examining judge in the framework of an investigation into a Skype user. Again, the Belgian authorities ignored the European Convention on Mutual Assistance in Criminal Matters and imposed the wiretap order directly on Skype in Luxembourg. The Court of Mechelen applied a similar reasoning to that applied by the Supreme Court in the *Yahoo!* case and held that the alleged offence, namely the refusal to provide technical assistance, can be deemed to have occurred in the place where the information should have been received, regardless of where the operator was established.

Notably, the context of the *Skype* case is totally different from the situation in the *Yahoo!* case. While the *Yahoo!* case involved the mere refusal to disclose information to the Belgian authorities (Section 46 *bis* Section 1 of the Belgian Code of Criminal Procedure), the *Skype* case concerns the refusal to set up a wiretap (Article 88 *bis* Section 2 and Article 90 *quater* Section 2 of the Belgian Code of Criminal Procedure). The latter is undeniably a completely different type of measure, encompassing not only the provision of information, but also material acts by Skype and the necessary technical infrastructure to perform them, which Skype did not have in Belgium. Unsurprisingly, Skype appealed against this judgment before the Court of Appeal of Antwerp. The final judgment is expected before the end of 2017.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Belgian enforcement agency with responsibility for privacy and data protection is the DPA.

The DPA's mission is, *inter alia*, to monitor compliance with the provisions of the Data Protection Act. To this end, the DPA has general power of investigation with respect to any type of processing of personal data and may file a criminal complaint with the public prosecutor. It may also institute a civil action before the president of the court of first instance. However, the DPA cannot impose any administrative penalties upon individuals or

organisations. In response to complaints filed by individuals, it will try to reach a solution by mediating between the parties, but if no solution can be found, the parties will need to go to court to settle their dispute.

Whereas the DPA currently only has limited sanctioning powers, the Belgian Council of Ministers recently approved a draft law to reform the DPA in light of the forthcoming GDPR. The reformed DPA will be an independent administrative authority with legal personality and extensive investigative and sanctioning powers, composed of six different bodies: an executive committee, a general secretariat, a front-line service, a knowledge centre, an inspection service and a dispute chamber.

The executive committee, composed of the leaders of the five other bodies, will be responsible for the adoption of the DPA's general policies and strategic plan.

A general secretariat will be established for the reception and processing of complaints and to inform citizens about their data protection rights.

The inspection service will function as the investigating body of the DPA, with a wide array of investigative powers (e.g., interrogation of individuals).

The front-line service will have a singular role in providing guidance (e.g., with regard to adequate data protection techniques under the GDPR) and supervising data controllers and processors and their compliance with data protection legislation.

Led by six experts in the field, the knowledge centre will provide public decision-makers with the necessary expertise to understand the technologies likely to impact on the processing of personal data.

The dispute chamber, composed of a president and six judges, will be able to impose sanctions of up to €20 million or up to 4 per cent of the total worldwide annual turnover of the infringing company.

As well as the above-mentioned bodies being established under the auspices of the reformed DPA, an independent think tank will be set up to reflect society as a whole, both participants in the creation of the digital world and those affected by it, and to provide the executive committee with a broad vision and guidance as it negotiates current and future data protection challenges.

Another novelty of the draft law is that, along with natural persons, legal persons, associations or institutions will also be able to lodge a complaint of an alleged data protection infringement.

In spite of the expansion of the DPA's powers, the government unfortunately decided not to increase its budget. In other words, the DPA will have to perform more tasks but with the same resources. Given the fact that, at present, the DPA only rarely conducts raids and investigations because of a lack of resources, it remains to be seen whether in future the DPA will be little more than a toothless tiger, new powers notwithstanding.

Recent investigations by the DPA concern the data processing practices of Belgium's largest telecom service providers: Telenet and Proximus.

The DPA investigated Telenet's direct marketing practices and examined whether Telenet was collecting its customers' prior and specific opt-in consent. In contrast to its regime for new customers, Telenet applied an opt-out regime for existing customers. According to the DPA, such an opt-out approach is unlawful as it does not adhere to the consent requirements laid down in the Data Protection Act (i.e., prior, free, specific, unambiguous and informed consent). Furthermore, the DPA raised concerns about whether Telenet customers had been

informed of the new processing activities in a clear and understandable manner. At present, the DPA is further investigating the matter and has engaged in discussions with Telenet to address the concerns raised.

Proximus, on the other hand, is planning to offer a tailored advertising service based on anonymised and aggregated (location) data of its end users. After investigation, the DPA found that the location data and otherwise encrypted data could still be connected to the data of an identified customer and therefore concluded that the Proximus anonymisation process was inadequate. Further to the DPA's findings, Proximus adapted its service to ensure adequate anonymisation of its customers' location data.

ii Recent enforcement cases

The most important recent enforcement case undertaken by the DPA is the one initiated against Facebook in June 2015. In May 2016, the Court of Appeal of Brussels overruled the interlocutory judgment of the President of the Court of First Instance imposing interim measures on Facebook, partially on jurisdictional grounds and partially because of a lack of urgency. For now, the DPA awaits the decision of the Court of First Instance of Brussels on the merits of the case and, particularly, the Court's answer to the question of who has jurisdiction over Facebook and is competent to judge the alleged privacy infringements. This decision on the substance of the DPA's claim is expected to be delivered later this year. The DPA has already been investigating the possibility of bringing the case before the Belgian Supreme Court if its claim against Facebook is rejected (see also Section II).

In a non-binding opinion, an advocate general of the Court of Justice of the European Union has recently stated that Facebook should indeed adhere to the national privacy rules of EU Member States if it collects and processes data from users in those Member States and has a physical establishment (e.g., a sales office) on their territory. Hence, the advocate general opposes Facebook's argument that it should comply only with Ireland's privacy legislation, the country where it has its European headquarters.

In addition to the *Facebook* case, the most important enforcement cases before the Belgian courts are the *Yahoo!* and *Skype* cases, discussed in Sections II and VI.

With respect to cases handled by the DPA, no information about individual complaints has been made publicly available. According to the DPA's Annual Report of 2016, the DPA processed 4,491 requests or complaints (an increase of 299 compared with 2015), including requests for information, mediation and control. The majority of information requests related to the use of CCTV, data subjects' rights, the right to one's image, data processing registrations and contractual clauses.

iii Private litigation

Private plaintiffs may seek judicial redress before the civil courts on the basis of the general legal provisions related to tort or, in some cases, contractual liability. In addition, they may file a criminal complaint against the party that committed the privacy breach. Financial compensation is possible, to the extent that the plaintiff is able to prove the existence of damages as well as the causal link between the damage and the privacy breach. Under Belgian law, there is no system of punitive damages.

Class actions were traditionally not possible under Belgian law until 1 September 2014, when a new Act on Class Actions entered into force. So far, there are no known cases of class action lawsuits filed in connection with data privacy.

In April 2016, the Supreme Court ruled in favour of the right to be forgotten. The case concerned the online disclosure of an archived database of a famous Belgian newspaper, which would result in the publication of the full name of a driver who was involved in a car accident in 1994 in which two people died. Both the Court of Appeal and the Supreme Court considered the right to be forgotten essential in this case and ruled in favour of a limitation of the right of freedom of expression (see also Section III.iv).

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Organisations based or operating outside Belgium may be subject to the Belgian data protection regime to the extent that they process personal data in Belgium. Physical presence in Belgium (either through a local legal entity or branch office, with or without employees, or through the use of servers or other infrastructure located on Belgian territory) will trigger the jurisdiction of Belgian privacy and data protection law even if the personal data that is processed in Belgium relates to foreign individuals. Foreign companies using cloud computing services for the processing of their personal client or employee data may therefore be subject to Belgian law (with respect to such processing) if the data is stored on Belgian servers.

In principle, the mere provision of online services to persons in Belgium, without actual physical presence, will not trigger Belgian jurisdiction. However, as discussed under Section VI, according to a recent Supreme Court decision, the Belgian judicial authorities would have jurisdiction over foreign entities providing online services or software to users in Belgium, even if they are not present in Belgium. This is certainly an issue to follow up, as it may have an important impact on the territorial scope of application of Belgian law, especially in light of the entry into force of the GDPR on 25 May 2018.

It should be noted that the GDPR will even apply to data controllers having no presence at all (establishment, assets, legal representative, etc.) in the EU but who process EU citizens' personal data in connection with goods or services offered to those EU citizens; or who monitor the behaviour of individuals within the EU.

IX CYBERSECURITY AND DATA BREACHES

As a member of the Council of Europe, Belgium entered into the Council's Convention on Cybercrime of 23 November 2001. Belgium implemented the Convention's requirements through an amendment of the Act of 28 November 2000 on cybercrime, which introduced cybercrime into the Belgian Criminal Code. With the Act of 15 May 2006, Belgium also implemented the requirements of the Additional Protocol to the Convention on Cybercrime of 28 January 2003 concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

As previously mentioned, the CCB will:

a monitor Belgium's cybersecurity;
b manage cybersecurity incidents;
c oversee various cybersecurity projects;
d formulate legislative proposals relating to cybersecurity; and
e issue standards and guidelines for securing public sector IT systems.

Since becoming operational at the end of 2015, the CCB has carried out several awareness campaigns; for instance, in the context of the Petya ransomware cyberattacks and the 'CEO

fraud' (a large-scale scam where cybercriminals contact a company as the alleged CEO of another big company with a request to make an important payment into the first company's bank account).

Furthermore, the management of CERT, which has been in the hands of Belnet since 2009, was transferred to the CCB in December 2016. The transfer of all CERT activities is part of the continuing coordination of Belgian cybersecurity and is aimed at assisting companies and organisations in the event of cyber-incidents by providing advice both about finding solutions when such incidents arise and about preventing incidents occurring.

Additionally, the Belgian Cyber Security Coalition, which is a partnership between parties from the academic world, public authorities and the private sector, was established in October 2014. Currently, more than 50 key participants from across the three sectors are active members. These include large financial institutions, universities, consultancy companies, professional organisations and government bodies. The main goals of the Coalition are to raise awareness about cybersecurity, exchange know-how, take collective actions in the fight against cybercrime and support governmental and sectoral bodies in setting policies and determining ways to implement these policies.

With respect to data breach notifications, Article 114/1, Section 2 of the Electronic Communications Act requires companies in the telecommunications sector to notify immediately (within 24 hours) personal data breaches to the DPA, which must transmit a copy of the notification to the Belgian Institute for Postal Services and Telecommunications. If there is a breach of personal data or the privacy of individuals, the company must also notify the data subjects affected by the breach.

The Data Protection Act does not, however, provide for a general data breach notification obligation, as is provided for in the GDPR. In 2013, the DPA was confronted by a series of data security incidents of which it only became aware after those incidents were published in the media. Unable to change the legislation itself (which, of course, would require legislative intervention), the DPA issued a recommendation upon its own initiative stating that it considered data breach notifications to be an inherent part of the general security obligations incumbent on any data controller.

More specifically, the DPA's recommendation stressed the importance of conducting risk assessments and implementing appropriate security measures (including security policies), and noted that incident management policies should specify that 'in the event of public incidents the competent authorities [i.e., the DPA] must be informed within 48 hours of the causes and damage'. Although the concept of a 'public incident' is not explained in greater detail, one may assume that this term refers to an incident in which data are lost, destroyed, altered or disclosed in a way that is likely to become known to the public or the DPA via, for example, the media, the internet or complaints from individuals. It is to be expected that this recommendation by the DPA will be transposed into a legal obligation as soon as the GDPR enters into force.

In relation to data security, the International Chamber of Commerce in Belgium and the Federation of Enterprises in Belgium, together with the B-CCentre, have taken the initiative to create the Belgian Cyber Security Guide in cooperation with Ernst & Young and Microsoft. The Guide is aimed at helping companies protect themselves against cybercriminality and data breaches. To that effect, it has listed 10 key security principles and 10 'must do' actions, including user education, protecting and restricting access to

information, keeping IT systems up to date, using safe passwords, enforcing safe-surfing rules, applying a layered approach to viruses and other malware, and making and checking backup copies of business data and information.

X OUTLOOK

With regard to the entry into force of the GDPR next year, the overall focus of the DPA will obviously be on preparing companies, data controllers and data processors for this new EU data protection framework. To this end, the DPA has already launched a new section dedicated to the GDPR on its website and a 13-step plan for companies involved in data collection or processing, or both, to help them comply with the forthcoming new rules of the GDPR.

Apart from the strengthening of the investigative and sanctioning powers of the DPA (see Section VII), we do not expect the GDPR to result in any major changes to the Belgian situation in practice. Belgium's legislation and the interpretation given to it by the DPA have traditionally been in line with EU law and the positions of the European Commission and the Article 29 Working Party.

As mentioned above (see Section VII), the investigative and sanctioning powers of the DPA will be significantly expanded under the GDPR. Unfortunately, the government decided not to increase its budget. As a result, the DPA is expected to have only very limited resources to support the use of its new powers and launch data protection investigations or conduct raids. We believe that the prospect of prosecutions being initiated by the DPA will remain rather unlikely given these budgetary constraints. Nevertheless, in the event of a complaint being lodged with the DPA or of a data breach incident, it will have broader competence to examine the complaint and to impose higher sanctions on the alleged violator. In its assessment of alleged data protection violations, the DPA will definitely check whether sufficient efforts have been made to meet the requirements laid down in the GDPR.

Appendix 1

ABOUT THE AUTHORS

ASTREA

Louizalaan 235
1050 Brussels
Belgium
Tel: +32 2 215 97 58
Fax: +32 2 216 50 91
sds@astrealaw.be
www.astrealaw.be

STEVEN DE SCHRIJVER

Astrea

Steven De Schrijver is a partner in the Brussels office of Astrea. He has more than 20 years of experience advising some of the largest Belgian and foreign technology companies, as well as innovative entrepreneurs on complex commercial agreements and projects dealing with new technologies. His expertise includes e-commerce, software licensing, website development and hosting, privacy law, IT security, technology transfers, digital signatures, IT outsourcing, cloud computing, advertising, drones, robotics and social networking.

Steven has also been involved in several national and cross-border transactions in the IT, media and telecom sectors. He participated in the establishment of the first mobile telephone network in Belgium, the establishment of one of the first e-commerce platforms in Belgium, the acquisition of the Flemish broadband cable operator and network, and the acquisition and sale of several Belgian software and technology companies. He has also been involved in numerous outsourcing projects and data protection (now GDPR) compliance projects.

Steven is the Belgian member of EuroITCounsel, a quality circle of independent IT lawyers. He is also a board member of ITechLaw and the International Federation of Computer Law Associations. In 2012, 2014 and 2017, he was awarded the Global Information Technology Lawyer of the Year award by *Who's Who Legal* and, in 2012, he received the ILO Client Choice Award in the corporate law category for Belgium.

Steven has been admitted to the Brussels Bar. He holds a law degree from the University of Antwerp (1992) and an LLM degree from the University of Virginia School of Law (1993).

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

ISBN 978-1-910813-89-8