Protection of Personal Data in Belgium

This is an unofficial translation of the Information Notes on the Protection of Personal Data in Belgium from the Belgian Privacy Commission's website at http://www.privacy.fgov.be

TABLE OF CONTENTS

PROTECTION OF PERSONAL DATA IN BELGIUM

The spectacular development of information and communication technologies offers many possibilities and numerous advantages. The use of the computer and telecommunications networks (Internet) elevates the effectiveness of the services and frequently facilitates everyday living. Nevertheless, the application of these technologies also holds new dangers for the privacy and the liberty of each one.

The dissemination of data in a large number of cases have related to persons. Databanks or files with personal data are tied up, applied, communicated, and sold. Henceforth, it is difficult to know who has whose data and what he must do with it. The individual no longer has control over data concerning him. For this reason, the danger of abuse becomes increasingly greater.

Since 1992, there exists a law in Belgium which guarantees the protection of the individual in respect of the use of his personal data. The law has introduced an obligation for transparency concerning the use of personal data: the persons, whose data are processed, must be informed of it, the persons who process the data, must identify themselves and communicate the purpose for which they process such data. Furthermore, the law lays down the rules concerning the use of personal data, namely to know what can or must happen with the obtained data. On the basis of the law, new rights have also been introduced for persons whose data have been incorporated in fact files or databanks: right to examine the recorded data, right to improve on it, to resist…

On 24 October 1995, a European Directive (legislative standard) was adopted with a view to harmonizing the rules concerning the protection of personal data in the entire territory of the European Union. Just like all the other member states, Belgium has transposed the principles of the Directive into Belgian law. As a result, the law of 8 December 1992 (B.S. 18 March 1993) has been amended thoroughly by the law of 11 December 1998 (B.S. 3 February 2001).

In this brochure, the new protection rules which come into force from 1 September 2001 in Belgium are presented. This brochure is not exhaustive and for continuous complete information it is necessary to consult the legal texts on the Commission's site (http://www.privacy.fgov.be).

SOME USEFUL DEFINITIONS

What is personal data?
Personal data shall mean any information relating to an identified or identifiable natural person (the 'data subject').

It can concern the name of a person, a photograph, a phone number (even a phone number at work), a code, a bank account number, an email address, a finger print,…

The term is not limited to data which concerns the privacy of persons. Data which are related to the professional or public life of a person are also considered as "personal data".

Only data which concerns a natural person will be taken into account and not that concerning a legal person or an association (civil or commercial company or a non-profit organization).

Who is the data subject?
Every one of us is a data subject. As soon as a person fills in a form, places an order, reserves a place for a concert or reserves a train ticket, uses a credit card, registers himself for a course or in a sports club, has himself hospitalized, borrows a book from a public library or a videocassette from a video library, he is supplying personal data.

The law does not distinguish between Belgians and non-Belgians.

What is understood as processing personal data?
Any operation or set of operations that is performed on personal data. The operations concerned vary and are related to the collection of data, storage, use, adaptation, disclosure of it, etc. Whenever a person is asked to fill in a reply tear-off slip, this would amount to processing by the person who will collect the data. A hotel which offers the possibility to make reservations by means of the Internet also processes data when it registers the name of the customer, the dates of the customer's stay and his credit card number. The municipality which passes on the names of the persons who submit a construction request to the contractor, who then wishes to send them promotions, also processes personal data.

The law applies as soon as processing of personal data occurs, whether wholly or partly by automatic means. Those automatic means are related to all information technologies: informatics, telematics, telecommunication networks (Internet). The law therefore applies for example on automated databanks in which the customers or suppliers of a company

have been registered, on the register for the registration of vehicles that the administration keeps, on the electronic list of the transactions on a bank account, the automated files of the staff in a venture or of the children who have been registered in a school, etc. The law also applies as soon as a single act of processing is performed by automatic means. Therefore, the employment agency which keeps a written version of the curriculum vitas of the candidates but transmits them by fax to employers must observe the regulations of the law concerning all processing it performs with their received curriculum vitas (storage, classification, transmission of them).

The person who places video cameras at the entrance of a building or a workplace also performs a processing as soon as the pictures of the persons who pass by the camera are registered and are or are not kept.

When the processing is carried out without the use of automatic means (especially on paper or microcard) the law must nevertheless be observed if the data is organized or incorporated into a manual filing system where the data can be accessed based on specific criteria (example an alphabetical sorting on the basis of the names of the persons).

Who is the Data Controller?

It is very important to know who is considered by law as "responsible for the processing". It is that person who has been charged with almost all obligations which the law places to guarantee the protection of the processed data. He therefore becomes responsible for the processing in the case of difficulties. The controller is also the most important conversational partner of the data subjects and of the supervisory bodies.

According to the law, the controller is the person who determines the purposes and means of processing personal data. It can be a natural or legal person, a factual association or public authority.

If the purposes and means of processing are determined by or by virtue of a law, decree or ordinance, the controller shall be the natural person, legal person, factual association or public authority that has been designated by or by virtue of that law, decree or ordinance as the controller.

Cases in which the law does not apply to the protection of data

This law does not apply to the processing of personal data which is carried out by a natural person in the course of exclusively personal or household activities. This is the case for example with a private address book or a personal electronic agenda. These types of filing systems may be kept without taking into account the law on the protection of personal data.

In a number of other cases, only a partial application of the law is anticipated. This is the case for the processing of personal data carried out exclusively for journalistic, artistic or literary expression purposes. A number of provisions cannot be applied on such

processing in order to ensure a balance on the aspect of protection of the freedom of expression of opinion.

For the processing of personal data which is performed in the framework of public security (by the State Security…) there are also partial exceptions.

PRECEDING FORMALITIES

Notification of the processing and the public register

Before a processing of wholly or partly by automatic means is performed (for example, before beginning with the collection of personal data), the controller must notify the Commission for the protection of privacy of the processing. The notification form is directly accessible on the site of the Commission (http://www.privacy.fgov.be) from 1 September 2001. A paper form and the explaining appendices are also available at the Commission through request by phone (02/542.72.31) or by written request (Waterloolaan 115, 1000 Brussel). For each notification, a payment must be made: 25 euro (1008 frank) when the notification is performed on a magnetic carrier, 125 euro (5042 frank) when the notification is performed by means of the papers form.

All information mentioned in the notification will be incorporated in the public register. Anyone can consult the register on location in the Commission for the protection of privacy's offices or remotely via the Internet. An excerpt from the register can be requested.

Contents of the notification

The notification contains a description of the characteristics of the processing. The following information must be mentioned:

- The name of the processing;
- The purposes;
- The categories of the processed personal data (not the data themselves)
- Possible legal or lawful bases for processing;
- The categories of recipients to whom the data may be supplied;
- The guarantees to be linked to the communication of data to third parties;
- The manner in which the persons to whom the data are related, are informed of it;
- The service where the right of access may be exercised and the measures taken to facilitate the exercise of that right;
- The categories of data transferred to a foreign country, the countries of destination, the reasons for the transfer of personal data to countries with no adequate level of protection taking place;
- The period of time whereupon the data may no longer be stored, used or disclosed;
- Organizational and technical security measures.

Exceptions to the obligation of notification

Along with the manual processing of personal data (on paper or microcard) which do not have to be indicated, are series of automatic processing of data which have been

exempted from the obligation of notification in so far as they observe the conditions stipulated by the Royal Decree of 13 February 2001 (Belgian State Gazette 13 March 2001), namely:

- Processing performed by a company with a view to personnel administration;
- Processing with a view to wage administration of personnel in service or in employment of the company;
- Processing concerning accountancy;
- Processing relating to the administration of clients or suppliers;
- Processing performed by a foundation or by a non profit organization concerning its own members, patrons and persons with whom the controller maintains regular contact with for the processing;
- Processing performed by schools and educational institutions concerning their pupils and students.

Even if the controller is exempted from the obligation of notification, he must nevertheless make available the same information as those incorporated in the notification on the request of the person who asks for it. Here, it is not a case of a certain meaningless task, but an element which contributes to good internal data management.

COLLECTION OF DATA

What are the obligations a person must comply with in the event he wishes to collect personal data?

The collection must be done fairly and lawfully. This means that the act must be transparent: the person who collects the data must indicate his reasons for obtaining the personal data. He cannot make believe a certain purpose for striving after the data whilst he has other intentions with the collected data. There can also not be any act without the knowledge of the data subjects (for example, by placing video cameras without informing the persons who are being filmed of it).

Information must be provided to the persons from whom the data is collected, unless they have it already. Along with what has already been stated concerning the objectives of the collection, the following information must be provided:

- The name and address of the controller and if such is the case, of his representative in Belgium;
- The recipients or categories of recipients of the data (persons to whom the data are communicated);
- Whether or not 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;
- If the data are processed with a view to direct marketing (act of publicity), the existence of the right to object on request and free of charge against the intended processing.

He who does not provide the said information when he collects data can be punished with a fine of 500 up to 500.000 Euro (20.000 BEF up to 20 million BEF)

Which type of data can be collected?

Only data which are *relevant and necessary* taking into account the purposes disclosed can be collected, for example:

- A trader can ask for the name and address of his customers in order to send them their invoices or to inform them of his commercial activities. However, he has no reason to ask for their birth date or profession;
- For a school, it is not necessary to ask for the wages of the parents;
- It is not necessary to ask for the civil status of a person in order for him to apply for a telephone line, register him in a public library or distribute to him a cable subscription;
- The accompanying psychosocial service linked to a school cannot systematically collect from all parents the accompanied classes of information concerning the medical condition and medical history of the family members.

Data of a sensitive nature cannot be collected. This is illustrated in respect of data in relation to race, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, suspicions, prosecutions, criminal or administrative convictions. This collection of data has been prohibited in principle. However, there are certain exceptions (see "sensitive data").
Persons who ask for unnecessary or prohibited data can be punished with a fine of 500 up to 500.000 Euro (20.000 BEF up to 20 million BEF).

Can data be obtained from third parties?

It is not always obligatory to turn to the data subjects in order to obtain data concerning them. The data can be obtained from a third party (for example, a general practitioner sends the data of a patient to a specialist) or from institutions or societies which have data banks which they can communicate (an employment agency can for example, be asked for a list with the curriculum vitae of persons who answer to a desired professional profile).

In this case, the following information must be provided to the data subjects, unless they have it already:

- The name and address of the new controller (the person who has obtained the data) and if such is the case, his representative in Belgium;
- The purposes of the processing;
- The categories of the data concerned;
- The recipients or categories of recipients of the data (persons to whom the data is communicated);
- The existence of the right of access to and the right to rectify the personal data concerning him;
- If the data are processed with a view to direct marketing (act of publicity), the existence of the right to object on request and free of charge against the intended processing.

However, an exemption to this obligation applies where it is impossible or it requires a disproportionate amount of effort to inform the data subject. However, if one or more of the data subjects are contacted (later), then at that time the abovementioned data must be provided. The person who indicates that it is impossible or it requires a disproportionate amount of effort to inform the data subjects must justify himself at the Privacy Commission. He must add this justification in the notification before starting the processing (see "Preceding Formalities").

UNDER WHICH CONDITIONS CAN PERSONAL DATA BE PROCESSED?

Personal data may be allowed to be processed (i.e. to collect, to use, to manage, to communicate… see "Some Useful Definitions"), subject to two exceptions: pursue a specific and justified purpose and be included in one of the six instances described below:

Provided a specific and justified purpose is pursued…
The personal data can only be collected with a view to one or more specific purposes. They can only be used in conformity with those purposes. Moreover, those purposes must be justified.

One or more specific purposes: no personal data can be collected and no decision may be made to use them without an accurately well-defined purpose. This purpose is defined at the beginning and stipulates further course of activities. On the basis of the pursued purpose, it can be determined which data can be collected, what can be done with the data, if it can be communicated and to whom, etc…

Only actions which fulfill and are compatible with the pursued purposes can be performed. What is considered compatible is that which is stipulated by law and what can be reasonably expected by the data subject.

Persons who do not observe the originally announced purpose and uses the data for other purposes incompatible with the said purpose, makes improper use of the processing and can be punished with a fine of 500 up to 500.000 Euro (20.000 BEF up to 20 million BEF). That is for example the case where:

- The mayor of a municipality who has access as the president of the council of the governing board of the municipal's child day care centres and retirement homes to the list of those registered in these institutions and uses this list for his election campaign (where he states in his leaflets "I attach much importance to the quality of childcare" or "the situation of the elderly is my priority" depending on the list he uses);
- The fitness club which sells their members list to a company which offers weight loss treatments;
- The oculist who passes on the names of its patients to a company which specializes in the sale of contact lenses (he may however, pass on his files to a colleague to know his opinion);
- A big department store which sells its files containing all recorded purchases of each customer who has a point-system loyalty card to a marketing company which wants to know the preferences of each registered customer concerning food, drink, hygiene, quantities purchased and brand of chosen products.

A justified purpose: In order for the processing of personal data to be permitted, the pursued purpose must be justified. This means that a balance must exist between the interest of the data controller and the interests of the persons to whom the processed data are related. A purpose which would be an excessive violation of the privacy of the data subjects would not be considered as justified. For example:

- Placing a security camera at the entrance of an apartment building which records comings and goings is a serious violation of the privacy of the occupants and visitors of the building (one would know who has entered, who has gone out, at what time and in whose company). This is a processing of personal data which can only be justified (or it can be considered justified) if this security reason is really necessary. This would be the case if the building is regularly burgled or the target of vandalism.
- Compiling a file of people who are almost 60 years old to send them documentation on their 60th birthday on an insurance that would contribute in the cost of a funeral or cremation "because the time has come to think about these things", can also be considered to be not justified. The disadvantage which these persons experience is undoubtedly larger than the commercial interest of the person who compiles the file.

…and provided that one of the following cases occurs

Personal data can only be processed:

- If the data subject has given his unambiguous CONSENT. The consent is only valid if it concerns a voluntarily given consent (in other words, in cases where it was given without the exercise of pressure), specific (the consent must concern an accurately well-defined purpose) and it has to be given with full knowledge of the matter (the person has received all useful information concerning the intended processing). It is not necessary for the consent to be in writing although there will be the problem of burden of proof;

- Or if the fact of processing is necessary for the performance of a CONTRACT or for the performance of pre-contractual measures at the request of the data subject. This is the case for the recording of data which is necessary in order to invoice a service, to grant credit, to set off an insurance policy, etc.

- Or if the processing is required by LAW, decree or ordinance. This is for example the case for the obligation of the employer to communicate certain information concerning his personnel to social security;

- Or if the processing is necessary to protect the VITAL INTEREST of the data subject. This is the case concerning the unconscious victim of an accident where medical data (in particular blood tests) are collected with a view to his care;

- Or if the fact of processing is necessary for the performance of a TASK carried out in the PUBLIC INTEREST or in the exercise of official authority. In this

respect, the NMBS (National Railways) has the right to keep a register of the holders of a train subscription and the Post has been authorized to keep a file of the changes of addresses to enable it to offer the option to forward mail in the event of a change of address;

- Or if the processing is necessary for the LEGITIMATE INTERESTS of the data controller or a third party to whom the data are disclosed, provided that the interests or rights of the data subject do not prevail. The processing is permitted if the interest of the compiler to process the data is higher than the interest of the registered person not to process the data.

SENSITIVE DATA

Which data?
Certain personal data are of a more sensitive nature than others. The name and address of a person are in fact innocent data but this is not the case concerning his political opinions, sexual preferences, or his past legal history. The law regulates the recording and the use of these sensitive data in a much stricter manner.

It concerns data in relation to race, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, suspicions, prosecutions, criminal or administrative convictions.

Prohibited data…
It has been prohibited in principle, to collect, to record or to request to communicate the above described data. Persons who do the above, can be punished with a fine of 500 up to 500.000 euro (20.000 BEF up to 20 million BEF) and in case of recurrence with a prison sentence from 3 months up to 2 years.

…except in very specific cases
These data can however be processed in accurately, well-defined cases.

Permitted cases:
With the exceptions of data concerning suspicions, prosecutions and convictions, sensitive data can be processed after the data subject has given his *written* consent. However, this exception does not apply in the case where the data controller is the current or potential employer of the data subject or when the data subject is in a dependant position in relation to the data controller, which prevents him from voluntarily refusing or consenting. In such a situation, the written consent is nevertheless accepted if through this the data subject can be given an advantage.

These data can also be processed if it is necessary to provide care (the processing must then take place under the supervision of a health professional), if the processing is necessary under employment law, if the processing relates to data that are apparently made public by the data subject (e.g. the membership of a political party of a person who has conducted an election campaign), if the processing is necessary for scientific research, etc.

Political parties, congregations, trade unions, health insurance funds and other institutions can naturally record and use the data of their members. However, they cannot communicate such data to third parties without the consent of the data subjects.

The data concerning suspicions, prosecutions and convictions can be processed by a government authority if that is necessary for the performance of its tasks, by a lawyer for

the defense of his clients, by every person for the management of his own litigation or if it is necessary for the realization of the objectives defined by law.

Additional precautionary measures
For all these cases, additional safeguards must be considered, namely:

- The data controller must designate the categories of persons who have access to the data, as well as define precisely what their function is in respect of the processing. This obliges the data controller not to designate persons by name but to develop profiles for access (e.g. doctors and nursing personnel of a hospital);
- At the time of informing the data subject (see "Collection") the data controller must state the law or the legalizing provisions on which basis the processing of data is permitted. Through this it can be examined on which grounds the data controller justifies the processing of data prohibited in principle.
- In case the written consent of a person to process his sensitive data forms the basis of the processing, the reasons for which those data are processed must be communicated to that person and he must be provided with the list of the categories of persons who have access to that data.

WHAT TO DO WITH THE DATA COLLECTED?

Take care of the quality of the data

The processed data must be accurate and if necessary, updated. The data controller must take all reasonable measures to rectify or erase inaccurate or incomplete data. If he does not do so, he can be punished with a fine of 500 up to 500.000 euro (20.000 BEF up to 20 million BEF).

Take care of the confidentiality of the data

The data controller must ensure that the persons, who work under his authority, only have access to and can use those data which are necessary for the performance of their tasks. Under no circumstance can members of personnel be granted access to data which is not necessary.

Moreover, the controller must inform the personnel the legal regulations concerning data protection. He must inform the principles of protection which must be promptly observed.

Take care of the security of the data

The data must be protected against harmful internal or external curiosity, as well as against non-permitted processing. The risk of leaks and violations of the integrity of the data is now all too clearly present. These violations can be accidental or malicious. It is of fundamental importance to take security measures to protect the data.

These security measures are of two kinds: organizational measures (restriction of the number of persons who have access to the data, use of access codes, locking up of the rooms in which the computers and data files are, etc) and technical measures.

The more sensitive the data concerned and the larger the risk for the data subject, the more the precautionary measures that must be taken. For example, data concerning the health of a person, used outside a medical context (for example, used by an insurance company to grant a life insurance) must be protected through strict security measures.

Erasure of data

Personal data cannot be kept in a form that permits identification of persons for longer than necessary in proportion to the pursued purpose. They must be erased or made anonymous. If not a fine of 20.000 up to 20 million BEF (... euro) can be imposed.

RIGHTS OF THE DATA SUBJECTS

Unto everyone, irrespective of their age, place of residence or nationality, rights are granted in respect of persons who process data concerning him

Right to information

Personal data cannot be processed without the knowledge of the data subjects. When personal data are collected, the data subjects must be informed of the purpose of that collection. It is defined in the law what information must be communicated. This formality must be fulfilled, irrespective of whether the data has been obtained from the data subject himself or indirectly (See “Collection of data”).

Right to ask questions

Everyone has the right to ask the data controller whether or not he has data concerning him in his possession. The questioned controller must confirm whether or not he has data concerning him and, if such is the case he must clarify the purpose for which he has this data, which categories of information it concerns, and who are the receivers of this data.

The right to direct access

To what do the data subjects have access?

Everyone has the right for a copy of the processed data in an intelligible form, as well as to receive all available information as to the source. The right to know the source of the used data is particularly important because it is especially this question which interests the data subjects.

It is possible that a decision, which has an important impact for the data subject, be taken only on the basis of an automated processing (this can be the case for the granting of a loan or the undersigning of insurance). In that case, the data subject must be able to access the logic which underlies the automatic processing concerned.

How does the right of access have to be exercised?

To exercise the right of access, the data subject must direct a request to the data controller and in so doing provide proof of his identity (for example by adding a photocopy of his identity card). The request can be through the post or via whatever means of telecommunication (fax, e-mail with electronic signature.

The controller must answer within forty-five days after the receipt of the request. Otherwise, he can be imposed with a fine of 500 up to 500.000 euro (20.000 BEF up to 20 million BEF). Moreover, such behaviour can be indicated to the Commission for the protection of privacy and a complaint can even be submitted to the judge (see below "Appeal"). This also applies when the data controller has provided inaccurate or incomplete data.

Right to indirect access

In two cases the data subject has indirect access to his data.

The person to whom the data are related has access to *data relating to his health*, either directly or through a health professional chosen by the data subject, upon the request of the data controller or the person himself for a mediator.

For data processed for state security, public security, defence of the realm, prevention or the punishment of indictable offences, an indirect access is also foreseen. In these cases, the data subject must address the Commission for the protection of privacy, whereby he provides proof of his identity and asks to consult the data concerning him. The Commission carries out the necessary controls, has the necessary modifications carried out and communicates to the data subject that the verification has been performed without exposing the contents of it.

Right to rectification

Everyone can, free of charge, rectify incorrect data relating to him, and erase incomplete, irrelevant or prohibited data or prohibit the use of them.

The data controller must within one month answer the person who has requested for the rectification. He must mention the rectifications or erasures carried out by him. Otherwise, the data subject can address the Commission for the protection of privacy to make a complaint about the behaviour of the controller. He can also lodge a complaint with the legal authorities. (see below "Appeal").

In case incorrect, incomplete, irrelevant or prohibited data have been provided to third parties, the controller must within one month communicate the carrying out of the rectifications or erasures to the persons to whom those data are communicated, unless this is evidently impossible or extremely difficult.

Right to object

Everyone has the right to object against the processing of data relating to him but to that end, he must invoke serious and justified reasons.
Restrictions of the right to object: the right to object is not permitted for the processing necessary at the closing or the implementation of an agreement; the data subjects also cannot object to the processing of their data, which have been imposed on the basis of a legal or lawful obligation.

When the data are collected with a view to direct marketing (act of publicity), the data subjects can free of charge and without any grounds object against the processing of his data. When there is a request to fill up a reply tear-off slip and the person collecting the data intends to give them to direct marketing companies, then he must mention this on the slip and the data subject has the right to object without any justification. Also the person, who is harassed by telephone proposals to go view leather furniture or to sample wine, can demand to be removed from the list of the person who called him up.

The right to be subject to an automated decision

It is not desirable that a decision which is imposed on a person depends simply and solely on the decisions of a machine. Thus, the law prohibits that a decision which has a serious impact on a person is taken only on the basis of automatic data processing that is destined for the evaluation of certain aspects of his personality.

This prohibition is however not applicable when the decision is taken within the framework of an agreement (for example the granting of a loan or undersigning of insurance) or is founded on a law or legalizing provision. In such agreement or provision appropriate measures must have been foreseen which guarantees the protection of the interests of the data subject. This last-mentioned must at least have the right to enforce his opinion in an *appropriate manner*.

Appeal where there are difficulties to have his rights respected
At the Commission for the protection of privacy

In case of difficulties with the exercise of the rights granted on the basis of the law or in the case of non-compliance of obligations resulting from the law, the data subject can direct a complaint to the Commission for the protection of privacy. This Commission intervenes to make the data controller comply with the obligations imposed on him by law. It tries to settle disputes amicably. In case of failure, the Commission advices on the soundness of the complaint. If it determines an indictable offence, it notifies the King's attorney. It can also present the dispute to the President of the tribunal of first instance.

At the court

Dissatisfied persons can also lodge a complaint with the King's attorney at the tribunal of first instance of their place of residence or get hold of the President of this tribunal.
In that last case, a lawyer is recommended for assistance.

TRANSFER OF DATA TO A FOREIGN COUNTRY

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

Personal data is as of now is freely transferable between Member States of the European Union. A person who is established in Belgium can therefore freely transfer personal data to another country of the European Union if this is justified according to Belgian law (if these transfers are necessary to achieve the announced purpose of the processing or if it is compatible with that purpose – see "Under which conditions can personal data be processed?").

A bank for example, can transfer data concerning one of its customers to execute a payment in France; a Belgian hospital can communicate the data to an Italian social security institution concerning the hospital expenses of a member of that institution; a travel agency can transfer data concerning its customer to a Dutch airline company and to a Spanish hotel reserved by the customer; a company can transfer personnel file to another state of the Union.

Transfer of personal data outside the European Union

Personal data is only transferable to countries outside the European Union which offer an equivalent protection to that offered on the territory of the European Union. Given the ease with which data can be transferred thanks to new technologies, the lack of such a rule would quickly undermine the extended protection guaranteed by the European Union.

All data controllers who wish to transfer personal data out of the European Union must firstly consider if the country of destination offers an appropriate level of protection for such data. The same principles of protection must be available as those established on the territory of the European Union. To assess the quality of the offered protection, the legislation of the country concerned, the applied deontological rules, etc. must be taken into account. In case of doubt, one can ask the Commission for the protection of privacy if a certain country offers appropriate protection or if transfer of data to that country is permitted.

Nevertheless, in certain cases, there can be transfer of data to countries which *do not offer an appropriate level of protection*. This is especially the case when the data subjects have given their unambiguous consent to the transfer of their data to such a country, when the transfer is necessary for the performance of a contract with the data subject or when the data comes from a public register which is intended to provide information to the public (for example, telephone guide, trade register).

The data controller can himself also offer appropriate protection via an agreement. Thus protection can be offered by means of an agreement which is binding on the person who transfers the data and on the one who receives them and which contains sufficient

guarantees concerning data protection. The European Commission proposes a model agreement which offers sufficient guarantees. This agreement is available on the Internet site of the Commission (http://www.privacy.fgov.be).

1 September 2001

