Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top-ranked lawyers

Data Protection & Privacy

Belgium
Lydian

chambers.com

2020

BELGIUM

Law and Practice

Contributed by:
Bastiaan Bruyndonckx, Olivia Santantonio and Liese Kuyken
Lydian see p.12

Contents

Contributed by: *Bastiaan Bruyndonckx, Olivia Santantonio and Liese Kuyken,* ***Lydian***

1. Basic National Regime

1.1 Laws

In Belgium, the provisions on privacy and data protection are spread over various laws. The general basis of the legal provisions can be found in the Constitution, Articles 22 and 29 of which acknowledge the right to respect for private life, family life and correspondence as fundamental human rights. These provisions are very similar to international regulations in this respect, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 and the Charter of Fundamental Rights of the European Union.

Since 25 May 2018, the principal data protection legislation in Belgium, as in other Member States of the European Union, has been Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC Regulation (EU) 2016/679 (hereinafter the GDPR).

In the aftermath of the enactment of the GDPR, two Acts implementing the GDPR have been adopted in Belgium.

First of all, the Belgian legislator adopted the law of 3 December 2017 on the establishment of the Data Protection Authority, which implements the requirements of the GDPR with respect to national supervisory authorities and reforms the Belgian Commission for the Protection of Privacy (hereinafter the DPA Act). As of 25 May 2018, the Belgian Commission for the Protection of Privacy carries the name "Data Protection Authority" and has the powers and competences which the GDPR requires national supervisory authorities to possess.

A second Act, the law of 30 July 2018 on the protection of individuals with respect to the processing of personal data (hereinafter the GDPR Implementation Act), addresses the national substantive aspects of the GDPR and introduces several specifications and derogations, such as determining the age of consent for children in an online context and imposing additional security measures in relation to sensitive data. At the same time, it abolishes and replaces the 1992 Data Protection Act and the 2001 Royal Decree that implemented it.

These data protection laws are supplemented by (sector-)specific legislation such as the law of 13 June 2005 on electronic communications (hereinafter the Electronic Communications Act) that implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (hereinafter the ePrivacy Directive), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In addition, the Belgian Code of Economic Law deals with certain legal aspects of information society services as well as market practices and consumer protection, and provides a specific set of rules regarding the use of personal data for direct marketing purposes via electronic post (which includes email, SMS and MMS) and via telephone, fax and automatic calling machines without human intervention.

Furthermore, as regards public administrations, the Law of 3 August 2012 contains provisions relating to the processing of personal data carried out by the Federal Public Service Finance in the framework of the carrying out of its mission, and the Flemish Decree of 18 July 2008 provides a specific set of rules concerning the exchange of administrative data by regional authorities within the Flemish region.

There is also an act that regulates the installation and use of surveillance cameras, namely the Camera Act of 21 March 2007. As regards employee monitoring, Collective Bargaining Agreement N° 68 on the use of cameras in the workplace and Collective Bargaining Agreement N° 81 on the monitoring of electronic communications in the workplace are relevant.

1.2 Regulators

The former Commission for the Protection of Privacy has been known as the Data Protection Authority since 25 May 2018, and has the powers and competences which the GDPR requires national supervisory authorities to possess. Together with the change of name, the powers of the Data Protection Authority have also been greatly expanded. The Data Protection Authority is responsible for monitoring compliance with the fundamental principles of the protection of personal data within the framework of the GDPR and the laws containing provisions on the protection of the processing of personal data.

The Data Protection Authority has six bodies, which play a specific role in the evaluation of a data protection matter:

- the Executive Committee, which determines the general policy and the strategic plan;
- the General Secretariat, which provides daily support and approves, amongst others, binding corporate rules;
- the First Line Service, which assesses the admissibility of complaints and requests, and streamlines mediation proceedings;
- the Knowledge Centre, which drafts general recommendations;
- the Inspection Service, which investigates pending procedures; and
- the Dispute Chamber, which serves as an administrative court.

Investigations that are carried out by the Inspection Service of the Data Protection Authority can be initiated on the initiative of the Data Protection Authority, or following a complaint or request. The Inspection Service has extensive powers when conducting an investigation – for example, it can conduct interrogations and site searches, identify persons present at the sites being checked or users of communication services, or even consult and copy computer systems and the data they contain, as well as carry out seizures.

At the level of the Flemish Region, the Flemish Supervisory Commission has been established and is responsible for monitoring compliance with the GDPR by the Flemish public authorities. No regulator has yet been created in the Walloon or Brussels Capital Region.

The Belgian Institute for Postal Services and Telecommunications has the authority to monitor compliance with the Electronic Communications Act, and can co-operate with the Data Protection Authority to perform investigations.

Finally, the Federal Public Service Economy has the authority to control, inspect and sanction any infringement of the provisions of the Belgian Code of Economic Law, including those which relate to, eg, direct marketing.

1.3 Administration and Enforcement Process

The Data Protection Authority can launch an investigation for various reasons, with the most logical way being in response to a complaint or request, which can come from anyone and does not necessarily have to come from an interested party or data subject. A complaint will first be checked for its admissibility by the First Line Service before being forwarded to the Dispute Chamber or the Inspection Service. It entails a written procedure. In addition to the admissibility check, the First Line Service may proceed to mediation. A complaint is admissible if it is drawn up in one of the national languages (Dutch, French or German), if it contains a statement of the facts and the necessary indications for identifying the processing to which it relates, and if it falls within the competences of the Data Protection Authority. A request is admissible if it is drawn up in one of the national languages and if it falls under the powers of the Data Protection Authority. The decision of the First Line Service on the admissibility of the complaint or request must be notified to the person making the complaint or request. Where the decision on inadmissibility is taken, the First Line Service must also communicate the reasons for its inadmissibility.

In addition to the possibility to rule on complaints and requests, the Data Protection Authority may be triggered in other ways in order to process a file and conduct an investigation. In this case, the file is immediately forwarded to the Inspection Service, which may also launch an investigation on its own initiative or at the request of the Executive Committee where it has serious indications of a possible breach of the fundamental principles of personal data protection, where this is within the framework of co-operation with the data protection authority of another State or where the Data Protection Authority is seized by a judicial authority or an administrative supervisor.

The Inspection Service can also be appointed by the Dispute Chamber, which has the ability to carry out a comprehensive examination of an organisation's practices before taking a decision (although it is not obliged to do so). Once more, this is done by the Inspection Service, which is authorised to conduct investigations.

If the organisation disagrees with certain decisions of the Inspection Service, it may lodge an appeal with the Dispute Chamber. This is only possible for fairly far-reaching measures, such as interim measures, seizure and sealing.

As described in the GDPR, the Data Protection Authority has far-reaching powers to impose sanctions. If a party concerned does not agree with the decision of the Dispute Chamber, an appeal can be lodged. This appeal must be submitted to the Market Court, a separate chamber within the Brussels Court of Appeal, which has exclusive competence for complex litigation against regulators, such as the Data Protection Authority.

1.4 Multilateral and Subnational Issues

As a civil law country, Belgium has legal codes that specify all matters capable of being brought before a court, the applicable procedure, and the appropriate sanction for each offence. These codifications are the primary source of law. Belgium applies a strict hierarchy of norms, which means that there is a hierarchy between the various regulatory texts, recognising international and European norms as the most important source of law.

1.5 Major NGOs and Self-Regulatory Organisations

In Belgium, several NGOs are actively dealing with privacy-related issues. For example, there are human rights organisations such as the "*Liga voor Mensenrechten*", which is actively involved in protecting privacy, and consumer organisations such as "*Test-Achats*", which organise privacy awareness campaigns aimed at consumers.

Moreover, the Federation of Enterprises of Belgium (FEB / VBO) is really active in the protection of personal data, and is now entitled to initiate class actions/collective redress under Belgian law.

Various self-regulatory organisations are also taking measures in view of protecting privacy. For example, various professional groups educate their members on privacy and have adopted rules in deontological codes, such as the Council for Journalism and the Medical Association.

1.6 System Characteristics

The GDPR permitted Member States to regulate some particular elements independently. It is in this context that the Belgian legislator decided to regulate several matters in its GDPR Implementation Act, as follows:

- the minimum age for consent in an online context was lowered to 13 years;
- the regime of criminal data has been detailed;
- in some cases, the public interest has been deemed necessary; and
- additional safeguards have been provided for the processing of genetic, biometric and health-related data.

In addition, the Belgian legislator has also given its own interpretation of the administrative procedure by the DPA Act. This can therefore differ considerably from the procedure in other countries.

So far, not enough decisions have been rendered in order to determine whether the Data Protection Authority has enforced the GDPR and the GDPR Implementation Act more or less aggressively than other Supervisory Authorities.

1.7 Key Developments

In the last 12 months, the Belgian Data Protection Authority has rendered a number of decisions,, and is more active than ever before. The first fine was issued by the Data Protection Authority on 28 May 2019. However, in addition to imposing administrative fines, the Data Protection Authority has issued reprimands and banned certain processing operations. The sanctions are diverse, as are the matters involved.

On 2 April 2019, the Data Protection Authority issued a ban on processing activities that were infringing data protection laws, which could not be rectified. The case involved the placement of cameras in the common areas of student rooms, which was considered to be disproportionate to the objective of combating vandalism, damage and nuisance.

On 19 September 2019, the Data Protection Authority imposed a fine on a merchant who, as the sole means of creating a loyalty card, used the reading of the electronic identity card, which was considered disproportionate and obtained without valid consent.

Furthermore, on 17 December 2019, the Data Protection Authority imposed an administrative fine of EUR15,000 on a company that manages a website with legal news and information, as the cookie practices of the company did not comply with the provisions of the GDPR and the Belgian provisions implementing the ePrivacy Directive.

On the same date, the Data Protection Authority imposed a fine of EUR2,000 on a non-profit association that provides specialised nursing care, for failure to comply with the access request of a data subject.

1.8 Significant Pending Changes, Hot Topics and Issues

On 28 January 2020, the Data Protection Authority released its 2019-2025 Strategic Plan, in which it describes its vision for the coming years, defines its priorities and strategic objectives, and lists the necessary means to achieve its objectives. The Data Protection Authority intends to raise awareness among data subjects and data controllers, and to enforce the rules effectively. In the following years, the Data Protection Authority will focus on five sectors, including telecommunications and media, government, direct marketing, education, and small- and medium-sized enterprises.

In the 2019-2025 Strategic Plan, the Belgian Data Protection Authority indicated that it will focus its actions on the following aspects of the GDPR:

- the role of the data protection officer, with a particular focus on companies that have appointed a DPO without allowing them to act in accordance with the GDPR;
- the lawfulness of data processing activities, and more particularly the (abusive) processing of personal data based on the legitimate interests legal basis; and
- data subjects' rights, specifically the scope of some of these rights.

The Data Protection Authority also has a number of social issues high on its agenda, such as photos and cameras, online data protection and sensitive data.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The Belgian legislator has further detailed the GDPR in two Acts: the GDPR Implementation Act and the DPA Act.

These two Acts are more far-reaching than the GDPR in several areas, and fill some gaps left by the GDPR with Belgian law. While the DPA Act establishes the Belgian Data Protection

Authority and lays down the procedural framework before the refurbished authority, the GDPR Implementation Act is substantive law. This analysis will concentrate on what matters are different in Belgium compared to the GDPR.

The GDPR Implementation Act broadens the scope for the appointment of a data protection officer (DPO) if the processing of data involves a high risk, mainly for companies that process personal data either (i) obtained from or on behalf of federal public authorities, or (ii) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. The former Commission for the Protection of Privacy issued guidelines on DPO and, more particularly, on incompatibilities with other functions in April 2017.

As regards processing for archiving, scientific research and statistical purposes, the GDPR Implementation Act provides further obligations and a derogation from data subjects' rights. The GDPR Implementation Act provides for the possibility of further processing for scientific or historical research or statistical purposes, meaning for a purpose other than the purpose for which the data was initially collected. Furthermore, the GDPR Implementation Act obliges the anonymisation or pseudonymisation of the personal data directly after collection.

The GDPR Implementation Act somewhat restricts the rights of data subjects. It is foreseen that intelligence agencies, the Coordination Unit for Threat Analysis and other specialised police forces can process personal data without being subject to transparency obligations towards data subjects. In addition, there are exemptions from several obligations when processing is done for journalistic purposes or for the purposes of academic, artistic or literary expression, such as the prohibition on processing sensitive and judicial data, the duty to inform the data subject and the requirement to give access to the data at the data subject's request.

Along with the vast majority of EU Member States, Belgium reduced the age of consent for information society services to 13 years instead of 16 years.

Belgian law also provides for broad protection of the national register number. This type of data cannot be accessed or used, unless there is a legal obligation to do so, or a specific authorisation is obtained from the relevant administration.

The Data Protection Authority does not require the conduct of privacy impact analyses in certain circumstances, but has published guidelines on the data protection impact assessment (DPIA) as well as the list of processing operations where a DPIA does or does not need to be carried out.

Other points, such as the application of "privacy by design" or "by default", have so far not been further discussed by the Data Protection Authority, so the guidelines of the European Data Protection Board need to be taken into account.

2.2 Sectoral and Special Issues

The processing of special categories of personal data (like union membership, sexual orientation, political or philosophical beliefs) is notably possible under the GDPR for reasons of substantial public interest. What is certainly already covered by this term is listed in the GDPR Implementation Act. Such personal data is allowed to be processed by associations whose main statutory objective is the defence and promotion of fundamental rights and freedoms of man, which carry out the processing for this purpose and have obtained an authorisation from the King. In addition, the foundation for missing and sexually exploited children, "Child Focus", can always process such data. Finally, special personal data relating to sexual life can be processed by associations whose main statutory purpose is the evaluation, supervision and treatment of persons whose sexual behaviour can be qualified as a crime, and which have been recognised and subsidised for this purpose.

As regards the processing of genetic, biometric and health-related data, the GDPR Implementation Act introduces several additional requirements, such as the obligation to list the types of individuals who have access to such data, and the obligations to ensure that these individuals are subject to legal, statutory or other similar confidentiality obligations. There is, however, no specific legal ground (other than consent that is challenged) in case of processing of such data by insurers or employers, for instance.

As regards criminal offence data, the same obligations shall apply. In addition, the GDPR Implementation Act Law lists the persons that are allowed to process such data, given their specific capacity or for specific purposes. The GDPR Implementation Act also provides for legal grounds to process such data (eg, consent).

The Belgian legislator has provided for strict telecom secrecy in the Electronic Communications Act. Without having obtained the consent of all other persons directly or indirectly concerned, no one may disclose the information, identification or data relating to electronic communications to a third party. It is also part of criminal law, with the secrecy of private communications and telecommunications being protected on the one hand by Article 314bis of the Criminal Code and, on the other, by Articles 90ter to 90decies of the Code of Criminal Proceedings. Only in exceptional circumstances can traffic data be retained for a maximum period of one year in the context of compli-

ance with the obligations laid down by or pursuant to the law regarding co-operation with a number of specified authorities.

Under Belgian Law, cookies are regulated in the Electronic Communications Act, which implements Article 5 of the ePrivacy Directive. The storage of cookies (or other data) on an end user's device requires prior consent, as defined in the GDPR. For consent to be valid, it must be informed, specific and freely given, and must constitute a real and unambiguous indication of the individual's wish. This does not apply if the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or if the cookie is strictly necessary to provide an "information society service" (ie, a service provided over the internet) requested by the subscriber or user, which means that it must be essential to fulfil the user's request. The use of cookies is only authorised if the person has had clear and precise information concerning the purpose of the processing and his or her rights, before any use of cookies. The controller must also freely give the opportunity to the subscriber or users to withdraw their consent at any time. Information must also be provided with respect to the term of validity of the cookies used. The Data Protection Authority has already expressed its views on cookies in a decision, but it has also indicated that it will issue a recommendation on this subject in the first months of 2020. The EU Commission intends to pass a new ePrivacy Regulation to replace the respective national legislation in the EU Member States. The ePrivacy Regulation appears to be a long-term process; drafts have been in progress since 2017 (and the last one was published on 21 February 2020), but the EU Council has failed to reach agreement on its approved text.

Regarding the other categories of personal data, there are no specific recommendations from the Data Protection Authority. However, when reading the guidelines on the DPIA published by the former Commission for the Protection of Privacy, it is clear that certain personal data – such as financial data, children data, location data, tracking and behavioural advertising – is also sensitive data, although, strictly speaking, it does not fall within the definition of sensitive/special categories of data.

2.3 Online Marketing

Under the Belgian Code of Economic Law, direct marketing via electronic post (which includes email, SMS and MMS) is only authorised where the recipient specifically and freely consented to it (opt-in). Opt-out is only permitted in two specific cases:

- sending electronic direct marketing to legal entities using a non-personal email address (eg, info@company.com); and
- sending electronic direct marketing to existing customers about identical or similar products, provided a number of strict conditions on information are met.

It should be noted that, even when the recipient previously consented to the use of his/her electronic contact details for direct marketing purposes, he/she can at any time oppose the further use of his/her electronic contact details for direct marketing purposes. The restrictions apply to business-to-consumer marketing and also in a business-to-business context.

For direct marketing by telephone, a national opt-out register (the so-called "Robinson List") exists, and businesses carrying out direct marketing by telephone are required to check this list in advance.

Direct marketing by post does not require the prior consent of the addressee but can be carried out on an opt-out basis. For direct marketing (on a personalised basis) by post, a national opt-out register has been put in place, but is only mandatory for businesses that are members of the Belgian Direct Marketing Association. For non-personalised advertising by post, anyone can ask to be provided with "Stop-Pub" stickers to stick on their mailbox.

For marketing by fax or via automated calling machines without human intervention, the prior consent of the recipient is required (opt-in).

The Data Protection Authority published a draft of its new guidelines on direct marketing on 17 January 2020.

2.4 Workplace Privacy

The protection of employees' privacy and personal data in Belgium is guaranteed in various ways. Besides the application of general data protection rules, there are specific protection mechanisms in place that apply to employees. In Belgium, several collective bargaining agreements (CBAs) have been concluded to provide specific privacy protection for employees. First of all, CBA no. 68 of 16 June 1998 lays down the conditions and principles with regard to camera surveillance in the workplace. Secondly, CBA no. 81 of 26 April 2002 develops a specific regime concerning the electronic monitoring of internet and emails.

Under Belgian law, the employee's privacy right is not absolute. The monitoring of employees, therefore, always requires a balancing between the employees' right to privacy embedded in Belgian legislation and the employer's legitimate interests to protect the business or comply with its own obligations. As part of the authority of the employer, there might be legitimate interests to monitor employees as far as the processing is relevant and proportionate.

The monitoring of electronic communications is only permitted under Belgian law for one of the exhaustively listed purposes of CBA no. 81. Permanent monitoring cannot be justified in

any case, as it is considered disproportionate. Monitoring is particularly permitted for the following purposes: preventing unauthorised acts, ensuring the security and/or proper technical operation of the IT network, protecting the economic, commercial and financial interests of the company, and compliance with internal policies.

Camera surveillance in the workplace is only permitted to attain the objectives specifically stipulated in CBA no. 68, and only if the employer has informed the employees of such surveillance. The objectives relate to health and safety, the protection of the company's goods, the monitoring of the production process or the monitoring of the employee's work. Only in the first three cases can the monitoring be continuous, provided that the monitoring of the production process relates to the monitoring of machinery.

Currently, no specific obligation or legislation exists on whistle-blowing hotlines in Belgium. However, a whistle-blowing hotline must comply with Belgian data protection rules, according to a recommendation of the Belgian Data Protection Authority of 29 November 2006.

2.5 Enforcement and Litigation

In principle, class actions are not permitted under Belgian law as the Judicial Code requires personal interest in order for a claim to be admissible. The Code of Economic Law allows for actions for collective redress/class actions, but such actions are rather rare.

Furthermore, the DPA Act provides that anyone can submit a written, dated and signed complaint or request to the Data Protection Authority, not just interested parties. However, the majority of cases are instigated by stakeholders.

The Dispute Chamber of the Data Protection Authority has the power to issue a warning, to order that the data subject's requests to exercise his/her rights be met, to order that the data subject be informed of the security problem, to order that the processing be temporarily or permanently frozen, restricted or prohibited, to order that the processing be rectified, restricted or erased, and to order that the recipients of the data be informed thereof, to order the withdrawal of recognition of certification bodies, to impose periodic penalty payments, to impose administrative pecuniary sanctions, to order the suspension of cross-border data flows to another State or to an international body, to transfer the file to the public prosecutor's office in Brussels in order to conduct a criminal investigation, and to publish its decisions on the website of the Data Protection Authority.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

The European Directive of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (the Data Protection Law Enforcement Directive) was implemented by the GDPR Implementation Act.

The Belgian Code of Criminal Proceedings permits the accessing of personal data necessary for the prevention, investigation and prosecution of criminal offences and the execution of sanctions. During the investigation, the judicial authorities will collect data as evidence. The way data is collected is subject to strict rules under the Belgian Code of Criminal Proceedings.

When someone is convicted of a crime by the court, that conviction is entered in the criminal record. The criminal record thus provides an overview of every conviction a person has already received.

Police forces, however, do not have access to the criminal record. Police forces work together and exchange data, using the General National Database, in which data on persons, organisations, places, events, vehicles, objects and numbers is registered by police entities. The database is managed by both the federal and local police, for both their administrative and judicial police tasks.

3.2 Laws and Standards for Access to Data for National Security Purposes

Following several terrorist attacks in Europe, the Belgian legislator has modified the criminal law in order to optimise the fight against terrorism. Since the so-called Terro I Act, telephone tapping has been possible for all terrorist offences from Book II, Title I ter of the Criminal Code. This means that interception of private communications is not only possible for all current terrorist offences, but also for all future terrorist offences. A second law, the Terro II Act, provided for a new dynamic database to ensure efficient co-operation between the various police services and State Security, and to collect data on so-called Foreign Terrorist Fighters. This common database was created to aggregate personal data and other information held by different public services in their databases. The Data Protection Authority exercises indirect supervision. If a person believes that he/she is included in the database, he/she can contact the Data Protection Authority with the request to consult the data concern-

ing him/her. The Data Protection Authority will carry out the necessary checks and verify whether the conditions for inclusion in the database have been complied with. If necessary, the Data Protection Authority will ask for the necessary changes to be made. The person concerned will then be informed that the verification has been carried out, without revealing its content.

3.3 Invoking a Foreign Government

At present, there is no legal basis in Belgian law for private companies to collect and/or directly transfer personal data from Belgium in response to a request from foreign governments.

The American CLOUD Act (Clarifying Overseas Use of Data Act) explicitly empowers US enforcement authorities to order providers of certain communication and cloud services to provide the data of their users, even if they are on servers located abroad. The CLOUD Act gives foreign governments the opportunity to conclude a bilateral agreement with the United States. The conditions should ensure robust protection of privacy, freedom of expression and other fundamental rights.

Under the CLOUD Act, access to personal data in Europe will constitute a violation of the GDPR. In Recital 115, the GDPR literally states that legislation of third countries that make an extraterritorial application with direct regulation of data transfer is contrary to international law and constitutes an obstacle to the protection of individuals guaranteed in the GDPR. The GDPR does provide for possibilities of transfer to third countries, but these possibilities are applied very strictly. Under Art. 48 GDPR, only mutual legal assistance treaties (so-called MLATs) or comparable international agreements provide a permissible basis for the extraterritorial transfer of personal data. Therefore, the CLOUD Act does not constitute a legal basis for transferring data to the United States, and is considered illegal.

3.4 Key Privacy Issues, Conflicts and Public Debates

In order to implement European Regulation 2019/1157, which came into force on 2 August 2019, Belgium will soon start the systematic registration of fingerprints on identity cards. The federal government put the procedure for this on paper at the end of 2019, in the long-awaited implementing decree by the Act of 25 November 2018, which contains the legal basis for the inclusion of fingerprints on the chip of the e-ID. The introduction of fingerprints on identity cards was opposed by many. The Data Protection Authority was not a fan and rejected the initial draft because of a disproportionate restriction of the right to privacy and protection of personal data.

4. International Considerations

4.1 Restrictions on International Data Issues

Within the European Union, the principle of free movement of personal data exists, with the consequence that no specific measures need to be taken with regard to cross-border data transfers.

Data transfers to other jurisdictions outside the European Economic Area (EEA) can only take place in the following circumstances:

- if the transfer is to a country recognised by the European Commission as providing an adequate level of data protection;
- if the business has implemented one of the required safeguards as specified by the GDPR (such as Standard Contractual Clauses or Binding Corporate Rules); or
- if derogations specified in the GDPR are applicable to the transfer.

On 25 May 2018, the European Data Protection Board set out in its Guidelines (2/2018) that a "layered approach" should be taken with respect to these transfer mechanisms. If no adequacy decision is applicable, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

The GDPR Implementation Act does not foresee any further requirements for international data transfers.

4.2 Mechanisms That Apply to International Data Transfers

Under the GDPR, transfers are only allowed to countries that provide an adequate level of protection, or under one of the other provisions of Chapter 5 of the GDPR.

The European Commission has compiled a list of third countries that have an adequate level of protection, and it is permitted to transfer personal data to countries that fall under an adequacy decision. Currently, the following countries have been white listed by the European Commission: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

The United States also appears on the list of third countries with adequacy decisions, but this is limited to a special regulation: the Privacy Shield. The organisations that join the Privacy Shield must adhere to the privacy rules established by the US Department of Commerce and the EU Commission within the Privacy Shield.

In case of transfers that are not subject to an adequacy decision, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR.

Standard Contractual Clauses are standard sets of contractual terms and conditions drafted by the EU Commission which can be used for international data transfers outside the EEA. These contractual obligations warrant compliance with the GDPR's requirements, and extend the scope of these rules to territories that are not considered to offer adequate protection to the rights and freedoms of data subjects. International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the GDPR, and have prior approval from the relevant data protection authority.

Another option for international data transfers within a group of companies is the Binding Corporate Rules. All employees and entities within the group must comply with this internal code of conduct. The Binding Corporate Rules will always need approval from the relevant data protection authority. Most importantly, the Binding Corporate Rules will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the Binding Corporate Rules require an explanation on the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

4.3 Government Notifications and Approvals

It is likely that the international data transfer will require prior approval from the relevant data protection authority, unless they have already established a GDPR-compliant mechanism for such transfers, as set out in **4.2 Mechanisms That Apply to International Data Transfers**.

In any case, most of the safeguards outlined in the GDPR need initial approval from the relevant data protection authority, such as the establishment of Binding Corporate Rules.

4.4 Data Localisation Requirements

Under Belgian law, there have been no specific data localisation requirements since the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data, which has been applicable since 28 May 2019 and aims to remove obstacles to the free movement of non-personal data across Member States and IT systems in Europe.

4.5 Sharing Technical Details

In Belgium, companies are not obliged to communicate their use of specific technical equipment or software, nor the source code, to the government or the Belgian Data Protection Authority.

4.6 Limitations and Considerations

Please refer to **3.3 Invoking a Foreign Government**.

4.7 "Blocking" Statutes

The Regulation of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, known as the EU Blocking Regulation, which was amended in 2018, prohibits European businesses from complying with certain US extraterritorial sanctions and export controls targeting Iran and Cuba. This EU Blocking Regulation was implemented in Belgium by the Act of 2 May 2019, which imposes administrative fines of up to 10% of a company's turnover in case of breach of the EU Blocking Regulation.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

When it comes to facial recognition, the GDPR and Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, should be taken into account. Where the processing of personal data (in this case visual images) entails risks, a data impact assessment is necessary and, where the nature of the processing "in particular when using new technologies" entails a high risk for the rights and freedoms of data subjects, a consultation of the supervisory authority is necessary. In Belgium, in the case of police camera surveillance, one should also look at the Law on the Police Force of 5 August 1992 and possibly the Camera Act of 21 March 2007. This tangle of laws ensures that there is no unanimity on this subject. The further use of data from facial recognition cameras is, in principle, possible today when people are travelling in cars: the photo of the driver and passenger of the vehicle being scanned with ANPR may be processed in the ANPR technical database. The Belgian legislator has not yet provided any clarification, and it is therefore not currently used in Belgium.

Drones are regulated in Belgium by the Royal Decree of 10 April 2016 on the use of remotely controlled aircrafts in the Belgian airspace. Since the Royal Decree, anyone wishing to fly a drone for private use is only allowed to do so above private property, at a maximum height of 10 metres above the ground and in accordance with privacy and data protection laws, as drones

can collect a very wide range of information. For example, a drone can not only receive video images or photographs but, depending on the technology with which it is equipped, it can also eavesdrop on communication signals, detect faces, track and identify objects and people, record their movements or signal movements that are considered abnormal. Given this great amount of possibilities, it is therefore important that drones are used in accordance with the data protection legislation. The Belgian legislator acknowledged the importance of this, as it is included in the training for drone operators. In order to avoid various inconveniences, the European legislator has chosen to harmonise the rules. This will, for example, allow a licence in one Member State to apply in other Member States. In this regard, the Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems was published on 11 June 2019. This Regulation lays down the requirements for the design and manufacture of drones and the rules to be complied with by non-European operators when flying a drone in Europe. The Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft lays down the rules and procedures for the operation of drones in Europe. The new rules will replace the existing national rules relating to drones from 1 July 2021. In other words, Member States will have two years to prepare for this transition. The Belgian legislator has not published any new legislation so far.

Regarding IoT or automated decision-making, profiling or artificial intelligence, on 17 January 2020 the Data Protection Authority approved a draft Act prohibiting life and health insurers from processing health sensor data. The Belgian legislator wants to prevent insurers from providing discounts to the "healthy ones", even if the insurers have their policy-holders' consent. There is a fear that such processing could lead to infringements of privacy and to unlawful discrimination.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Organisations in Belgium have not yet established any protocols for digital governance or fair data practice review boards or committees to address the risks of emerging or disruptive digital technologies.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

Please refer to **1.7 Key Developments**.

5.4 Due Diligence

A due diligence investigation – where the prospective buyer or seller wants to gather as much information as possible about a company – involves a large amount of data, including personal data. For example, contracts, such as employment contracts or contracts with suppliers, will often contain personal data. These contracts are made available in a data room in order to gain a better insight into the company.

The Belgian Data Protection Authority decided in 2016 that the processing of personal data is possible in the context of an acquisition of a company. It indicated that the legal basis for processing is the legitimate interest in making this information available to a prospective buyer. It must, of course, be ensured that the processing remains proportionate and that no unnecessary personal data is processed. In addition, efforts should be made to make the data anonymous where possible. Confidentiality clauses (NDAs) should be foreseen with regard to persons having access to the data room. It may also be recommended that the data rooms are protected by technical limitations such as not being able to download documents, thereby protecting personal data.

It goes without saying that, in the event of a due diligence investigation, the data subjects must be informed that their personal data will be processed. This possibility can be provided for contractually in advance.

As far as data rooms are concerned, recourse is often made to an external virtual data room, which will therefore act as processor. This requires the conclusion of a processing contract between the company and the service provider, and the processor will have to provide for security measures to prevent data breaches.

5.5 Public Disclosure

Belgium does not currently have any non-privacy/data protection-specific laws that mandate disclosure of an organisation's cybersecurity risk profile or experience.

5.6 Other Significant Issues

There are no further significant issues.

Lydian has an Information Governance & Data Protection (Privacy) team of eight specialised lawyers, who represent clients, large and small, from all industry sectors, on all aspects of information governance and data protection. The team covers corporate privacy risk management, (GDPR) compliance, international data transfers, records management, e-discovery, (direct) marketing, e-commerce, cybersecurity and cybercrime. It provides services ranging from legal advice to integrated consulting on corporate privacy risk management, as well as legislative strategic policy advice and legal compliance. The firm also litigates on behalf of clients in data protection-related matters. It advises clients on global data protection and privacy compliance challenges, including by taking data protection and privacy rules into account on a global basis. Lydian is one of the few independent law firms in Belgium operating outside a US/UK law firm banner, and is a popular referral choice for foreign firms seeking a high-quality law firm in Belgium with recognised skills in data protection.

Authors

Bastiaan Bruyndonckx is a partner in Lydian's Commercial & Litigation department and heads the Information & Communications Technology (ICT) practice as well as the Information Governance & Data Protection (Privacy) practice. He has a particular focus on information governance, privacy, data protection and cybersecurity, and advises businesses in a broad range of industry sectors. Bastiaan is a fellow of the Belgian American Educational Foundation (BAEF) and a member of the International Association of Privacy Professionals (IAPP). He is a regular speaker at conferences on privacy and data protection, and also regularly publishes in international legal reviews such as Computerrecht, Privacy & Informatie, DataGuidance, Tijdschrift voor Privacy en Persoonsgegevens and Bulletin des Assurances.

Olivia Santantonio is counsel in Lydian's Information & Communications Technology (ICT), Information Governance & Data Protection (Privacy) and Intellectual Property practices. She frequently advises on data protection issues regarding, inter alia, the obligations and liability of the data controller and data processor, the transfer of data into and out of the EU and the processing of sensitive data. She also frequently assists clients to assess their level of compliance with the new legislation, and assists them in data subject requests, data breaches or Data Protection Authority requests. She also often drafts and reviews privacy policies as well as (data processing) agreements. Olivia is regularly invited to speak at conferences and seminars, and is a member of the International Association of Privacy Professionals (IAPP) and the International Association for the Protection of Intellectual Property (AIPPI).

Liese Kuyken is an associate in Lydian's Information & Communications Technology (ICT), Information Governance & Data Protection (Privacy) and Intellectual Property practices. She frequently assists clients in data protection matters regarding, for instance, data processing agreements, privacy and cookie policies, and data subject rights. She also specialises in global privacy issues (GDPR compliance, contracts review, binding corporate rules, etc). Liese is involved in several procedures regarding the processing of personal data, before the Belgian Data Protection Authority as well as Belgian courts. She has recently published in the legal review Tijdschrift voor Privacy en Persoonsgegevens.

Lydian

Havenlaan - Avenue du Port 86c b113
Tour & Taxis
1000 Brussels
Belgium

Tel: +32 2 787 90 00
Fax: +32 2 787 90 99
Email: info@lydian.be
Web: www.lydian.be