

**Protection of personal data in Belgium**

**TABLE OF CONTENTS**

**A few useful definitions.....3**

**A preliminary formality.....4**

**The collection of data.....6**

**Under which conditions may personal data be processed?.....8**

**Sensitive data .....9**

**What to do with the data collected? .....11**

**Rights of the data subjects.....11**

**Data transfers abroad.....14**

## PROTECTION OF PERSONAL DATA IN BELGIUM

The spectacular development of information and communication technologies offers many possibilities and numerous advantages. The use of personal computers and telecommunication networks (the Internet) has increased the efficiency of services and facilitated our everyday life. Using these technologies, however, also implies new dangers for individuals' privacy and freedoms.

In a great number of cases, the data being spread relate to natural persons. Databases or files with personal data are created, used, disclosed, sold. It has become difficult to know who has data about whom and what they are doing with them. The individual no longer has control over his data. Consequently, the danger of abuse also keeps getting bigger.

Since 1992, a Belgian law ensured the protection of the individual in relation to the use of the personal data relating to him. This law introduced a duty of transparency when personal data are used: the individuals whose data are processed, must be informed of that, and the individuals processing the data have to identify themselves and communicate why they are processing the data. The law also establishes the rules for the use of personal data, that is what the data collected may or have to be used for. With this law, new rights were also introduced for individuals registered in data files or databases: the right to access the registered data, the right to rectify them, the right to object to the processing, ...

On 24 October 1995 a European directive (a legislative standard) was introduced with a view to harmonising the rules for personal data protection on the entire territory of the European Union. Just like all other member states, Belgium had to transpose the principles of that directive into Belgian law. The Law of 8 December 1992 (hereafter the Privacy Law) (Belgian Official Journal of 18 March 1993) consequently underwent significant changes, introduced by the Law of 11 December 1998 (Belgian Official Journal of 3 February 2001). Further modifications were made, among others with the Law of 26 February 2006 (Belgian Official Journal of 26 June 2003)<sup>1</sup>.

This general document takes into account the protective rules in force in Belgium since the Privacy Law was modified. It does not relate, however, to the establishment of Sectoral Committees within the Commission, nor to the specific rules for certain matters (credit registration, telecommunication, etc.). More detailed information about these matters (in French and Dutch) is available on the Commission's website (<http://www.privacycommission.be>).

---

<sup>1</sup> See also the Royal Decree of 13 February 1990 implementing the Law of 8 December 1992 (Belgian Official Journal 13 March 2001).

This is consequently not an exhaustive document. For more complete information, it is recommended to consult the legislative texts or the other documentation on the Commission's website:

<http://www.privacycommission.be>.

## **A FEW USEFUL DEFINITIONS**

### **What are personal data?**

Personal data are understood to mean any information relating to an identified or identifiable natural person (called the "data subject"), for example a person's name, a picture, a telephone number (even a professional phone number), a code, a bank account number, an e-mail address, a fingerprint, ...

The concept of personal data is not limited to data relating to individuals' privacy. Even the data relating to a person's professional or public life are considered as "personal data". Only data relating to a natural person are taken into account, not data relating to a legal person or an association (civil or commercial corporation or non-profit organization).

### **Who is the "data subject"?**

We are all data subjects. As soon as a person fills in a form, places an order, books concert tickets or buys a train ticket, uses a credit card, registers for a course or becomes a member of a sports club, is admitted to hospital, borrows a book from a public library or a videotape from a video shop, gives someone his mobile number, ... personal data are disclosed. The law does not make a distinction between Belgians and non-Belgians.

### **What does "processing personal data mean"?**

Processing means any operation or set of operations performed on personal data. The operations concerned are particularly varied and relate to the collection, storage, use, modification, disclosure of data, etc. Every time a person is asked to fill in an answer slip, this is considered as a processing operation carried out by the person that will collect the data. A hotel offering the possibility of online booking also processes data when registering the customer's name, the dates of his stay and his credit card number. A municipality disclosing the name of persons having submitted a building application to a contractor who wants to send them publicity, also processes personal data. The law is applicable as soon as personal data are processed, even partially, by automatic means. Those automatic means relate to all information technologies: computer technology, telematics, telecommunication networks (the Internet).

For example, the law applies to a computerized database containing a corporation's customers or suppliers, to the administrative service for vehicle registration, to the electronic list of transactions on a bank account, to a company's computerized personnel files or to a file with data of children enrolled in a school, etc. But the law is also applicable as soon as a single processing operation is carried out by automatic means. An employment agency keeping a written version of candidates' curriculum vitae but sending it to employers by fax, for example, has to observe the rules for all processing operations

it performs on the *curricula vitae* (storing, organizing, sending them). When the data are processed otherwise than by automatic means (especially on paper or on microfiche), the law nevertheless has to be observed if the data form part of or are intended to form part of a manual file, viz. an aggregate of data that can be accessed according to specific criteria (for example alphabetical order based on individuals' names).

### **Who is the controller?**

It is very important to know who is considered as "controller" by the law, for it is on this person that the law imposes almost all obligations regarding protection of the data being processed. He is therefore considered liable in case of problems. The controller is also the most important contact for the data subject and supervisory authorities. From a legal point of view, the controller is the person determining the purposes and the resources for the processing. The controller is a natural person or a legal person, an un-associated organization or a public authority.

If the purpose and the resources for the processing have been established by virtue of a law, decree or ordinance, the controller will be the natural person, legal person, un-associated organization or public authority designated as such by virtue of the law, decree or ordinance.

### **Cases where the data protection law is not applicable**

The data protection law does not apply to the processing of personal data *in the course of purely personal or household activities*, which is the case, for example, for a private address file or a personal electronic diary. That sort of files may be kept without taking the data protection law into account.

In a number of other cases, the law is applied only partially, as for *the purposes of journalism, and artistic or literary purposes*. A number of provisions must not be applied to such processing operations, so that a balance is created with regard to freedom of opinion. Also for processing operations carried out with a view to public security (by the State Security Service, ...) partial exceptions have been provided for.

### **A PRELIMINARY FORMALITY**

#### *Notification of processing operations and public register*

Prior to a completely or partially automatic processing operation (for example prior to the collection of personal data), the controller has to notify this to the Commission for the protection of privacy. Notification is not intended to request an authorization or permission, but only to notify a processing. Apart from very exceptional cases, in Belgium no authorization is needed to process personal data.

The notification form is directly accessible on the Commission's website:

<http://www.privacycommission.be>. A paper form, with an explanatory document, can also be requested on the website, by phone (+32 (0)2/213.85.40) or in writing (rue Haute, 139, 1000

Brussels). A fee has to be paid for each notification: 25 euros for an online notification, 125 euros for a notification on paper.

All information mentioned in the notification is entered into a public register, which is accessible to all members of the public in the offices of the Commission for the protection of privacy or at a distance, through the Internet. An extract from the register may also be requested.

#### *Contents of the notification*

The notification contains a description of the characteristics of the processing. The following elements have to be mentioned:

- the name of the processing;
- the purposes;
- the categories of data being processed (not the data themselves);
- any possible legal or regulatory basis for the processing;
- the categories of recipients to whom the data may be disclosed;
- the safeguards established for disclosure to third parties;
- the way in which the data subjects are informed of the processing;
- the person the data subjects may address to exercise their right of access and the measures taken to facilitate this;
- the categories of data intended to be transferred abroad, the countries of final destination and the reason why the data are transferred even if the destination countries do not ensure an adequate level of protection;
- the period of time after which the data must no longer be stored, used or disseminated;
- organizational and technical security measures.

#### *Exemptions from the duty of notification*

Besides manual processing operations (on paper or on microfiche), which do not have to be notified, a number of other automatic processing operations are exempt from the duty of notification provided that they meet the conditions set out in the Royal Decree of 13 February 2001 (Belgian Official Journal of 13 March 2001), viz.:

- processing operations carried out by a corporation with a view to personnel management;
- processing operations regarding the wages of the members of staff;
- processing operations related to accounting;
- processing operations in relation to customer or supplier management;
- processing operations carried out by a foundation or a non-profit organization concerning its members, supporters and the individuals the controller regularly contacts;

- processing operations carried out by schools and education institutions relating to their pupils and students.

Even if the controller is exempt from notification of those specific processing operations, he still has to make the information in the notification available to any person requesting it. This is most definitely not a useless task, but a contribution to good internal data management.

## THE COLLECTION OF DATA

### **Which obligations does a person have to comply with if he wants to collect personal data?**

The data have to be collected *fairly*, meaning that the person collecting the data has to act transparently: he has to indicate why he wants to obtain the personal data. He must not let other people believe that he has a purpose different from the one he has informed them of. He must also not act without the data subjects' knowledge (e.g. when you place an order on a website and have to disclose your personal data to do so, the website has to include a feature informing you about what will happen to your data. This feature is usually called "privacy policy").

*Information has to be provided* to the persons whose data are collected, unless they have already received that information. Besides the purposes of the data collection, as described above, the following elements have to be provided:

- the name and the address of the controller and of his representative in Belgium, if any;
- the recipients or categories of recipients of the data (persons to whom the data will be disclosed);
- whether it is compulsory to reply and what the possible consequences are if a person fails to do so;
- any individual's right to access and rectify personal data relating to him;
- if the data are processed with a view to marketing (publicity), the data subjects have to be informed that they have the right to object to such a processing operation free of charge.

Not providing this information when collecting the data is punishable with a fine of 550 to 550,000 euros.

### **Which data may be collected?**

Data may only be collected if they are *relevant and necessary* considering the announced purpose, for example:

- a shopkeeper may ask his customers for their name and address to send them invoices or to inform them about his commercial activities. He has no reason, however, to ask them for their date of birth or profession;
- it is not necessary for a school to ask for the salary of its pupils' parents;

- it is not necessary to ask for an individual's marital status in order to open a phone line for him, register him at the public library or give him a cable subscription;
- the psychological and social support service linked to a school must not systematically ask parents for information about family members' health and their medical history.

Certain *sensitive data* must not be collected, such as data relating to race, political opinions, religious or philosophical beliefs, trade-union membership, sex life, suspicions, persecutions, criminal or administrative convictions. There are a few exceptions, however (see "sensitive data"). Individuals asking for unnecessary or prohibited data are punishable with a 500 to 550,000 euro fine.

### **May data be collected from third parties?**

It is not always compulsory to contact the data subjects in order to obtain data about them. The data may be obtained from a third party (e.g. a general practitioner sends patient data to a specialist) or from institutions or companies owning databases they may disclose (a temporary employment agency may, for example, be asked for a list with the curriculum vitae of the individuals meeting a specific profile).

In that case, the following information has to *be provided* to the data subjects, unless they have already been informed:

- the name and the address of the new controller (the person having obtained the data) and of his representative in Belgium, if any;
- the purposes of the data processing;
- the categories of data involved;
- the recipients or categories of recipients of the data (persons to whom the data will be disclosed);
- any individual's right to access and rectify data relating to him;
- if the data are processed with a view to direct marketing (publicity), the data subjects must be informed that they have the right to object free of charge to such a processing operation. There is an *exemption from this duty*, however, if it is impossible or would involve a disproportionate effort to inform the data subject. But if one or more data subjects are contacted (at a later time), the elements listed above must be disclosed on that occasion.

A person indicating that it is impossible to inform the data subjects or that it would involve a disproportionate effort to do so, has to justify this to the Commission for the protection of privacy. He will add that justification to the notification he has to make before he begins to process personal data (see "preliminary formality").

## **UNDER WHICH CONDITIONS MAY PERSONAL DATA BE PROCESSED?**

To be allowed to process personal data (in other words collect, use, manage, disclose them etc. – see "A few useful definitions"), two conditions have to be met: the processing operation must aim at a specific and legitimate purpose and take place in the context of one of the six cases below.

### **Provided that a specific and legitimate purpose is aimed at ...**

The personal data may only be collected with a view to one or more specific purposes. They may only be used in accordance with those purposes. Moreover, the purposes have to be legitimate.

*One or more specific purposes:* personal data must not be collected and used without an exact purpose, which is determined at the beginning and affects the further sequence of activities. Based on the purpose that is aimed at, it can be established which data may be collected, what may be done with them, whether they may be disclosed and to whom, etc.

Only operations meeting the purposes aimed at may be performed, and they must be compatible with those purposes. Compatible is what has been laid down by law and what the data subject may *reasonably* expect. Individuals not respecting the originally announced purpose and using the data for other purposes, incompatible with the original one, use the processing operation unlawfully and are punishable with a 550 to 550,000 euro fine. Examples of such situations are given below:

- the mayor of a municipality, in the capacity of chairman of the board of directors of the municipality's day care centres, has access to the lists of the children and the elderly staying at the centres and uses these lists for his electoral campaign (mentioning in his flyers "I attach a great deal of importance to day care quality" or "The situation of the elderly is one of my priorities", according to the list he uses);
- a fitness club sells the list of its members to a company marketing diets;
- an ophthalmologist passes the names of his patients on to a company specialised in selling contact lenses (he may, however, pass his files to a colleague whose opinion he would like);
- a supermarket that keeps a file of all the purchases of a customer who has a loyalty card with a points system, and sells this file to a marketing company curious about all registered customers' preferences regarding food, drink, hygiene, about the quantity and the brand of the products purchased.

*A legitimate purpose:* to authorize the processing of personal data, the purpose aimed at must be legitimate. In other words, there has to be a balance between the controller's interest and the data subjects' interests. A purpose excessively violating the data subjects' privacy will not be considered as legitimate. For example:

□ creating a file of people going on sixty to send them documentation on their sixtieth birthday, concerning an insurance partially paying the costs of a funeral or cremation " because it is time to think about this", cannot be considered as legitimate. The disadvantage for the data subjects is undoubtedly greater than the controller's commercial interest.

### **... and in one of the following cases**

Personal data may only be processed:

- if the data subject has given his unambiguous CONSENT. The consent is only valid if it was freely given (in other words if it was not given under pressure), specific (the consent has to relate to a well-specified processing operation) and informed (the data subject was given all useful information on the intended processing operation). The consent does not necessarily have to be given in writing, but this does create problems with the burden of proof;
- if the processing is necessary for the performance of a CONTRACT or to take steps requested by the data subject with a view to entering into a contract. This is what happens when data are registered for invoicing, credits, insurance policies, etc.;
- if the processing is required under a LAW, decree or ordinance, for example the employer's duty to communicate certain data about his members of staff to social security;
- if the processing is necessary to safeguard a VITAL INTEREST of the data subject. When a victim of an accident loses consciousness, for example, and medical data relating to him (particularly results of blood tests) are collected with a view to his treatment;
- if the processing is necessary to perform a task of PUBLIC INTEREST or which is part of the exercise of public authority. In this context the Belgian railway company (NMBS/SNCB) has the right to keep a register of travellers with a season ticket and the postal service is authorized to create a file of address changes so that it can continue to deliver people's letters after their removal.
- if the processing is necessary to safeguard a LEGITIMATE INTEREST of the controller or of a third party, provided that it is not overridden by the data subject's interest or rights. The processing is authorized if the controller's interest in processing the data is greater than the data subject's interest in not processing the data.

## **SENSITIVE DATA**

### **Which data?**

Certain personal data are more sensitive than others. A person's name and address are innocent data, but that is not true for his political opinions, sexual preferences or an individual's judicial past. The law regulates the registration and use of these sensitive data much more strictly.

Sensitive data relate to race, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, prosecutions or criminal or administrative convictions.

## **Prohibited data ...**

In principle, it is prohibited to collect, register or ask to disclose the data mentioned above. Anyone doing so, is punishable with a 50 to 550,000 euro fine, and in case of recidivism with imprisonment from three months to two years.

## **... except in very specific cases**

Sensitive data may be processed, however, in well-defined cases.

### *Authorized cases:*

Except for data relating to suspicions, prosecutions and convictions, sensitive data may be processed with the *written* consent of the data subject. This exception is not valid, however, if the controller is the data subject's current or potential employer or if the data subject is in a dependent position with respect to the controller, preventing the former from giving his free consent. In such situations, written consent is nevertheless accepted if the processing would be advantageous to the data subject.

Sensitive data may also be processed if this is necessary to provide treatment (the processing then has to take place under the supervision of a health-care professional), if the processing is required by virtue of employment law, if it involves data manifestly made public by the data subject (e.g. an individual's membership of a political party after an electoral campaign), if the processing is necessary for scientific research, etc. Political parties, congregations, trade unions, public health insurance and other institutions may obviously register and use their members' data. They must not disclose the data to third parties, however, without the data subjects' consent.

Data relating to suspicions, prosecutions and convictions may be processed by a public authority if it is necessary for the fulfilment of its duties, by a lawyer to defend his clients, by any person to manage his own litigation or if it is necessary to achieve purposes laid down by law.

### *Additional precautions*

For all these cases the following additional safeguards have to be ensured:

- the controller has to designate the categories of individuals having access to the data, and give a precise description of their function with respect to the processing. The controller does not have to designate these individuals by name, but has to elaborate access profiles (e.g. the hospital's doctors and nursing staff);
- when the data subject is informed (see "Collection"), the controller has to mention the law or normative provision authorizing the processing operation. This is a way to check the controller's basis for processing data when in principle that is prohibited;
- if the processing operation is based on an individual's written consent to processing his sensitive data, this individual must be provided with the reasons why the data are processed and with the list of categories of individuals having access to the data.

## **WHAT IS TO BE DONE WITH THE DATA COLLECTED?**

### **Ensure the quality of the data**

The data being processed have to be exact and, if necessary, kept up-to-date. The controller must take all reasonable measures to rectify or erase incorrect or incomplete data. If he fails to do so, he is punishable with a 550 to 550,000 euro fine.

### **Ensure the confidentiality of the data**

The controller has to make sure that the individuals working under his authority only have access to and make use of the data they need to perform their duties. Under no circumstances may members of staff have access to data they do not need.

Moreover, the controller must inform his staff of the legal provisions on data protection. He has to explain the protection principles members of staff have to observe.

### **Ensure the protection of the data**

The data have to be protected from unwanted internal or external curiosity, as well as from unauthorized processing operations. The risk of data breaches and infringement of the data's integrity is all too clear – regardless of whether these violations are accidental or malicious. It is of fundamental importance to take security measures in order to protect the data.

There are two types of security measures: organizational measures (restriction of the number of individuals having access to the data, use of access codes, locking offices with computers and data files, etc.) and technical measures.

The more sensitive the data and the higher the risk for the data subject, the more precautions have to be taken. Data relating to a person's health, for example, that are used outside a medical context (such as when an insurance company wants to grant a life insurance), have to be protected with strict security measures. To provide clarity in this matter, the Commission has elaborated a document for the controller, containing reference measures for the protection of any processing operation. This document is available on the Commission's website ([link to reference measures](#)).

### **Erasure of data**

Personal data must not be kept in a form allowing for identification of the data subjects any longer than necessary for the purpose aimed at. They consequently have to be erased or anonymised. If not, a 550 to 550,000 euro fine may be imposed.

## **RIGHTS OF THE DATA SUBJECTS**

Any person, irrespective of his age, place of residence or nationality, has rights with respect to whoever is processing data relating to him:

### **The right to be informed**

personal data must not be processed without the the data subjects' knowledge. When personal data are collected, the data subjects have to be informed of the purpose of the collection. The law stipulates which data have to be provided. This formality has to be complied with, regardless of whether the data were obtained from the data subject or indirectly (See "Collection of data").

### **The right to ask questions**

Any person has the right to ask any controller whether the latter owns data about him. The controller then has to confirm whether he has data relating to the person asking the question. If so, he must clarify the purpose of keeping the data, what categories of data are involved and who the recipients of the data are.

### **The right of indirect access**

*What may data subjects access?*

Any person has the right to obtain an extract of the data being processed in an intelligible form, as well as all available information on the origin of the data. The right to know the origin of the data is particularly important, as it is especially this question that is relevant for the data subjects.

It is possible for a decision having far-reaching consequences for the data subject to be taken solely on the basis of an automatic processing operation (this may be the case for loans or insurance policies). The data subject must then also be able to access the logic the automatic processing is based on.

*How does the right of access have to be exercised?*

To exercise the right of access, the data subject must submit a request to the controller and include proof of his identity (for example a photocopy of his identity card). The request may be sent by letter or using any means of telecommunication (fax, e-mail with electronic signature).

The controller has to reply at the latest forty-five days after receipt of the request. If not, he is punishable with a 550 to 550,000 euro fine. Moreover, his failure to reply can be notified to the Commission for the protection of privacy and a complaint may even be made to a court (see below "Appeal"). This is also possible if the controller provided incorrect or incomplete information.

### **The right of indirect access**

In two cases, the data subject has indirect access to his data. He has access to *data relating to his health*, either directly, or through a person working in the health sector he has chosen himself, if the controller or the data subject request the intervention of an intermediary.

For *data processed with a view to state security, public security, defence, the prevention or punishment of crimes* there is also direct access. In those cases the data subject has to address the Commission for the protection of privacy, prove his identity, and request access to his data. The Commission will perform the necessary checks, will ensure that modifications are made if necessary, and will communicate to the data subject that the verification was carried out, without disclosing the data themselves.

### **The right of rectification**

Any person may have incorrect data relating to him rectified free of charge, and have incomplete, irrelevant or incomplete data erased or prohibited. The controller must answer the person having requested the rectification within one month. He has to mention what he has rectified or erased. If not, the data subject may address the Commission for the protection of privacy to submit a complaint. He may also bring the case before a court (see below "Appeal").

If incorrect, incomplete, irrelevant or prohibited data have been disclosed to third parties, the controller must inform the recipients of the data of the rectifications or erasures within one month, unless it is impossible or extremely difficult to do so.

### **The right to object**

Any person has the right to object to the processing of data relating to him, but he has to have serious and legitimate reasons for that.

*Restrictions of the right to object:* the right to object is not granted for a processing operation that is necessary to enter into or perform a contract; it is also impossible for data subjects to object to the processing of their data if it is imposed by a legal or regulatory provision.

If the data are collected with a view to *direct marketing* (including publicity), the data subject may object to the processing free of charge and without reason. When he is asked to fill in an answer slip and the person collecting the data intends to provide this slip to direct marketing companies, this has to be mentioned on the slip and the data subject has the right to object to the disclosure of his data without reason. If people are harassed on the phone with proposals to go and look at leather sofas or taste wine, they may also demand to be erased from the list of the person calling them.

### **The right not to be subject to an automatic decision**

It is not recommended that a decision imposed on an individual only depends on a machine. That is why it is prohibited by law that a decision having far-reaching consequences for an individual is taken purely on the basis of an automatic processing operation, intended to assess certain aspects of his personality.

This prohibition does not apply, however, when the decision is taken in the context of a contract (e.g. for loans or insurance policies) or if it is based on a legal or normative provision. The contract or provision must contain measures safeguarding the interests of the data subject, who has to have at least the right to make his opinion known *appropriately*.

### **Appeal in case of difficulties to have one's rights respected**

#### *To the Commission for the protection of privacy*

In case of difficulties when exercising the rights granted by law or when the obligations imposed by the law are not complied with, the data subject may submit a complaint to the Commission for the protection of privacy. The Commission will intervene to make the controller comply with the obligations imposed on him by law. It will try to come to an amicable settlement, but if it fails to do so, the Commission will issue an opinion on the legitimacy of the complaint. If it finds a crime has been committed, it will report this to the Public Prosecutor. The Commission's President may also submit any litigation about the application of the Privacy Law to the President of the Court of First Instance.

#### *To a court*

Dissatisfied persons may also make complaint to the Public Prosecutor at the Court of First Instance of his place of residence or to the President of this court. In that last case, legal assistance is recommended.

## **DATA TRANSFERS ABROAD**

### **Transfer of personal data to a Member State of the European Union**

Personal data may be transferred freely between European Union Member States. Anyone established in Belgium can consequently transfer data to another country of the European Union if it is legitimate according to Belgian Law (if the transfer is necessary to achieve the announced purpose of the processing or if it compatible with that purpose – see “Under which conditions may personal data be processed?”).

A bank may for example transfer data relating to its clients in order to make a payment; a Belgian hospital may inform an Italian social security institution of data relating to hospital admission costs for a member of the institution; a travel agency may send customer data to the Dutch airline and the Spanish hotel they have booked; a company may transfer its personnel files to another EU State.

### **Transfer of personal data outside the European Union**

Outside the European Union and more in general outside the European Economic Area personal data may only be transferred to countries ensuring a level of protection equivalent to that on European Union territory. Considering how easy data circulate thanks to new technologies, the lack of such a rule would quickly erode the elaborate protection measures of the European Union. Any controller

wishing to transfer personal data outside the European Union first has to make sure that the country of final destination offers an adequate level of protection.

If a country's level of protection can be considered adequate, the transfer may take place as if it involved two Belgian controllers or as if it were a transfer to another country of the European Union. Nevertheless the general principles of the law (among other things legitimacy, compatibility of the disclosure of the data to a third party with the original processing, informing the data subjects) will have to be observed.

The adequacy of the level of protection of countries outside the European Union will be assessed by the European Commission, partly on the basis of the general and sectoral legislation of the country concerned and of its professional rules. The European Commission has already recognized an adequate level of protection for the following countries: Switzerland, Canada, Argentina, the United States (if the recipient of the data has adopted the "Safe Harbor principles"), Guernsey and the Isle of Man. For all additional information or for the updated list of countries ensuring an adequate level of protection, it is strongly recommended to consult the European Commission's website.

If the country envisaged as final destination for a data transfer is not included in the European Commission's list, this does not necessarily mean that a transfer is impossible. The controller may also ensure adequate protection by means of a contract. Protection may be ensured, for example, with a binding contract for the person transferring the data and for the one receiving them, if the latter offers sufficient safeguards for data protection.

In Belgium such a contract needs to be authorized by Royal Decree, following the opinion of the Commission for the protection of privacy. To help controllers in this process, the European Commission has drawn up standard contractual clauses, which are automatically considered as sufficient safeguards for data protection. In Belgium, contracts copying the European Commission's standard contractual clauses exclusively and entirely do not have to be "ratified" in practice by Royal Decree, neither do they have to be authorized by the Commission. A copy of the contract will nevertheless have to be sent to the Commission, so that it can make sure the contract corresponds to the European Commission's standard contractual clauses.

Moreover, in principle these processing operations will have to be notified in the public register of the Commission, except if the applicable rules concerning notification provide otherwise. The standard contractual clauses are available on the European Commission's website. Multinationals envisaging data flows within their corporate group, if it includes members established outside the European Union, may also provide sufficient safeguards for data protection through internal codes of conduct (Binding Corporate Rules). These codes have to be ratified by the different national data protection authorities involved in the data flows (in Belgium a Royal Decree must be adopted, following the

opinion of the Commission for the protection of privacy). A coordinated European procedure was introduced, offering multinationals the possibility to submit their request to a national authority, which will then contact the other European authorities involved to jointly examine the draft code of conduct and take coherent decisions.

For more information, we advise you to consult the European Commission's website as well as the Working Papers that were approved by the Article 29 Working Party (including paper 74, 107, 108 and 133; the latter document contains a standard form for a coordinated approval procedure).

In the absence of an agreement, there are certain "exceptions" allowing for the transfer of data to third countries, for example when the data subjects give their unambiguous consent to the transfer of their data to such a country, if the transfer is necessary to perform a contract with the data subject or if the data come from a public register containing information for the public (e.g. phone book, trade register). These exceptions have to be interpreted restrictively and cannot constitute a normal framework for data transfers (See Working Paper 114 of the Article 29 Working Party regarding the common interpretation of the provisions of article 26, paragraph one of Directive 95/46/EC of 24 October 1995 (adopted on 25 November 1995). A contractual solution is recommended, as it provides more important safeguards for the protection of citizens' data.