Chambers
Global Practice
Guides

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

Data Protection & Privacy 2022

Belgium: Law & Practice
and
Belgium: Trends & Developments

Bastiaan Bruyndonckx, Olivia Santantonio
and Liese Kuyken
Lydian

practiceguides.chambers.com

BELGIUM

Law and Practice

Contributed by:
Bastiaan Bruyndonckx, Olivia Santantonio and Liese Kuyken
Lydian see p.20

CONTENTS

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 conventions in this respect, particularly 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.

General Data Protection Regulation (GDPR)

Since 25 May 2018, the main 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 (the GDPR).

Acts implementing 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 Belgian Data Protection Authority, which has implemented the requirements of the GDPR with respect to national supervisory authorities and reformed the Belgian Commission for the Protection of Privacy (the DPA Act). On 25 May 2018, the Belgian Commission for the Protection of Privacy became the "Data Protection Authority" and has the powers and competences that 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 (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 the processing of 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 (the Electronic Communications Act) that implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the ePrivacy Directive), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector, and the European Electronic Communications Code. The ePrivacy Directive will be replaced by the ePrivacy Regulation in the future.

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 public authorities within the Flemish region.

The Camera Act of 21 March 2007 regulates the installation and use of surveillance cameras.

As regards employee monitoring, Collective Bargaining Agreement No 68 on the use of cameras in the workplace and Collective Bargaining Agreement No 81 on the monitoring of electronic communications in the workplace are relevant.

1.2 Regulators

Data Protection Authority

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 that 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: it is now 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 Litigation 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 Data Protection Authority's own initiative, 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.

Other Regulators

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

The Belgian Institute for Postal Services and Telecommunications has the authority to monitor compliance with the Electronic Communications Act. However, in the context of the implementation of the European Electronic Communications Code in Belgium at the end of 2021, certain of its powers (notably in respect of the processing of personal data, such as cookies and call monitoring) have been formally transferred to the Data Protection Authority.

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 relating to direct marketing, for example.

1.3 Administration and Enforcement Process

Investigations

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 Litigation 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);
- contains a statement of the facts and the necessary indications for identifying the processing to which it relates; and
- 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 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 a complaint or request is found inadmissible, 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 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 if there are 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.

Litigation Chamber

The Inspection Service can also be appointed by the Litigation 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).

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

Sanctions

As set out in the GDPR, the Data Protection Authority has far-reaching powers to impose sanctions. However, administrative fines cannot be imposed upon public authorities. The Belgian Constitutional Court rejected an appeal that argued that the exemption for public authorities would be discriminatory, and the Constitutional Court held that the difference of treatment between public and private entities is justified and non-discriminatory.

Procedure

The procedure before the Litigation Chamber has undergone step-by-step fine-tuning through several decisions of the Litigation Chamber. As a body of active governance (and not an administrative disputes body), the Litigation Chamber is not subject to the general procedural rules described in either the Judicial Code or the administrative legislation. However, like any body of active governance, the Data Protection

Authority (including its Litigation Chamber) is subject to the principles of good administration (impartiality, motivation of decisions, legal certainty, etc). Because of the unique position of the Litigation Chamber, at the end of 2020 and in 2021 it issued four guidelines relating to:

- the publication of the decisions taken by the Litigation Chamber;
- penalty payments;
- the language used in proceedings before the Litigation Chamber; and
- the discontinuance of the proceedings before the Litigation Chamber.

If one of the parties concerned does not agree with the decision of the Litigation Chamber, an appeal can be lodged. This appeal must be submitted to the Market Court, which is a separate chamber within the Brussels Court of Appeal and has exclusive competence for complex litigation against regulators such as the Data Protection Authority. Depending on the decision of the Market Court, the case could be finally decided by the Market Court or referred back to the Litigation Chamber, which will then have to take a new decision, taking into account the parts of the former decision that were challenged by the Market Court.

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 organises privacy awareness campaigns aimed at consumers and is entitled to act as a representative of the consumer group in a collective redress action in Belgium.

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

Following the Ministerial Decree of 30 September 2020, NOYB – European Center for Digital Rights (founded notably by Maximilien Schrems) is also entitled to act as a representative of the consumer group in a collective redress action in Belgium.

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 certain particular elements independently. In this context, 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 for the processing of criminal data has been detailed;

- in some cases, 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 laid down the administrative proceedings before the Data Protection Authority in the DPA Act, which can therefore differ considerably from the proceedings in other countries.

The Data Protection Authority is rather active and the Litigation Chamber regularly imposes sanctions, including administrative fines. The highest fine – EUR600,000 – was imposed on Google Belgium for not respecting a Belgian citizen' right to be forgotten of, and for a lack of transparency in its request form to delist.

1.7 Key Developments

COVID-19

In the past two years, the Supervisory Authorities have focused in part on the COVID-19 health crisis. The EU Commission, the European Data Protection Board (EDPB) and some Data Protection Authorities, including the Belgian Data Protection Authority, have published the following:

- guidance on the legal framework of tracing apps as one of the tools of a broader set of measures for fighting the virus; and
- a number of opinions regarding draft laws or royal decrees imposing, for example, recourse to the Covid Safe Ticket (CST) or face masks in public places.

General obligations of controllers under the GDPR, such as transparency and integrity, will have to be complied with, and public health authorities and employers must always have legal grounds for the processing of personal data.

Moreover, the Belgian Data Protection Authority published an analysis of the processing of vaccination data. As vaccination is voluntary in Belgium, requesting and registering a person's vaccination status is in principle prohibited, unless the controller can rely on an exception laid down in Article 9 (2) of the GDPR, such as the explicit consent of the person concerned or a legal obligation.

In an employment context, the processing of personal data may be necessary for compliance with a legal obligation to which the employer is subject, such as obligations relating to health and safety in the workplace, or relating to the public interest, such as the control of diseases and other threats to health. The employer may ask employees to undergo a medical examination (eg, temperature check), but not on a general or systematic basis and only when required by health and safety (eg, for employees returning from risk areas). More recently, the Litigation Chamber has decided to temporarily suspend the verbal verification by a hospital network of the vaccination status of candidates for recruitment, as there was no legal basis for such processing.

Court of Justice of the European Union (CJEU)

The impact of the CJEU on the data protection landscape in past years cannot be underestimated, as many controllers struggle with the effects of the Schrems II Case, which invalidated the Privacy Shield and questioned the validity of standard contractual clauses (SCCs) (and other adequate safeguard mechanisms) for transfers of personal data to the US and other third countries. Organisations are required to re-evaluate all their data transfers to third countries if they are based on SCCs (and other adequate safeguard mechanisms) and to perform a Transfer Impact Assessment (TIA). Whether the SCCs (and other adequate safeguard mechanisms) are sufficient

safeguards for transfers to certain third countries will require further examination. For instance, in the US, it is hard to see how the concerns raised by the CJEU regarding the Privacy Shield would not apply when the SCCs are at issue and similar organisations are concerned.

Data Protection Authority

On a national level, as the GDPR has become a real buzzword, many data subjects found their way to the Belgian Data Protection Authority. In the last year, the Data Protection Authority's Inspection Service initiated a large number of investigations (either following complaints filed or on its own initiative), and its Litigation Chamber (which is an administrative body dealing with data protection matters and imposing the administrative sanctions foreseen in the GDPR) pronounced a large number of decisions. The sanctions imposed are diverse (but the fines are, with certain notable exceptions, not that high so far), as are the subject matters involved (more often, data subjects' rights, purpose limitation, legal grounds and transparency), and apply to individuals and the public and private sectors (more to the banking, insurance and telecom sectors in the latter). Nevertheless, the Litigation Chamber was somewhat tempered in its enthusiasm by the Brussels Market Court, which decides on appeals against the Litigation Chamber's decisions.

1.8 Significant Pending Changes, Hot Topics and Issues

On 14 January 2021, the Belgian Constitutional Court rendered its decision in proceedings concerning the nullity of a provision in Belgian legislation implementing the sanction mechanism under the GDPR, thereby providing for an exemption from administrative fines for the public sector. The Court recalled that the public authorities are not exempted from the obligations of the GDPR, but that the Belgian legislator chose not to impose administrative fines on them. However, the public authorities are subject to administrative non-financial sanctions, as well as criminal sanctions.

On 6 December 2021, the Data Protection Authority published a recommendation on the processing of biometric data, with the aim of providing guidelines to controllers and processors on how to interpret and comply with the GDPR when processing biometric data.

As regards to the case law of the Data Protection Authority, following the 2020–2025 Strategic Plan, the Litigation Chamber has focused on the following aspects of the GDPR and has rendered numerous decisions in this regard:

- the role of the data protection officer (DPO), with a particular focus on companies that have appointed a DPO without allowing the DPO 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 base; and
- data subjects' rights, specifically the scope of some of these rights.

Each year, the Data Protection Authority publishes a management plan in which it converts the strategic goals of the 2020–2025 Strategic Plan into concrete objectives for the coming year. The management plan for 2022 is yet to be published.

2021 was a difficult year for the Belgian Data Protection Authority. The European Commission questioned the independence of the Data Protection Authority and found that some of its members could not be considered to be free of outside influence because they either report to a management committee dependent on the Belgian government, participated in government projects to detect COVID-19 contacts, or

are members of the Information Security Committee. As a consequence, the Data Protection Authority did not remain free of political and internal conflicts in 2021, leading to one of the Data Protection Authority's directors voluntarily stepping down. A proposed law currently pending could potentially resolve this in 2022.

"A Europe fit for the digital age" is one of the six priorities of the European Commission for 2019–2024. As digital technology is increasingly impacting people's lives, the EU's digital strategy aims to make this transformation work for people and businesses, while helping to achieve the EU's target of a climate-neutral Europe by 2050. Various initiatives have already been taken within the framework of the European Commission's digital strategy, including a series of new – and often bold – legislative proposals, which will have a material impact on businesses and organisations inside (and often also outside) the EU:

- the Digital Services Act (DSA);
- the Digital Markets Act (DMA);
- the Data Governance Act;
- the Artificial Intelligence Regulation;
- the Omnibus Directive (already adopted but not yet implemented in Belgian law); and
- the Digital Operational Resilience Act (DORA).

At the same time, existing legal frameworks are being re-assessed and updated, such as the review of the Network and Information Systems (NIS) Directive and the e-Privacy Regulation. Member states were required to implement the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, which sets out the minimum standards for the enhanced protection of whistle-blowers, particularly through protection against retaliation and claims for damages, before 17 December 2021. Like many other member states, Belgium did not manage to complete the implementation into national law before this deadline, but a preliminary draft act is currently circulating and is expected to be submitted to Parliament and voted on by the end of June 2022.

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.

GDPR Implementation Act

The GDPR Implementation Act broadens the scope for the appointment of a DPO if the processing of data involves a high risk, mainly for companies that process personal data that is obtained from or on behalf of federal public authorities, or that is 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 DPOs and, more particularly, on incompatibilities with other functions in April 2017. The Data Protection Authority published a DPO box in order to assist DPOs to perform their tasks correctly.

As regards processing for archiving, scientific research and statistical purposes, the GDPR Implementation Act provides further obligations

and a derogation from data subjects' rights. It provides for the possibility of further processing for scientific or historical research or statistical purposes – ie, for a purpose other than that for which the data was initially collected. Furthermore, the GDPR Implementation Act mandates the anonymisation or pseudonymisation of the personal data directly after collection.

The GDPR Implementation Act restricts the rights of data subjects in certain areas. It is foreseen that intelligence agencies, the Coordination Unit for Threat Analysis and other specialised police forces will be able to 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 upon 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.

National Register Number

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 unless specific authorisation is obtained from the relevant administration. Following Regulation 2019/1157/EU, which entered into force on 2 August 2021, member states will be obliged to include two fingerprints in interoperable digital formats in national ID cards. Prior to this Regulation, however, Belgium already adopted a similar obligation through Article 27 of the Law of 25 November 2018 on various provisions relating to the National Register and population registers. The legality of such controversial provision was contested by many and was appealed before the Belgian Constitutional Court. However, after a balancing of interests, the Constitutional Court concluded that the inclusion of digital fingerprints on ID cards does not violate the fundamental right to respect for private life.

The Data Protection Authority does not require privacy impact analyses to be conducted 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 not yet been the subject of further guidance from 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

Personal Data

The processing of special categories of personal data (such as 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 the fundamental rights and freedoms of humans, which carry out the processing for this purpose and have obtained an authorisation by Royal Decree. 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.

The GDPR Implementation Act introduces several additional requirements regarding the processing of genetic, biometric and health-related data, such as the obligation to list the types of individuals who have access to such data, and the obligation to ensure that these individuals are subject to legal, statutory or other similar confidentiality obligations. However, no specific legal grounds in addition to those set out in the GDPR have been provided for. The Act of 8 October 2020 was enacted to address the processing of health sensor data in the insurance sector; please refer to **5.1 Addressing Current Issues in Law**.

The same obligations apply in relation to criminal offence data. The GDPR Implementation Act lists the persons that are allowed to process such data, given their specific capacity or for specific purposes. It also provides for legal grounds to process such data (eg, explicit written consent).

Electronic Communications Act

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 information, identification or data relating to electronic communications to a third party. This 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 hand, by Articles 90ter to 90decies of the Code of Criminal Proceedings.

Only in exceptional circumstances could traffic data be retained for a maximum period of one year in the context of compliance with the obligations laid down by or pursuant to the law regarding co-operation with a number of specified authorities. However, the Constitutional Court annulled this so-called Data Retention Act in a judgment of 22 April 2021, ruling that the general and indiscriminate retention of data relating to electronic communications violates the right to respect for private life and to protection of personal data. Meanwhile, Belgium is working on a new draft Data Retention Act that again stipulates that telecom operators must keep records of customers and their traffic data for one year.

Cookies

Under Belgian Law, cookies were regulated in the Electronic Communications Act, but these provisions were moved to the GDPR Implementation Act at the end of 2021. The provisions on cookies implement 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 subscriber or users the opportunity 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 few decisions, and inserted a recommendation on this subject into the guidelines on direct marketing of 17 January 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, with the last one being published on 5 January 2021, and a version of the EU Council of Ministers was published on 10 February 2021.

Other Categories of Personal Data

There are no specific recommendations from the Data Protection Authority regarding the other categories of personal data, except on biometric data (Recommendation dated 6 December 2021).

However, when reading the DPIA guidelines published by the former Commission for the Protection of Privacy, it is clear that certain personal data – such as financial data, children's data, location data, tracking and behavioural advertising – is considered more sensitive than other data, although, strictly speaking, it does not fall within the definition of sensitive/special categories of data.

2.3 Online Marketing

Direct 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 are met.

It should be noted that, even when the recipient previously consented to the use of their electronic contact details for direct marketing purposes, they can at any time oppose the further use of their 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, there is a national opt-out register (the "Do not call me List"), which must be checked in advance by businesses carrying out direct marketing by telephone (call centres).

Direct marketing by post does not require the prior consent of the addressee but can be carried out on an opt-out basis. A national opt-out register has been put in place for direct marketing (on a personalised basis) by post, but it 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 its new guidelines on direct marketing on 17 January 2020, using a rather broad definition of what constitutes "(direct) marketing".

2.4 Workplace Privacy

Protection of Employees' Privacy and Personal Data

The protection of employees' privacy and personal data in Belgium is guaranteed in various ways. Besides the application of the general data

protection rules, there are specific protection mechanisms in place that apply to employees. 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 sets out a specific regime concerning electronic monitoring of internet use and email.

Under Belgian law, the employee's privacy right is not absolute. The monitoring of employees, therefore, always requires a balance 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.

Monitoring of electronic communications

This 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

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.

Whistle-Blowers

Member states were required to implement Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, which sets out the minimum standards for an enhanced protection of whistle-blowers, in particular through protection against retaliation and claims for damages, before 17 December 2021. Like many other member states, Belgium did not manage to complete the implementation into national law before this deadline, although a preliminary draft bill is pending but not yet published; the text should be adopted by June 2022.

2.5 Enforcement and Litigation

Class Actions

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, however, allows for actions for collective redress/class actions, but such actions are rather rare. Please refer to **1.5 Major NGOs and Self-Regulatory Organisations** regarding the entities entitled to introduce such actions.

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.

Litigation Chamber Powers

The Litigation Chamber of the Data Protection Authority has the power to:

- issue a warning;

- order that the data subject's requests to exercise their rights be met;
- order that the data subject be informed of the security problem;
- order that the processing be temporarily or permanently frozen, restricted or prohibited;
- order that the processing be rectified, restricted or erased, and order that the recipients of the data be informed thereof;
- order the withdrawal of the recognition of certification bodies;
- impose periodic penalty payments;
- impose administrative pecuniary sanctions;
- order the suspension of cross-border data flows to another State or to an international body;
- transfer the file to the public prosecutor's office in Brussels in order to conduct a criminal investigation; and
- 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, 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 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 the interception of private communications is possible not only 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 they are included in the database, they can contact the Data Protection Authority with the request to consult the data concerning themselves. 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 Foreign Government Obligations

At present, there is no specific 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.

CLOUD Act

The US 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 of which 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 the 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 Article 48 of the 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 of 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 in favour 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

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

Data Transfers to Jurisdictions Outside the EEA

Such transfers can only take place in the following circumstances:

- if the transfer is to a country that is recognised by the European Commission as providing an adequate level of data protection ("adequacy decision");
- if the undertaking has implemented one of the required safeguards as specified by the GDPR, such as Standard Contractual Clauses (these are currently under revision – a new draft of sets has been published for consultation by the EU Commission) or Binding Corporate Rules; or
- if derogations specified in the GDPR are applicable to the transfer.

It should be noted that the UK no longer forms part of the EU, so is considered a third country. However, an adequacy decision has been adopted in respect of transfers of personal data to the UK.

On 25 May 2018, the EDPB 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 contain any additional requirements for international data transfers.

In any case, the EDPB has placed international transfers of personal data high on the agenda. It has adopted Recommendations on supplementary measures to ensure compliance with the EU level of protection of personal data on 18 June 2021, and on 18 November 2021 adopted new guidelines on the interplay between Article 3 and Chapter V of the EU General Data Protection Regulation.

4.2 Mechanisms or Derogations that Apply to International Data Transfers

Adequate Protection

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 are deemed to offer 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, the Republic of Korea, Switzerland and Uruguay.

The European Commission has recognised that the UK is providing adequate protection under the GDPR as well as the Law Enforcement Directive.

Since the recent Schrems II Decision of the CJEU, the United States no longer benefits from the Privacy Shield mechanism (see **1.7 Key Developments**).

In the case of transfers that cannot benefit from an adequacy decision, undertakings must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR, and carry out a prior Transfer Impact Assessment.

SCCs

SCCs 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. SCCs have recently been revised. The European Commission issued an implementing decision on new SCCs on 4 June 2021 for the transfer of personal data to countries outside the EEA, including the UK. As of 27 September 2021, any new transfers based on SCCs are required to have adopted the new SCCs, and current data transfer agreements are required to adopt the new SCCs as of 27 December 2022. 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 Supervisory Authority. In such a case, a TIA is also required.

Binding Corporate Rules

Another option for international data transfers within a group of companies is the adoption of Binding Corporate Rules. All employees and entities within the group must comply with this internal code of conduct. Binding Corporate Rules will always need approval from the relevant Supervisory Authority. Most importantly, Binding Corporate Rules need to include a mechanism to ensure they are legally binding and enforced by every member in the group of undertakings. Among other things, 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 complaint procedures.

4.3 Government Notifications and Approvals

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

In any case, most of the safeguards outlined in the GDPR need initial approval from the relevant Supervisory 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 Foreign Government Obligations**.

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. The 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 for a breach thereof.

5. EMERGING DIGITAL AND TECHNOLOGY ISSUES

5.1 Addressing Current Issues in Law

Facial Recognition

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, 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 take into account 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 Automatic Number Plate Recognition (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

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 m above the ground and in accordance with privacy and data protection laws, as drones can collect a wide range of information. For example, not only can a drone 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 large number of possibilities, it is important that drones are used in accordance with 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.

Internet of Things (IoT), Automated Decision-Making, Profiling or Artificial Intelligence

On 8 October 2020, the Belgian legislator approved an Act prohibiting life and health insurers from processing health sensor data. The Belgian legislator intends to prevent insurers from providing discounts to the "healthy ones", even if the insurers have their policy-holders' consent. The law ensures that the policyholder cannot be refused insurance nor be subjected to higher charges simply because they do not purchase or use a connected device that processes their health data. Moreover, no difference may be made in terms of the underwriting, pricing and/or scope of coverage based on the condition that the insured applicant agrees to purchase or use a connected device that collects personal information about their lifestyle or health, agrees to share information collected by such a connected device, or based on the insurer's use of such information.

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 involves a large amount of data, including personal data. For example, employment contracts or contracts with suppliers will often contain personal data. These contracts are made available in a data room in order for a prospective buyer to gain 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 the 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 implemented for 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 the 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 and data protection (privacy) team of eight specialised lawyers, who represent large and small clients 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 and litigation department, and heads the information and communications technology (ICT) practice and the information governance and 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 also holds a CIPP/E certification. He is a regular speaker at conferences on privacy and data protection, and regularly publishes in international legal reviews such as Computerrecht, Privacy & Informatie, DataGuidance, Tijdschrift voor Privacy en Persoonsgegevens and Bulletin des Assurances.

Olivia Santantonio is a counsel in the information governance and data protection (privacy) and intellectual property practices at Lydian. She frequently advises on data protection issues regarding the obligations and liabilities of data controllers and data processors, international data transfers and the processing of sensitive data. She also frequently assists clients in assessing their level of compliance with the legislation, and in responding to data subject requests, data breaches or Data Protection Authority requests. She also offers (daily) support to DPOs. 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 and communications technology (ICT), information governance and data protection (privacy) and intellectual property practices. She frequently assists clients in data protection matters regarding data processing agreements, privacy and cookie policies, and data subject rights. She also specialises in global privacy issues (GDPR compliance, contract review, binding corporate rules, etc). Liese is involved in several proceedings regarding the processing of personal data, before the Belgian Data Protection Authority as well as Belgian courts. She teaches Media Law in the journalism programme at KU Leuven, where she educates students on issues such as privacy and image rights. Furthermore, Liese is a member of the International Association of Privacy Professionals (IAPP) and has 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

Trends and Developments

Contributed by:
Bastiaan Bruyndonckx, Olivia Santantonio and Liese Kuyken
Lydian see p.26

Data Protection in Belgium

Data protection was again high on the agenda of policymakers and authorities in 2021. In several areas, the data protection landscape changed or was further clarified in 2021. New developments are also awaited in 2022, especially at an EU level.

Exemption from Administrative Fines for the Public Sector

On 14 January 2021, the Belgian Constitutional Court rendered its decision in proceedings concerning the nullity of a provision in Belgian legislation implementing the sanction mechanism under the General Data Protection Regulation (GDPR), thereby providing for an exemption from fines for the public sector. The Court recalled that the public authorities are not exempted from the obligations of the GDPR, but that the Belgian legislator chose not to impose administrative fines on them. However, the public authorities are subject to administrative non-financial sanctions, as well as criminal sanctions.

Recommendation on Biometric Data

On 6 December 2021, the Data Protection Authority published a recommendation on the processing of biometric data, with the aim of providing guidelines to controllers and processors on how to interpret and comply with the GDPR when processing biometric data. The recommendation only recognises two possible legal grounds for the processing of biometric data in Belgium: explicit consent (Article 9 (2) (a) of the GDPR) and substantial public interest (Article 9 (2) (g) of the GDPR). Because of this and the difficulties in obtaining valid consent from employees, the implementation of biometric systems (eg, for access control or time registration) by organisations for use by their employees has become rather uncertain.

Whistle-Blowing

Member states were required to implement Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, which sets out the minimum standards for the enhanced protection of whistleblowers, particularly through protection against retaliation and claims for damages, before 17 December 2021. Like many other member states, Belgium did not manage to complete the implementation into national law before this deadline, but a preliminary draft act is currently circulating and is expected to be submitted to Parliament and voted on by the end of June 2022. It should be noted that a whistle-blowing system already exists at the level of the Flemish public administration. It is likely that such system will need to be brought in line with the Directive and the upcoming law implementing the Directive in Belgium.

IAB Europe's Transparency and Consent Framework (TCF)

On 2 February 2022, the Belgian Data Protection Authority found that the Transparency and Consent Framework (TCF) developed by IAB Europe fails to comply with a number of provisions of the GDPR. The TCF is a widespread mechanism that facilitates the management of users' preferences for online personalised advertising, and that plays a pivotal role in the so-called Real Time Bidding (RTB) system for online advertising space. Contrary to IAB Europe's claims,

the Litigation Chamber of the Data Protection Authority found that IAB Europe is acting as a data controller with respect to the registration of individual users' consent signal, objections and preferences by means of a unique Transparency and Consent (TC) String, which is linked to an identifiable user. This means that IAB Europe can be held responsible for possible violations of the GDPR. The Belgian Data Protection Authority imposed a EUR250,000 fine on the company, and gave it two months to present an action plan to bring its activities into compliance.

Proceedings against Facebook

On 15 June 2021, the Court of Justice of the European Union (CJEU) ruled in the case between Facebook and the Belgian Data Protection Authority, which has been ongoing since 2015.

In 2015, the Privacy Commission (which became the Belgian Data Protection Authority on 25 May 2018) went to court against Facebook for what it considered to be a serious invasion of the privacy of Belgian citizens: collecting information on the surfing behaviour of millions of internet users in Belgium by placing cookies on their computers and then collecting these cookies via social plug-ins and pixels on the websites that they visit.

Before ruling on the merits of the case, the Court of Appeal of Brussels, which was examining the case, decided to refer certain questions to the CJEU in order to verify whether the Belgian Data Protection Authority has the competency to pursue its legal action against Facebook given the entry into force of the GDPR and the introduction of a new co-operation mechanism between European data protection supervisory authorities called the "one-stop shop", which provides that the authority of the country where the main establishment of the respondent company is located (the Irish Data Protection Commission in the case of Facebook) is competent to take sanctions.

According to the CJEU, under certain conditions (provided for in the GDPR), a national supervisory authority may indeed exercise its power to bring an alleged infringement of the GDPR to the attention of the judicial authorities of a member state, even if this supervisory authority is not the lead authority for that processing. The CJEU also gives a broad interpretation of the powers of the (national) authority that is not the lead authority, as advocated by the Belgian Data Protection Authority. The Belgian Data Protection Authority will now analyse the judgment to better understand its impact on its ongoing case before the Brussels Court of Appeal.

EU Cloud Code of Conduct (CoC)

On 20 May 2021, the Belgian Data Protection Authority approved the first transnational code of conduct to be adopted within the European Union since the entry into force of the GDPR. The EU Cloud CoC aims to establish good data protection practices for cloud service providers and will contribute to a better protection of personal data processed in the cloud in Europe.

The EU Cloud CoC further specifies the requirements of Article 28 of the GDPR (concerning the processor) – and other relevant related Articles of the GDPR – for practical implementation within the cloud market (including IaaS, PaaS and SaaS). Adherence to the EU Cloud CoC is also achievable for SMEs that are active in this sector. Through the approval of this code, the Belgian Data Protection Authority has contributed to a harmonised interpretation of GDPR provisions in the cloud sector across the EU.

Case Law of the Data Protection Authority

Following the 2020–2025 Strategic Plan, the Litigation Chamber has focused on the following

aspects of the GDPR and has rendered numerous decisions in this regard:

- the role of the Data Protection Officer (DPO), with a particular focus on "pro forma" (external) DPOs, the independence of the DPO (ie, no conflicts of interest) and companies that have appointed a DPO without allowing the DPO 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
- the exercise of data subjects' rights, and, specifically, the scope of some of these rights.

Each year, the Data Protection Authority publishes a management plan in which it converts the strategic goals of the 2020–2025 Strategic Plan into concrete objectives for the coming year. The management plan for 2022 is yet to be published.

Independence of the Data Protection Authority

2021 was a difficult year for the Belgian Data Protection Authority. The European Commission questioned the independence of the Belgian Data Protection Authority and found that some of its members could not be considered to be free of outside influence because they either report to a management committee dependent on the Belgian government, participated in government projects to detect COVID-19 contacts, or are members of the Information Security Committee for the federal public sector. As a consequence, the Data Protection Authority did not remain free of political and internal conflicts in 2021, leading to one of the Data Protection Authority's directors voluntarily stepping down. A proposed law currently pending could potentially resolve this in 2022.

COVID-19

In the past two years, the Supervisory Authorities have focused in part on the COVID-19 health crisis. The EU Commission, the European Data Protection Board (EDPB) and some national supervisory authorities, including the Belgian Data Protection Authority, have published the following:

- guidance on the legal framework of tracing apps as one of the tools of a broader set of measures for fighting the virus; and
- a number of opinions regarding draft laws or royal decrees imposing, for example, recourse to the Covid Safe Ticket (CST) or face masks in public places.

General obligations of controllers under the GDPR, such as transparency and integrity, will have to be complied with, and public health authorities and employers must always have legal grounds for the processing of personal data.

Moreover, the Belgian Data Protection Authority published an analysis of the processing of vaccination data. As vaccination is voluntary in Belgium, requesting and registering a person's vaccination status is in principle prohibited, unless the controller can rely on an exception laid down in Article 9 (2) of the GDPR, such as the explicit consent of the person concerned or a legal obligation.

In an employment context, the processing of personal data may be necessary for compliance with a legal obligation to which the employer is subject, such as obligations relating to health and safety in the workplace, or relating to the public interest, such as the control of diseases and other threats to health. The employer may ask employees to undergo a medical examination (eg, temperature check), but not on a general or systematic basis and only when required

by health and safety (eg, for employees returning from risk areas). More recently, the Litigation Chamber has decided to temporarily suspend the verbal verification by a hospital network of the vaccination status of candidates for recruitment, as there was no legal basis for such processing.

International Data Transfers

The impact of the CJEU on the data protection landscape in past years cannot be underestimated, as many controllers struggle with the effects of the Schrems II decision, which invalidated the Privacy Shield and questioned the validity of standard contractual clauses (and other adequate safeguard mechanisms) for transfers of personal data to the US and other third countries.

Organisations are required to re-evaluate their data transfers to third countries if they are based on SCCs (and other adequate safeguard mechanisms) and to perform a "Transfer Impact Assessment" (TIA). Whether the SCCs (and other adequate safeguard mechanisms) are a sufficient safeguards for transfers to certain third countries will require further examination. For instance, in the US, it is hard to see how the concerns raised by the CJEU regarding the Privacy Shield would not apply when the SCCs are at issue and similar organisations are concerned.

EU Regulatory Developments

"A Europe fit for the digital age" is one of the six priorities of the European Commission for 2019–2024. As digital technology is increasingly impacting people's lives, the EU's digital strategy aims to make this transformation work for people and businesses, while helping to achieve the EU's target of a climate-neutral Europe by 2050.

Various initiatives have already been taken within the framework of the European Commission's digital strategy, including a series of new – and often bold – legislative proposals, which will have a material impact on businesses and organisations inside (and often also outside) the EU:

- the Digital Services Act (DSA);
- the Digital Markets Act (DMA);
- the Data Governance Act;
- the Data Act;
- the Artificial Intelligence Regulation;
- the Omnibus Directive (already adopted but not yet implemented in Belgian law); and
- the Digital Operational Resilience Act (DORA).

At the same time, existing legal frameworks are being re-assessed and updated, such as the review of the Network and Information Systems (NIS) Directive and the e-Privacy Regulation.

Lydian has an information governance and data protection (privacy) team of eight specialised lawyers, who represent large and small clients 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 and litigation department, and heads the information and communications technology (ICT) practice and the information governance and 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 also holds a CIPP/E certification. He is a regular speaker at conferences on privacy and data protection, and regularly publishes in international legal reviews such as Computerrecht, Privacy & Informatie, DataGuidance, Tijdschrift voor Privacy en Persoonsgegevens and Bulletin des Assurances.

Olivia Santantonio is a counsel in the information governance and data protection (privacy) and intellectual property practices at Lydian. She frequently advises on data protection issues regarding the obligations and liabilities of data controllers and data processors, international data transfers and the processing of sensitive data. She also frequently assists clients in assessing their level of compliance with the legislation, and in responding to data subject requests, data breaches or Data Protection Authority requests. She also offers (daily) support to DPOs. 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).

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

Liese Kuyken is an associate in Lydian's information and communications technology (ICT), information governance and data protection (privacy) and intellectual property practices. She frequently assists clients in data protection matters regarding data processing agreements, privacy and cookie policies, and data subject rights. She also specialises in global privacy issues (GDPR compliance, contract review, binding corporate rules, etc). Liese is involved in several proceedings regarding the processing of personal data, before the Belgian Data Protection Authority as well as Belgian courts. She teaches Media Law in the journalism programme at KU Leuven, where she educates students on issues such as privacy and image rights. Furthermore, Liese is a member of the International Association of Privacy Professionals (IAPP) and has 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