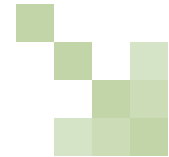


# Belgium

Steven De Schrijver and Jan Dhont, Lorenz



[www.practicallaw.com/1-385-8611](http://www.practicallaw.com/1-385-8611)

## REGULATION

### 1. What national law(s) apply to the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

The Data Protection Directive has been implemented by the Belgian Data Protection Act (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/ Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*) of 8 December 1992 (as amended by the Law of 11 December 1998) (DPA) and the Royal Decree of 13 February 2001.

The authority that oversees and enforces the DPA is the Data Protection Commission (*Commissie voor de Bescherming van de Persoonlijke Levenssfeer/Commission de la protection de la vie privée*) (CBPL) (see box, *The regulatory authority*).

### 2. To whom do the rules apply (EU: data controller)?

The DPA applies to data controllers, that is, any natural or legal person, administrative body or other entity which determines the purpose of, and means for, processing personal data (*Article 1 §1, DPA*). Certain rules of the DPA (*Article 16, DPA*) also apply to a data processor, that is, any natural or legal person, factual association or public authority that processes personal data on behalf of the controller, except for the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

### 3. What data is regulated (EU: personal data)?

The DPA regulates personal data, that is, any information relating to an identified or identifiable natural person. A person is identifiable if he can be directly or indirectly identified, in particular, by reference to an identification number or to one or more elements specific to his physical, physiological, psychical, cultural or social identity (*Article 1 §1, DPA*). The person to whom personal data relate is defined as the “data subject”.

### 4. What acts are regulated (EU: processing)?

The DPA applies to the fully or partly automatic processing of personal data, that is, by means of a computer system, and the

non-automatic processing of personal data entered or intended to be entered into a file (*Article 3 §1, DPA*). A file is defined as any structured set of personal data that is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Processing includes the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination (by means of transmission, distribution or making available in any form), merging, linking, blocking, erasure or destruction (*Article 1 §2, DPA*).

### 5. What is the jurisdictional scope of the rules?

The DPA applies to data controllers in respect of any processing of personal data if either:

- The data controller has a permanent establishment in Belgium and the personal data are processed in the context of that establishment (*Article 3 bis 1°, DPA*).
- The data controller is established neither in Belgium nor in any other EU member state, but uses equipment in Belgium for processing the data otherwise than just in transit. Where a data controller falls under this heading, it must nominate a representative in Belgium for the purposes of the DPA (*Article 3 bis 2°, DPA*).

### 6. What are the main exemptions (if any)?

The DPA does not apply to non-automatic data processing, if the personal data being processed is not contained in a file or is not intended to be indexed.

In addition, the DPA does not apply to data processing for personal or household use (*Article 3 §2, DPA*). The following categories are partly exempted from the DPA (*Article 3 §3, DPA*):

- Processing by or on behalf of intelligence or security services or for the purposes of implementing police tasks.
- Processing for the purposes of implementing money laundering legislation.
- Processing exclusively for journalistic, artistic or literary purposes (under certain conditions for some of the provisions of the DPA).

---

## 7. Is notification or registration required before processing data? If so, please provide brief details.

---

The DPA requires every data controller who is processing personal data by automatic means to notify the CBPL before the data processing begins, unless the data processing falls under one of the following exemptions (*Royal Decree of 13 February 2001*):

- Personal data necessary for the payroll management of the employer.
- Personal data used by the employer exclusively for staff management.
- Personal data necessary for the accountancy of the data controller.
- Personal data necessary for the administration of shareholders and partners.
- Personal data necessary for the administration of customers and suppliers.
- Personal data indispensable for contacting the data subject.
- Personal data relating to access control in company buildings and premises.

The notification should be made by means of paper forms which can be downloaded from the CBPL's website ([www.privacycommission.be](http://www.privacycommission.be)) or electronically via the internet. Each purpose for which personal data are processed or each group of connected purposes requires a separate notification, that is, by using a separate form. The notification form should be completed either in French or in Dutch and contain in particular the following information:

- Name and address or name and registered office of the data controller.
- Purpose(s) of the automatic processing.
- Categories of the personal data processed.
- Categories of the recipients of the data.
- Manner in which the data subjects are informed of their rights.
- Retention period of the personal data.
- General description of the security measures taken.
- Categories of personal data that are transferred to other countries and the country of destination.

Further, within the scope of its power of supervision and investigation, the CBPL is entitled to demand additional information from the data controller. In particular, the CBPL can demand information on the origin of the personal data, a copy of the data transfer agreement (if any), the automation technology selected and the applicable security measures.

Paper notification forms must be sent to the CBPL either by mail or submitted in person at the CBPL.

The fee for an online notification amounts to EUR25 (about US\$32) (EUR125 (about US\$158) in the case of a paper notification). The fee for modifying an existing notification amounts to EUR20 (about US\$25).

The data controller can start the processing when the CBPL acknowledges receipt of the notification. The acknowledgment of receipt is usually sent within three days.

---

## 8. What are the main obligations imposed on data controllers to ensure that data is processed properly?

---

Data controllers are under the following obligations to ensure fair and lawful processing of personal data (*DPA*):

- The processing of personal data should be legitimate (*Article 5, DPA*) and comply entirely with the principles relating to data quality. That is, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. Personal data must be relevant, not excessive, accurate, up to date, and kept no longer than necessary (*Article 4, DPA*).
- Data controllers must provide certain information to the data subjects concerned and grant the data subjects concerned the rights to access, object, rectify, block and/or delete personal data (*Articles 9 to 12, DPA*).
- Data controllers must adopt appropriate technical and organisational security measures to protect personal data against accidental or unauthorised destruction, accidental loss, alteration, access and any other unauthorised processing (*Article 16 §4, DPA*).
- If a data processor processes personal data on behalf of the data controller, such a party must be carefully selected, supervised and its compliance with the security requirements checked. In addition, a written contract with the data processor must be concluded (*Article 16 §1, DPA*).

---

## 9. Is the consent of data subjects required before processing personal data? If so:

- **What rules are there regarding the form and content of consent? Would online consent suffice?**
  - **Are there any special rules regarding the giving of consent by minors?**
- 

Personal data can be processed without prior consent of the data subject if the data processing can be based on one of the other legitimate grounds for data processing (*see Question 10*).

## Form and content of consent

"Consent" means any freely given specific and informed indication that the data subject or his legal representative gives to signify his agreement that the personal data may be processed (*Article 1 §8, DPA*). Online consent that complies with this definition will suffice. However, for the processing of sensitive data, if such processing cannot be based on other legitimate grounds (see *Question 11*), written consent is required (*Article 6 §2 (a), DPA*). In any event, the data controller should be able to prove that consent has been given.

## Consent by minors

The consent of a minor can be given by his legal representative (*Article 1 §8, DPA*), who can withdraw it at any time on behalf of the minor.

## 10. If there is no consent, on what other grounds (if any) can processing be justified?

If no consent has been given, the processing can be justified if it is necessary:

- For the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract.
- To comply with a legal obligation.
- To protect a vital interest of the data subject.
- For the proper performance of a task carried out in the public interest or for the exercise of official authority vested in the data controller or in a third party to whom the personal data are disclosed.
- To uphold the legitimate interests of the data controller or a third party to whom the data are supplied, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

## 11. Do special rules apply in the case of certain types of personal data, for example sensitive data? If so, please provide brief details.

Special categories of personal data include:

- Sensitive data (for example, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as data concerning sex life).
- Health-related personal data.
- Personal data relating to litigation that has been submitted to courts and tribunals as well as to administrative judicial bodies, relating to suspicions, persecutions or convictions in matters of criminal offences, administrative sanctions or security measures (legal personal data).

Under the DPA, the processing of special categories of personal data is, in principle, prohibited. However, the processing can take place if specific requirements for each of the above categories of personal data are met. For example, sensitive and health-related data can be processed in the following circumstances:

- The data subject has given his written consent to the processing (provided that this consent can be withdrawn by the data subject at any time).
- The processing is necessary to comply with labour law or social security law obligations.
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.
- The data have been manifestly made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of a right in law.
- The processing is done for the purpose of scientific research (provided that certain conditions are satisfied).
- The processing is necessary for some medical purposes, such as preventative medicine.
- The processing is necessary with a view to an important public interest.

In addition, sensitive data can be processed:

- By a non-profit-making organisation in the course of its legitimate activities.
- For statistical purposes under the Law of 4 July 1962.
- By an organisation promoting the defence of human rights (provided that certain conditions are satisfied).

Health-related data can also be processed if the processing is necessary for the prevention of a specific danger or the punishment of a particular criminal offence, or for the promotion and protection of public health.

Legal data can only be processed in the following exceptional cases:

- Under the supervision of a public authority.
- By other persons if the processing of the data is necessary for purposes set out by law.
- By legal or natural persons for the management of their disputes.
- By lawyers exclusively for the defence of their clients' rights.
- For the purpose of scientific research (provided that certain conditions are satisfied).

**RIGHTS OF INDIVIDUALS****12. What information should be provided to data subjects at the point of collection of the personal data?**

The data controller must provide the following information to the data subject at the time he obtains the personal data directly from the data subject, unless the data subject is already aware of this information (*Article 9, DPA*):

- The name and address of the data controller and, if applicable, of his representative.
- The purpose(s) of the data processing.
- Other additional information (unless it is unnecessary to guarantee fair processing, taking into account the specific circumstances in which the data are obtained), in particular:
  - the recipients or categories of recipients of the data;
  - whether replies to the questions are obligatory as well as possible consequences of a failure to reply;
  - the existence of the right of access to and the right to rectify the personal data concerning him.
- Any other information, dependent on the specific nature of the processing, that will be specified by Royal Decree after advice from the CBPL.

If the personal data are not obtained from the data subject himself, the above information must be provided either at the time when the data relating to the data subject are recorded, or when the data are intended to disclose the data to a third party, but at the latest on the first occasion that these data are disclosed.

However, this obligation does not apply if, particularly for statistical, historical or scientific research purposes, it is impossible or requires disproportionate effort to provide the requested information to the data subject. In such cases, the data controller must provide this information when he contacts the data subject for the first time.

**13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?****Right of access**

A data subject is entitled, on request but free of charge, to be informed by any data controller, normally within 45 days, whether his personal data are being processed (*Article 10 of the DPA*). If they are being processed, he is entitled to receive a description of the:

- Personal data of which that individual is the data subject.
- Purpose(s) of processing.

- Data categories to which the processing relates.
- Recipients or classes of recipients to whom the data are or may be disclosed.
- Available information about the origin of the data.

**Right to be informed about automated decision-making**

A decision resulting in legal effects for a data subject or affecting him seriously cannot be taken purely on the basis of automatic data processing aimed at the evaluation of certain aspects of his personality (*Article 10 §1 (c), DPA*).

However, this prohibition does not apply if the decision is taken in the context of an agreement or if it has its ground in a provision laid down by, or by virtue of, a law, decree or ordinance. Appropriate measures for the protection of the legitimate interests of the data subject must be included in such agreement or provision and the data subject must at least be allowed to express his point of view in an effective manner.

If automated decision-making is applied, the data subject should be informed about the logic involved in the automatic processing of the personal data concerning him.

**Right to object**

Any data subject has the right to object against the processing of data relating to him for serious and legitimate reasons that relate to his particular situation, unless the lawfulness of the processing is based on (*Article 12, DPA*):

- The performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract.
- Compliance with an obligation to which the data controller is subject by, or by virtue of, a law, decree or ordinance.

In addition, the data subject should be allowed, free of charge, to oppose the use of his personal data for direct marketing purposes (*Article 12, DPA*).

If the data subject objects to the processing or the intended processing of personal data relating to him, the data controller must inform the data subject within one month what has been done about the request. If the objection is legitimate, the data controller can no longer process these personal data for the purpose concerned.

**Right to rectify, block and erase**

A data subject has the right to have inaccurate personal data rectified, free of charge, (*Article 12, DPA*), as well as to have personal data erased, also free of charge. The personal data will only be erased or corrected to the extent that the data are incomplete or not necessary in view of the purpose of the processing.

The data subject can also forbid the use of personal data:

- That are incomplete or irrelevant in view of the purpose of the processing.

- The recording, communication or storage of which are prohibited.
- That have been stored for longer than the authorised period of time.

The data controller has one month to rectify or erase the personal data on receipt of the data subject's request. Within this period, the data controller should also notify the rectification or the erasure to the recipients of the relevant personal data, if he still has knowledge of these recipients and if such notification does not appear to be impossible or require a disproportionate effort.

## SECURITY REQUIREMENTS

### 14. What security requirements are imposed in relation to personal data?

Data controllers need to ensure that appropriate technical and organisational security measures are taken that are necessary for the protection of personal data against accidental or unauthorised destruction, accidental loss, as well as against alteration, access and any other unauthorised processing (*Article 16 §4, DPA*).

These measures should ensure an appropriate level of security, taking into account the state of the art in this field and the cost of implementing such measures on the one hand, and the nature of the data to be protected and the potential risks on the other. To assist data controllers in determining the required levels of security, the Belgian CBPL has issued standard measures for the security of personal data processing (*Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens/Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*). These can be found at [www.privacycommission.be](http://www.privacycommission.be).

## PROCESSING BY THIRD PARTIES

### 15. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

If a data controller outsources the processing to a processor, a written contract should be concluded between them (*Article 16 §1, DPA*). Such a contract must contain provisions in relation to technical and organisational security measures and the data processor's responsibility towards the data controller. It must also stipulate that the data processor will only act on behalf of the data controller and that the data processor is bound by the same obligations as those imposed on the persons acting under the authority of the data processor. In addition, the data controller must carefully select the data processor and supervise its compliance with all security measures.

## INTERNATIONAL TRANSFER OF DATA

### 16. What rules govern the transfer of data outside your jurisdiction?

The DPA applies to all transfers of personal data, either within the European Economic Area (EEA) or outside the EEA. No additional

rules apply to transfers within the EEA as EEA countries provide an "adequate level of protection".

Special rules apply to data transfers outside the EEA to countries which have not been officially recognised as providing an adequate level of protection. These transfers are in principle prohibited (*Article 21, DPA*). However, such transfers are allowed in the following cases (*Article 22, DPA*):

- The data subject has given his unambiguous consent to the transfer.
- The transfer is necessary for the execution of a contract between the data subject and the data controller, or for actions to be carried out at the request of the data subject and which are necessary for the conclusion of a contract.
- The transfer is necessary for the conclusion or execution of a contract between a data controller and a third party in the interest of a data subject.
- The transfer is necessary for an important public interest, or for the establishment, exercise or defence in law of right.
- The transfer is necessary to protect a vital interest of the data subject.
- The transfer is carried out from a public register set up by law or from a register which can be consulted by anyone who can invoke a legitimate interest, provided that the legal requirements for consultation are met.

Despite the above provisions, the Belgian Minister of Justice can, following an opinion of the CBPL, individually authorise a specific transfer of personal data or a category of transfers to a non-EEA country which does not provide an adequate level of protection, if the data controller provides "sufficient guarantees", for example, by concluding an *ad hoc* data transfer agreement or adopting binding corporate rules. In practice, no prior CBPL authorisation is required to the extent that the EU model clauses are used in an unamended format.

### 17. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Data transfer agreements are in use. Data transfer agreements based on the European Commission's standard contractual clauses for transfers to third countries (*Commission Decision 2004/915/EC of 27 December 2004, OJ 2004, L385/74; Commission Decision 2002/16/EC of 27 December, OJ 2002, L6/52; Commission Decision 2001/497/EC of 15 June 2001, OJ 2001, L181/191*) are automatically considered to provide "sufficient guarantees" for the transfer of personal data to third countries. Therefore, if such a data transfer agreement has been concluded, prior authorisation is not required (*see Question 16*). A copy of this data transfer agreement must, however, be sent to the CBPL.

### 18. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

A data transfer agreement is sufficient to transfer personal data to a third country not providing an adequate level of protection if the European Commission's standard contractual clauses for transfers to third countries are used (see *Question 16*). The data subject must be informed of the recipients or the categories of recipients of the data (see *Question 12*). An explicit consent for the transfer to third countries is not required. However, the data transfer, as a form of data processing, must also be based on one of the grounds for making the data processing as such legitimate (see *Question 10*).

### 19. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.

The CBPL only has an advisory function in the authorisation process (for example, in the context of approving *ad hoc* data transfer agreements or binding corporate rules). The final decision is taken by the Minister of Justice by means of a Royal Decree. For details of the approval required for a data transfer agreement, see *Questions 16, 17 and 18*.

## ENFORCEMENT AND SANCTIONS

### 20. What are the enforcement powers of the national regulator?

The CBPL can mediate or provide an opinion in case of a dispute between a data subject and a data controller (*Article 31 §3, DPA*). It can also inform the public prosecutor of offences of which it is aware (*Article 32 §2, DPA*). For sanctions and remedies for non-compliance with the data protection laws, see *Question 21*.

### 21. What are the sanctions and remedies for non-compliance with the data protection laws? To what extent are the laws actively enforced?

The processing of personal data in violation of the DPA may constitute a criminal offence (*Articles 37 to 39, DPA*).

The following criminal offences are punishable by a fine of EUR550 (about US\$700) up to EUR110,000 (about US\$159,400):

- Failure to comply with a request for rectification, blocking or erasure of personal data (see *Question 13*).
- Failure to implement the requisite technical and organisational measures (see *Questions 8 and 15*).

The following criminal offences are punishable by a fine of EUR550 up to EUR550,000 (about US\$700,000):

- Failure to comply with the general data protection principles (see *Question 8*).
- Failure to comply with the rules on legitimate data processing (see *Questions 9 and 10*).

## THE REGULATORY AUTHORITY

Data Protection Commission (*Commissie voor de Bescherming van de Persoonlijke Levenssfeer/La Commission de la protection de la vie privée*) (CBPL)

Hoogstraat/ Rue Haute, 139  
1000 Brussels  
Belgium  
**T** +32 2 213 8540  
**F** +32 2 213 8565  
**E** [commission@privacycommission.be](mailto:commission@privacycommission.be)  
**W** [www.privacycommission.be](http://www.privacycommission.be)

**Main area of responsibility.** The CBPL supervises compliance with the DPA.

**Contact for queries.** +32 2 213 8599.

**Obtaining information.** General information on the standards and rules for the protection of personal data can be obtained by telephone or e-mail.

- Failure to comply with the rules on the processing of sensitive personal data (see *Question 11*).
- Failure to comply with rules regarding the information to be provided to the data subject (see *Question 13*).
- Failure to communicate the information requested by the data subject within 45 days of receipt of the request, or knowingly communicating inaccurate or incomplete data (see *Question 13*).
- Failure to notify a data processing operation (see *Question 7*).
- Providing incomplete or inaccurate information in the notification of a data processing operation to the CBPL (see *Question 7*).
- Failure to comply with a request for information of the CBPL (see *Question 7*).
- Transferring personal data to a country outside the EEA contrary to the applicable rules (see *Question 16*).

In addition, a court can order (*Article 41 § 1-2, DPA*):

- Confiscation of the carriers of personal data to which the offence relates.
- Erasure of the data.
- Prohibition of the management of any processing of personal data, directly or through an agent, for a period of up to two years.

Any repeated offences are punishable by imprisonment from three months up to two years, and a fine from EUR100 (about US\$127) up to EUR100,000 (about US\$126,700) or with one of these sanctions only (*Article 41 § 3, DPA*).

Finally, a person suffering any harm as a consequence of acts infringing the provisions of the DPA can initiate a civil action for damages (*Article 42, DPA*).

## CONTRIBUTOR DETAILS

**Steven De Schrijver****Lorenz****T** +32 2 239 2000**F** +32 2 239 2002**E** [s.deschrijver@lorenz-law.com](mailto:s.deschrijver@lorenz-law.com)**W** [www.lorenz-law.com](http://www.lorenz-law.com)

**Areas of practice/expertise.** Partner Steven De Schrijver is Head of the IT & New Media Department of Lorenz. His practice covers commercial IT law (data protection, e-commerce, software licensing, website development and hosting, technology transfer, digital signature and IT-outsourcing) and technology-related transactions. He regularly publishes and speaks in these fields and is involved in the Computer & Telecommunications Law Commission of the UIA, the IP/IT Commission of AIJA, ITech-Law, and is the Belgian member of EuroITCounsel.

**Jan Dhont****Lorenz****T** +32 2 239 2000**F** +32 2 239 2002**E** [j.dhont@lorenz-law.com](mailto:j.dhont@lorenz-law.com)**W** [www.lorenz-law.com](http://www.lorenz-law.com)

**Areas of practice/expertise.** Partner Jan Dhont is Head of the Data Protection Department of Lorenz. Jan has built a truly international privacy practice advising a broad number of private sector companies as well as public bodies, including DPAs. Jan was previously in-house counsel of the Belgian DPA. He is now an active member of IAPP and often gives speeches on privacy and related matters.