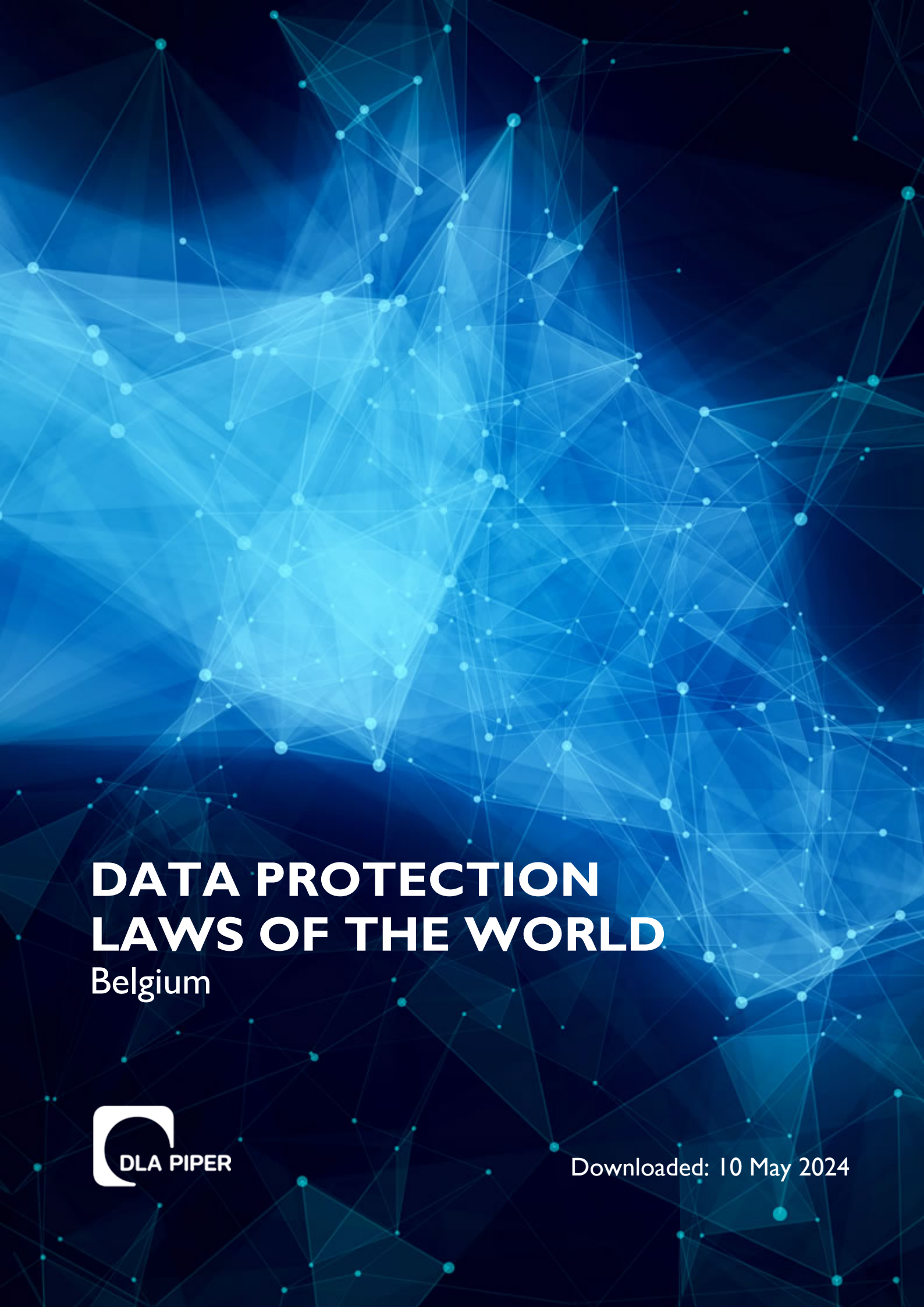

DATA PROTECTION LAWS OF THE WORLD

Belgium

DLA PIPER

BELGIUM

Last modified 6 February 2024

LAW

The GDPR has been integrated in Belgium through a few laws. The 'Data Protection Act' of July 30, 2018 provides for the implementation of some of the GDPR provisions open to further definition, derogation or additional requirements. It also includes the transposition of the 2016/680 Directive regarding the processing of personal data in the criminal justice chain and the establishment of a Control body on police information (called 'COC'). Additionally, it regulates the authorities outside the scope of the EU law (including intelligence and security services).[1]

The Belgian Data Protection Authority, the successor of the Belgian Privacy Commission, was established by the Belgian Federal Chamber of Representatives by the Act of December 3, 2017 ("**DPA Act**")[2]. Several other laws have also been adapted to align them with the GDPR (e.g. Video Surveillance Act).

The competent Secretary of State has announced legislative proposals for a reform of Belgian data protection law (i.e. both the Data Protection Act and DPA Act). The reform proposal of the Data Protection Act has been introduced before the Federal parliament and currently sits at the level of inter-cabinet operations. If approved, it will go to the Council of Ministers and subsequently to the COC and Council of State for advice. Delays are possible as stakeholders might view it as an ideal opportunity to address specific longstanding issues. The exact timing of adoption is thus currently unclear. The reform proposal of the DPA Act has been approved by the Chamber of Representatives on 14 December 2023. The reform of the DPA Act intends to strengthen the functioning, the independence and the pragmatic approach and sectoral expertise of the Belgian Data Protection Authority.

In addition to the above-mentioned reform of the DPA Act, there has been another legislative proposal to amend this Act due to a judgment of the Belgian Constitutional Court. The Court found Article 108 of the DPA Act to be unconstitutional insofar it does not allow interested third parties to appeal a decision of the Litigation Chamber. To accommodate the Court’s findings the proposal provides in the opportunity for third parties to appeal decisions of the Litigation Chamber before the Market Court and to intervene in the proceedings before the Litigation Chamber.

---

1. See Data Protection Act.
2. See DPA Act.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Data Protection Act builds on the definitions contained in the GDPR and further clarifies some notions, such as the notion of 'public authority'[1]. It further adds the definitions of a ‘**trusted third party**’, ‘**disclosure of personal data’** and ‘**distribution of personal data**’ in the context of the research and statistical purposes exception. The Data Protection Act also clarifies certain concepts such as 'processing in the substantial public interest'[2], the 'processing for journalistic purposes'[3] and introduces new concepts such as 'a joint database'[4].

1. Art. 5 Data Protection Act.
2. Article 8 para. 1 Data Protection Act.
3. Art. 24 para. 1 Data Protection Act.
4. Article 48 Data Protection Act.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The DPA Act establishes the Data Protection Authority as the successor of the Privacy Commission which was established under the old data protection legislation. The Data Protection Authority has the competences as set out in the GDPR whenever that competence has not been explicitly assigned to another body.

The Data Protection Act appoints three more regulatory authorities at the federal level (COC[1], Committee I[2] and Committee P[3]) with varying data protection related competences next to the general Data Protection Authority. In addition, there are also regional supervisory authorities who have been entrusted mainly with the supervision of the public authorities of the regions.

The composition of the Data Protection Authority has proven controversial due to the involvement of some members in government bodies. The European Commission warned Belgium mid 2021 that it would start an infringement procedure before the EU Court of Justice if the problems regarding the Data Protection Authority’s independence would not be resolved. Therefore, a legislative proposal has been introduced before the Federal Parliament at the end of 2021 to amend the DPA Act by partially reforming the rules on the composition of the Data Protection Authority[4]. Additionally, a revocation procedure was initiated by the Belgian federal parliament in March 2022 following an audit of the Belgian Court of Auditors. The Belgian Chamber of Representatives voted to revoke the mandate of two directors of the Data Protection Authority under the so-called Article 45 procedure of the DPA Act. As the Chamber’s decision is not public, the exact allegations and reasons for revocation of the mandates are unknown. In 2023, the two mandates have been reinstated. Two new directors have been appointed at the Data Protection Authority. Hopefully, this will bring about more stability as it is clear that these events were testing / challenging the well-functioning of the Data Protection Authority.

1. Art. 231 Data Protection Act.
2. Art. 72 para. 2 °7 Data Protection Act.
3. Art. 26 °7, c) Data Protection Act.
4. Legislative proposal 26 November 2021, amending the Act of 3 December 2017 establishing the of the Data Protection Authority, in order to modify the composition of the centre of expertise so that the independence of its members its members can be guaranteed (Doc. No. 55-2347/001), www.lachambre.be/flwb/pdf/55/2347/55K2347001.pdf

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The registration of processing activities through a notification has been abolished. However, in the public sector, the Data Protection Act obliges the controller of processing activities in the context of police services to publish a protocol detailing the transfer to a public authority or private body based on public interest and compliance with legal obligations[1].

1. Art. 20 Data Protection Act.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In addition to the GDPR, the Data Protection Act requires the appointment of a DPO depending on the impact of the processing activity, namely if it may entail a high risk as referred to in article 35 of the GDPR when (i) a private law body processes personal data on behalf of a federal public authority or a federal public authority transfers personal data to this private law body in the context of police services[1] or (ii) the processing falls under the exception necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[2]. Some public authorities regulated by the Data Protection Act are also required to appoint a DPO[3].

The Data Protection Authority has addressed the GDPR requirements for the appointment of DPOs and the exercise of its tasks in several cases, including in relation to the position of the DPO and its independence, the obligation to directly report to the highest management level, the necessary resources to carry out his tasks and the requirement that a DPO must have “expert knowledge”.

1. Art. 21 Data Protection Act.
2. Art. 190 Data Protection Act.

3. The Center for Missing and Sexually Exploited Children (Child Focus) Art. 8 para. 3 Data Protection Act; Competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security implementing Directive 2016 /680 Art. 63 et seq Data Protection Act; Intelligence and security services Art. 91 Data Protection Act; Bodies for security clearances, certificates and recommendations Art. 124 Data Protection Act; Coordination Unit for Threat Assessment Art. 157 Data Protection Act.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or

have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Data Protection Act adds only specificities to the general processing requirements. The age for consent of children for the purposes of article 8.1 GDPR is 13 year[1]. When processing genetic, biometric and health data, a controller needs to indicate who has access to these personal data, keep a list of the categories of people who have access to these data, keep this list at the disposal of the DPA, and ensure that these people are bound by a legal, statutory or contractual obligation of confidentiality[2]. The Data Protection Authority has adopted specific guidelines regarding the processing of biometric data[3].

The Data Protection Act also provides a list of legal bases for processing data relating to criminal convictions and offences and requires an access management list and confidentiality duties (as described here above) for processing such data[4].

Data subject rights

The Data Protection Act provides further exceptions to data subject’s rights, including the right to be informed when personal data is received from authorities under special regimes[5] or when personal data is disclosed to these bodies [6]. With respect to the special regimes addressed in the Data Protection Act, the Data Protection Act also sets out the corresponding data subject rights (which are often more limited than those included in the GDPR)[7].

The Data Protection Act clarifies that data subject rights, including the right to information in judicial proceedings /decisions, will be accommodated in accordance with the Judicial Code, the Code on Criminal proceedings and any specific laws related to criminal law procedure[8].

1. Art. 7 Data Protection Act.
2. Art. 9 Data Protection Act.
3. Data Protection Authority, Recommendation on the processing of biometric data (No. 1-2021, 1 December 2021).
4. Art. 10 Data Protection Act.
5. Art. 11, Art. 13 and Art. 14 Data Protection Act.

6. Art. 12 Data Protection Act.
7. Art. 36 et seq, Art. 79, Art. 105 (9), Art. 113, Art. 145, Art. 173 Data Protection Act.
8. Art.16 Data Protection Act.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

No general additional requirements relating to transfers are introduced by the Data Protection Act. The Data Protection Act only regulates the transfer of personal data under the special regimes, which in certain cases provides for less leeway for transfers[1].

For more information, please visit our Transfer - global data transfer methodology website.

1. Art. 66-70, Art. 93-94, Art. 126-127, Art. 159-160 Data Protection Act.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Data Protection Act inserts no general additional requirements in relation to security measures. In the context of archiving, scientific or historical research purposes or statistical purposes, the Data Protection Act sets out specific rules including anonymization or pseudonymization requirements[1].

Security measures are also detailed for each special regime but resemble the GDPR[2].

---

1. Art. 198 et seq Data Protection Act.
2. Intelligence and security services Art. 88-89 Data Protection Act, Bodies for security clearances, certificates and recommendations Art. 121-122 Data Protection Act, Coordination Unit for Threat Assessment Art. 154-155 Data Protection Act, Passenger Information Unit Art. 179-180 Data Protection Act.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

No general additional requirements are inserted in the Data Protection Act relating to data breaches.

Data breach obligations are also detailed for each special regime, but they resemble those contained in the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In addition to the GDPR, the Data Protection Act introduces a specific procedure for actions for injunctions that can be initiated by the data subject or by the Data Protection Authority (DPA)[1]. These claims should be brought before the President of the Court of First Instance except when the personal data is processed in criminal investigations or procedures[2]. There is no single court territorially competent to hear these claims[3].

The Data Protection Act also contains a legal basis that allows a body, organisation or non-profit organisation to represent the data subject upon its request when it:

- was founded in accordance with Belgian law
- has legal personality
- has statutory objectives of public interest
- has been active in the area of the protection of personal data for at least 3 years[4]

The DPA can impose administrative fines under article 83 of the GDPR[5], but public authorities, their agents and authorised representatives are exempted insofar they are not offering goods or services on the market[6]. A supervisory authority can exercise the corrective measures set out in article 58.2 GDPR but with regard public authorities, only over the categories enumerated in the Data Protection Act[7].

Depending on the infringement and the infringer, the controller, processor, competent public authority or their agent can be subjected to criminal sanctions, such as criminal fines between 800 EUR – 160.000 EUR and a publication of the judgement[8].

The DPA consists of 6 different Committees. The **Inspection Committee** of the DPA enjoys investigation powers, such as to identify persons, interview persons, conduct written interrogations, conduct on-site investigations, consult information systems and copy the data they contain, consult information electronically, seize or seal goods or computer systems and demand the identification of the subscriber or the normal user of an electronic communication service or of the electronic means of communication used[9]. Additionally, the inspector-general and the inspectors of the inspection committee may order the temporary suspension, restriction or freezing of the data processing activities that are the subject of an investigation if this is necessary to avoid a serious, immediate and difficult to repair disadvantage.[10] They can also request further information[11].

The **Litigation Chamber** can *inter alia* follow-up on a complaint but also propose a settlement, formulate warnings and reprimands, order compliance with data subjects’ requests to exercise their rights, order the suspension of cross-border data flows and can also impose periodic penalty payments and/or administrative fines[12].

Specific provisions according to Art. 85 to 87 and Art. 89 GDPR

The legislator has made use of the opportunity offered by the GDPR to provide exemptions or derogations from certain obligations when the processing is carried out for journalistic purposes and the purposes of academic, artistic or literary expression. For those purposes, the Data Protection Act exempts the controller not only from respecting certain data subjects’ rights under the GDPR but also some obligations of the controller (e.g. notification in case of breaches, transfer requirements, etc) and the investigative powers of the DPA[13].

The Data Protection Act also introduces two regimes for the derogations relating to the processing for archiving, scientific or historical research purposes or statistical purposes:

- general safeguards requiring among others register, information[14], contractual[15] and security requirements, or
- compliance with a code of conduct[16]

The Data Protection Act does not include other derogations relating to employment.

---

1. Art. 211 par. 3 Data Protection Act.
2. Art. 209 Data Protection Act.
3. Art. 209 par. 2 Data Protection Act.
4. Art. 220 par. 2 Data Protection Act.
5. Art. 101 DPA Act
6. Art. 221 par. 2 Data Protection Act.
7. Art. 221 par. 1 Data Protection Act.
8. Art. 222 et seq Data Protection Act.
9. Art. 66 DPA Act.
10. Art. 70 DPA Act.
11. Art. 76 DPA Act.
12. Art. 95 DPA.
13. Art. 24 Data Protection Act.
14. Art. 193 Data Protection Act.
15. Art. 194 Data Protection Act.
16. Art. 187 Data Protection Act.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Data Protection Act applies to most electronic marketing activities, as there is likely to be processing of personal data involved (e.g. an email address is likely to be ‘personal data’ for the purposes of the Data Protection Act). The Data Protection Act does not contain additional rules to the GDPR for the use of personal data for the purposes of electronic marketing.

However, specific rules are set out in the Belgian e-commerce legislation (Book XII of the Code of Economic Law) regarding opt-in requirements:

- These rules apply to all ‘electronic messages’, such as emails and text messages (Short Message Systems or SMS). Other types of electronic communication such as instant messaging and chat may also fall within the scope of these rules depending on the specific context. This covers not only clear promotional messages, but also newsletters and similar communications. Indeed, any form of communication intended to directly or indirectly promote goods, services, the image of a company, organisation or person which/who exercises a commercial, industrial or workmanship activity or regulated profession falls within the scope of these rules.

- As a general principle, the prior, free, specific and informed consent of the recipient of the message must be obtained (‘opt-in principle’).

- Two exceptions apply to the opt-in principle. No prior, free, specific and informed consent is to be obtained if:

    - the electronic marketing message is sent to existing customers of the service provider, or

    - the electronic message is sent to legal persons (e.g. to a general email address such as info@company.com).

  These exceptions are subject to compliance with strict conditions.

- Furthermore, all electronic messages must contain a clear reference to the recipient's right to opt out, including means to exercise this right electronically.

Neither the Data protection Act nor the DPA Act include specific provisions on electronic marketing.

The Data Protection Authority has adopted specific guidelines regarding direct marketing[1].

1. Data Protection Authority, Recommendation on the processing of personal data for direct marketing purposes (No. 1-2020, 17 January 2020).

ONLINE PRIVACY

Cookies

Article 5 (3) of the E-Privacy Directive was initially implemented into Belgian Law by means of an amendment to article 129 of the Belgian Electronic Communication Act. By the Act of 21 December 2021 transposing the European Electronic Communications Code and amending various provisions on electronic communications, article 129 was abolished and a similar provision was inserted in the Belgian Data Protection Act by means of a new article 10/2. This amendment explicitly confirms the competence of the Belgian Data Protection Authority regarding cookies.

The use and storage of cookies and similar technologies requires:

- the provision of clear and comprehensive information; and
- consent of the website user.

Consent is not required for cookies that are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
- strictly necessary for the provision of a service requested by the user.

The DPA has provided useful additional guidance related to topics such as cookie walls, social media plugins and the validity of consent through browser settings. Recently it published a so called ‘Cookie Checklist’ as a guidance tool for

companies to ensure the compliant use of cookies. Furthermore the DPA has taken several enforcement decisions with regard to cookies.[1]

Download DLA Piper's Guide on Cookies.

Location data

As location data are personal data, the processing of these data must comply with the general rules stipulated by the GDPR and the Data Protection Act (including, depending on the context, article 10/2). Neither the Data Protection Act nor the DPA Act include any other specific provisions on location data.

In addition, article 123 of the Belgian Electronic Communication Act stipulates that mobile network operators may process location data of a subscriber or an end user only to the extent that the location data has been anonymised, or if the processing is carried out in the framework of the provision of a service regarding traffic or location data.

The processing of location data in the framework of a service regarding traffic or location data is subject to strict conditions set forth in article 123.

Traffic data

As traffic data constitute personal data, the processing of traffic data must comply with the general rules stipulated by the GDPR and the Data Protection Act (including, depending on the context, article 10/2) . Neither the Data Protection Act nor the DPA Act include any other specific provisions on traffic data.

However, in accordance with article 122 of the Belgian Electronic Communication Act, mobile network operators are required to delete or anonymise traffic data of their users and subscribers as soon as such data is no longer necessary for the transmission of the communication (subject to compliance with cooperation obligations with certain authorities).

Subject to compliance with specific information obligations and subject to specific restrictions, operators may process certain traffic data for the purposes of:

- invoicing and interconnection payments;
- marketing of the operator’s own electronic communication services or services with traffic or location data (subject to the subscriber’s or end user’s prior consent); and
- fraud detection.

1: I.a. Decision on the merits, 21 January 2022, nr. 11/2022; Decision on the merits, 24 May 2022, nr. 84/2022; Decision on the merits, 25 May 2022, nr. 85/2022; Decision on the merits, 16 June 2022, nr. 103/2022.

KEY CONTACTS

Kristof De Vulder
Partner
T +32 (0) 2 500 15 20
kristof.devulder@dlapiper.com

Heidi Waem
Counsel
T +32 2500 1614
heidi.waem@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.