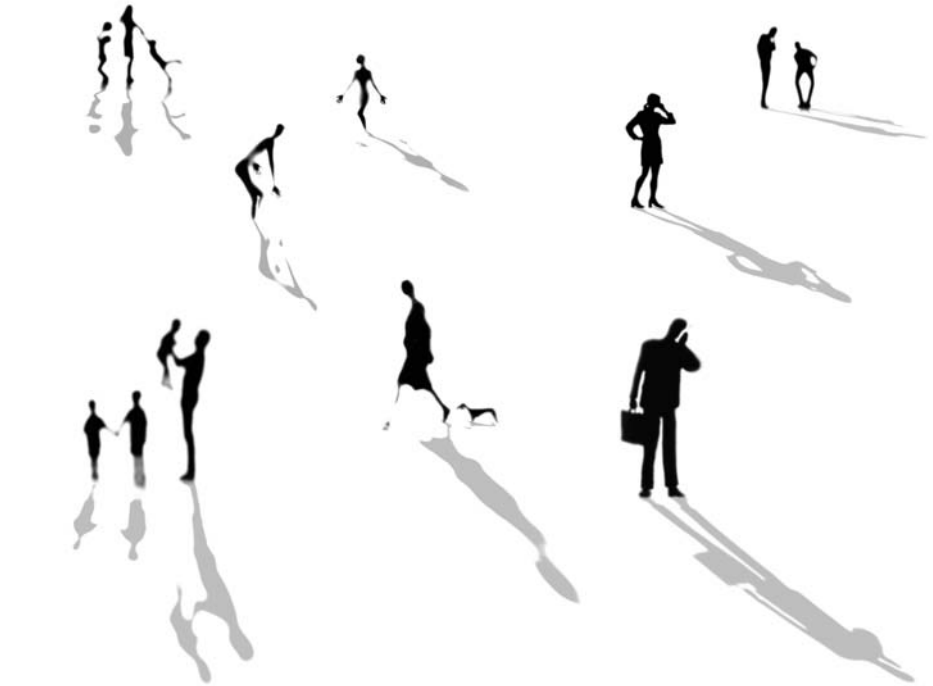


Data **protection** and **privacy**

PRIVACY AND PROCESSING OF PERSONAL DATA

SUMMARY

WHAT IS **DATA PROTECTION?**

In the information society, there are numerous organisations and institutions collecting more and more information about individuals.

We all disclose personal information, voluntarily or not, to a multitude of organisations, for example, to:

- local or government authorities (permits, licences, grants);
- tax authorities (tax return);
- doctors and pharmacies (consultations and prescriptions);
- health insurance funds (claims);
- banks (loan applications and credit card statements);
- supermarkets (loyalty cards and lotteries);
- mobile phone operators, post and telecommunication services (telephone communications);
- sports clubs, cultural and leisure organisations (membership cards);
- or simply when browsing the Internet, or even spending the afternoon shopping because of the recordings of surveillance systems.

In this way, the circulation of our personal data is growing and spreading to more and more places.

Due to modern computing techniques, this data can now be exploited more easily and in a variety of ways, either by the State and its authorities, by companies and professionals, or by clubs and associations.

The building of personal profiles which reveal our life style and consumer habits is becoming a common practice (surveys, customer cards, Internet, etc).

Whether data is collected or recorded, consulted or disclosed to third parties, there are real and constant risks for the identifiable person, resulting from this accumulation and exploitation of personal data.

However, loss of control over your personal data and unwarranted intrusion into your private life are not inevitable, far from it. The **law of 2nd August 2002** which transposes a European Directive relating to data protection [1] affords you certain rights. The law aims at protecting the privacy of individuals (and so even the interest of corporate bodies) with regard to the processing of their personal data by third parties.

The authorities, companies, professionals, associations and other organisations who collect, record, use and disclose personal data cannot do so without restrictions. They must notify the identifiable person ("data subject") and inform them of the purpose of what the law calls "the processing of personal data". This processing must be limited to what is necessary and proportionate to the aims stipulated at the outset. Data must therefore always be used in accordance with strict rules, under the supervision of the *Commission nationale de protection des données* [2]. To ensure transparency, any filing system must previously be either declared or authorised (depending on the type of data and processing).

The legislation on the protection of personal data does not only apply to computer files, but covers every kind of medium (paper files, audio and video recordings).

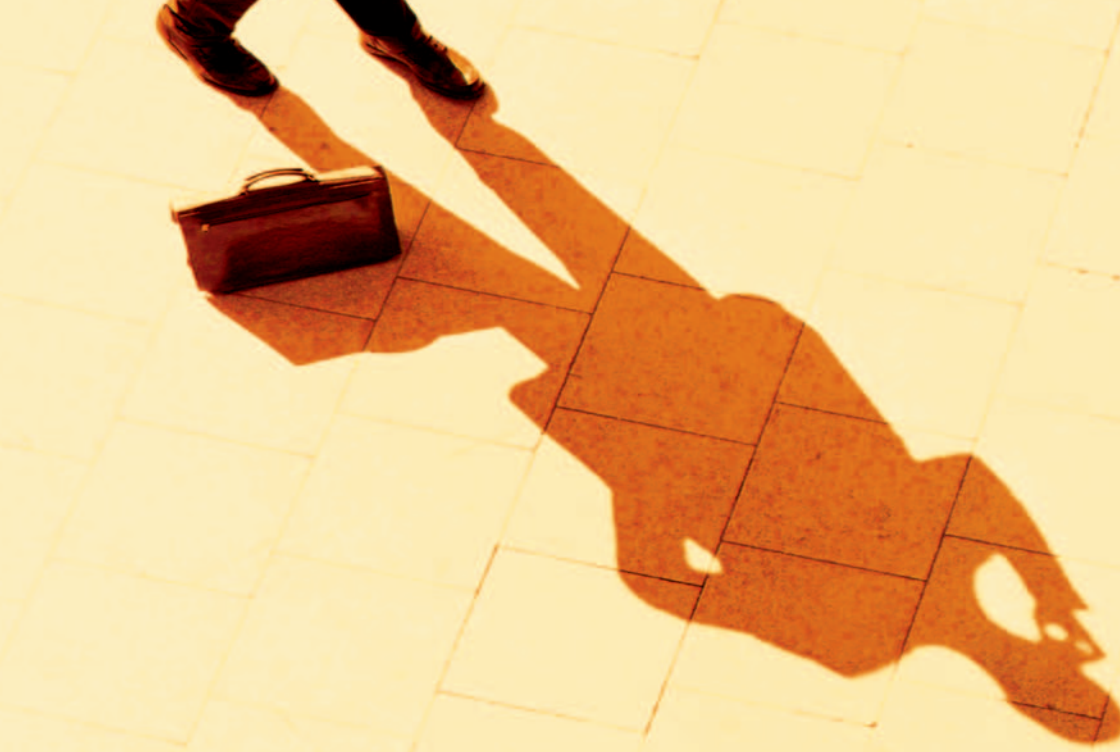
[1] (Directive 95/46/EC dated 24 October 1995)

[2] www.cnpd.lu

The protection of privacy is a fundamental right, just like the inviolability of the home, the confidentiality of correspondence and freedoms of opinion and expression.

The same principles apply in all 25 Member States of the European Union and beyond (Switzerland, Norway, Liechtenstein, Iceland, etc).

THE 10 COMMANDMENTS
OF PERSONAL DATA PROTECTION



Those who process personal data concerning other people must comply with to the following principles:

1. THE PRINCIPLE OF LEGITIMACY

The processing of personal data is allowed only if there is a legitimate reason to justify it. Anyone who wants to process data concerning you must ask for your consent beforehand. Data processing is also permitted if it is essential in order to fulfil a contract, a task in the public interest or a legal obligation, or to protect your life. Finally, the processing can be legitimate if there is a justified interest, provided the processing of your data has only a minimal effect on your privacy.

This first criterion is used to determine whether the processing is legal. It answers the question of **when** your data can be requested and used. The next principles describe the rules that must be observed when processing your data. They answer the question of **how** your data can be processed.

2. THE PRINCIPLE OF PURPOSE

The use of your personal data (including images and sounds) must be rigorously confined to a purpose which has been explicitly determined beforehand.

The collection, recording and use of your personal data are strictly limited to what is necessary to achieve the aims specifically declared in advance by the authority, agency, company, association, professional or self-employed worker involved.

These users cannot disclose the data to other organisations or people, unless it is needed to accomplish the same aims.

EXAMPLE

Following an accident at work, your employer tries to find out about your state of health from your GP. Thinking she is doing the right thing in reassuring him, the doctor's assistant provides information on the doctor's diagnosis.

In doing so, she is transgressing the purpose for which the medical practice holds this information, i.e. in order to provide health care.

3. THE PRINCIPLES OF NECESSITY AND PROPORTIONALITY

The principle of proportionality ensures that the processing of your personal data is limited to cases where there is a direct connection with the initial purpose of the processing. The information must not only be useful, but also necessary to whoever is processing your data. The data being processed must not be excessive in relation to the aim pursued.

EXAMPLE

When booking a table at a restaurant by telephone, the manager of the establishment asks you to supply your credit card number.

This information should be regarded as excessive in relation to the aim being pursued, which is only to arrange available tables.

4. THE PRINCIPLE OF THE ACCURACY OF DATA

As inaccurate or incomplete information can harm the person to whom it relates, every effort must be made to ensure the data being processed is correct and up-to-date. If this is not the case, the personal data must be rectified or erased.

The law also protects you against any negative decision automatically taken about you by a computer, without you being able to put forward your personal point of view.

EXAMPLE

You are applying to your bank for a personal loan to buy some furniture. After submitting your application via the Internet, you immediately receive a negative reply from your bank which refuses to grant you the requested loan. It transpires that no bank adviser has been involved, but that your application has been assessed using a software which evaluated your request upon pre-established ratios and statistics.

In this event, you have the right to insist on your application being re-examined on the basis of an interview with your bank adviser who should listen to your argumentation.

During this interview, you might point out, for example, that your financial situation has recently improved thanks to an inheritance. It could even be possible that the figures used were incorrect or that there was a mix-up with a debt-ridden person of the same name.

5. THE PRINCIPLE OF FAIRNESS

Your personal data must be collected, recorded, used and communicated fairly, and with your knowledge.

Also, your data must be erased or rendered anonymous as quickly as possible. Subsequent use of your personal data for purposes other than those stipulated from the outset, is prohibited as a rule.

EXAMPLE

Your supermarket offers you a loyalty card to give you special discounts on your shopping or an end-of-year rebate. As you subsequently pass through the checkout, the contents of your basket are recorded and used to build a consumer profile, which will be monitored on a regular basis.

If this is done without your knowledge, and if you weren't informed about it when signing up, the principle of fairness has been violated.

6. THE PRINCIPLE OF SECURITY AND CONFIDENTIALITY

Your personal data must be processed in a confidential manner and stored in safe forms and places.

In the event of non-compliance with this principle, the person who processes your data assumes personal responsibility. This includes the individual behaviour of employees, and contracts entered into with subcontractors (suppliers for instance) as well as the choice of technical equipment (in terms of computer security).

EXAMPLE

You want to change your mobile phone network. However, having looked at your application, the sales consultant of the company you have just chosen refuses to accept you as a new client. This person, who used to work as a sales agent for your previous GSM operator, refers to a dispute over a bill which you had with the first company.

By allowing its sales agents to obtain information from its accounts department, your previous GSM operator failed to ensure that personal information on its clients could only be accessed by those employees really needing it for their work.

So, was the staff properly warned against the temptations of misusing client-related data? How was the sales agent able to bring a client file from his old employer to his new employer? Was the file stolen?

Whatever the case, the security measures and internal organisation of the company were inadequate in terms of maintaining the confidentiality of personal data. The management which failed in its legal obligations, as well as the unscrupulous employee are to blame for this.

7. THE PRINCIPLE OF TRANSPARENCY

The law guarantees that you can obtain the information you need about the processing operations performed on your personal data and gives you the opportunity to exercise personal control. Anyone who wants to process your personal data must notify you when the data is collected or in the event of your data being communicated to third parties.

You have the right to request details of the personal information on record and about its use, you also have the right to demand that any data not processed in accordance with the law be deleted.

The registration of all databases with the C.N.P.D. contributes to transparency. The public register of the processing of personal data will be accessible via its website [3].

EXAMPLE

Seeing that you have been in a state of exhaustion for a long time, your GP suggests having your blood analysed to determine the causes of your fatigue. The blood sample is taken by an external laboratory, which sends the results of this analysis to your doctor. It turns out that an HIV test has been done without your knowledge.

This constitutes a breach of the principles of transparency and loyalty.

[3] www.cnpd.lu Expected to be on line by the end of 2004.

8. PARTICULARLY SENSITIVE INFORMATION IS SUBJECT TO EVEN MORE STRINGENT PROTECTION

The processing of personal information which reveals your opinions and beliefs, or which relates to your state of health or your sex preferences, including your genetic data, is prohibited, apart from a few exceptions which are enumerated in a restrictive way in the law.

Moreover, the processing of this type of data must, in principle, be explicitly authorised by the C.N.P.D.

EXAMPLE

At a job interview, the company's Human Resources Manager to whom you are presenting yourself asks you what you think about financing retirement and the respective views of the political parties on this subject. He also makes it known to you that he keeps a list of employees who are members of trade unions.

Gathering this kind of information (sensitive data) is normally prohibited by the law.

9. SURVEILLANCE (VIA AUDIO, VIDEO, DATA) OF IDENTIFIABLE PEOPLE IS STRICTLY LIMITED BY LAW

An authorisation from the C.N.P.D. is required before using technical means for monitoring people, particularly by video camera, electronic tracing, etc. Personal data gathered in this way can only be processed under certain very specific circumstances enumerated by the law. This includes surveillance on public premises, in public transportation, in shopping centres and also at your workplace. In the latter case, surveillance cannot be undertaken unless the staff representatives, joint committee or the *Inspection du travail et des mines* and yourself, have been previously informed.

EXAMPLE

Your telephone conversations are recorded by the company you work for, without you having been told beforehand.

This is contrary to the principle of transparency. Furthermore, the employer requires authorisation from the C.N.P.D., which is responsible for verifying the legitimacy and proportionality of such a practice.

10. USE OF YOUR PERSONAL DATA FOR ADVERTISING OR MARKETING PURPOSES REQUIRES YOUR PERMISSION

You may object to the use of your personal data for commercial purposes at any time. Direct marketing using modern means of communication (SMS, e-mail, etc) is in principle prohibited if you haven't given your consent.

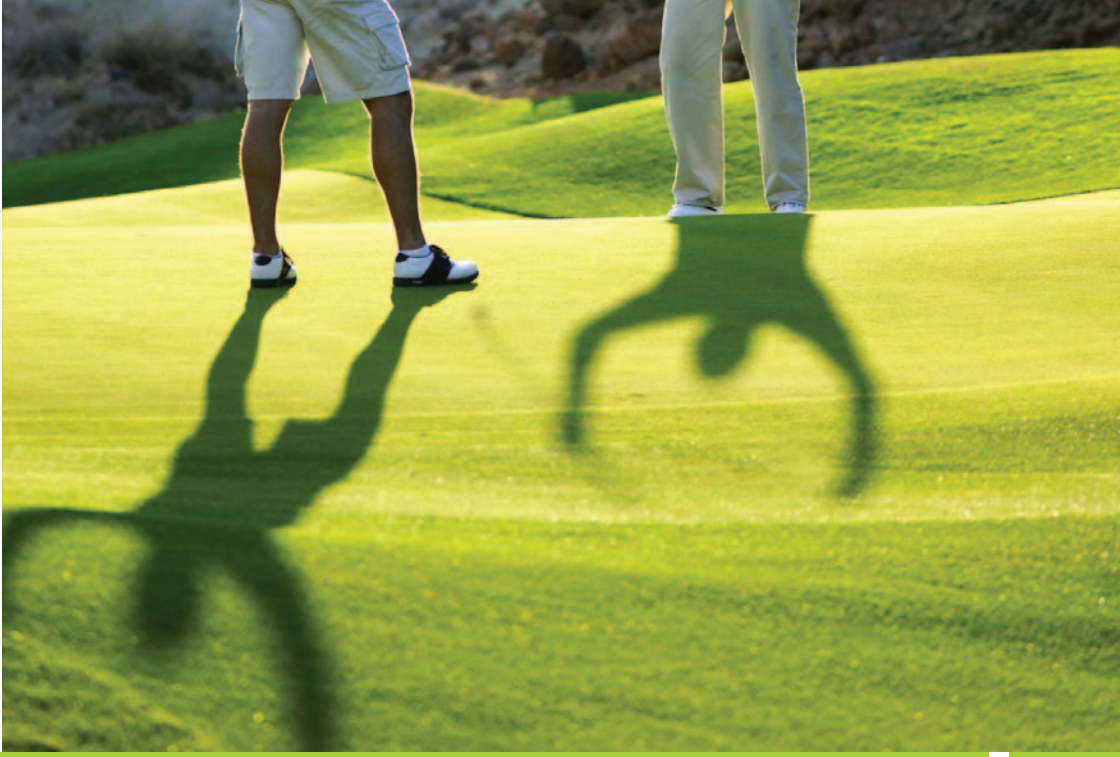
EXAMPLE

Being assailed with junk mail, you can require the business stores and commercial companies to stop sending this mail.

It turns out that the company sending the personalised mailings is sponsor to your sports club from whom it received your address as well as the database of all the club members. The club should not have communicated its file of recordings concerning its members as the information contained is only meant to be used to manage the club and organise its activities.

This unlawful misuse of the purpose for which the personal data was given is a breach of data protection law as well as an offence that is subject to punishment.

YOUR RIGHTS AS A CITIZEN



The law on the protection of personal data aims to ensure transparency in the processing of your personal data and encourages a certain amount of self-help from each data subject. It confers rights which allow you to personally check on what is happening to your data.

1. RIGHT TO BE INFORMED

You must be informed at the time of collection or recording of the data. The purposes for which your data is being used must be explained to you by the authority, company, association, professional or self-employed worker collecting and processing this personal data. The same applies if whoever is processing your personal data considers disclosing it to third parties.

2. RIGHT OF ACCESS

You have the right to find out what information about you is held and to obtain a copy thereof. You are entitled to have inaccurate or inadequate data rectified, blocked, erased, destroyed or deleted.

3. RIGHT TO OBJECT TO THE PROCESSING OF YOUR PERSONAL DATA

You have the right to object to the processing of your personal data for any legitimate reasons relating to your private situation.

You can request, without having to provide any justification, that your personal data be not used for direct marketing purposes or for any commercial reasons or canvassing of an ideological nature (political parties, unions, churches and religious groups, etc).

4. RIGHT TO INFORMATION ON AUTOMATED DECISION-MAKING PROCESSES

For decisions taken on the basis of automated processes (e.g. approval of an application for consumer credit or an insurance contract), you have the right to be informed about the logic governing this automated process. The organisation or company using this method must grant you the necessary safeguards so you can put forward your point of view and, if appropriate, ask for the decision to be reconsidered using a different method.

HOW AND WHEN CAN YOU **ENFORCE YOUR RIGHTS?**

1. CONSULTING THE PUBLIC REGISTER

The C.N.P.D. has set up a public register of data processing which can be accessed via the Internet [4].

This public register makes it possible to check whether a certain authority, company, association, professional or self-employed worker is likely to be holding information about you and whether it has declared such processing to the C.N.P.D. Every database and all data processing must separately be registered with, or authorised by the C.N.P.D. For example, an authorisation for use of a video surveillance system does not exempt one to register a database concerning clients.

[4] www.cnpd.lu

2. SUBMIT A REQUEST DIRECTLY TO THE DATA CONTROLLER

You can exercise your rights of access and rectification at any time by dealing directly with the relevant authority, company, association, professional or self-employed worker, when your personal information is collected, recorded, used or processed. You can ask to be informed about the purpose of the processing. Anyone who processes your data must inform you precisely of what personal information is being held so you can check its accuracy, its relevance and the necessity of keeping it, considering the purpose being pursued by the controller.

Send your request in writing, preferably by registered letter, attaching a copy of your identity card. Access to information on the processing of your personal data should be provided free of charge.

3. COMPLAIN TO THE C.N.P.D.

If a request sent directly to the relevant authority, company, association, professional or self-employed worker has had no effect, you can consider contacting the C.N.P.D.

The C.N.P.D. can consider complaints from data subjects. It can prohibit unlawful data processing operations. It can also order the destruction of data and refer offences to prosecution. Penalties can be applied if an offence has been committed.

It is strongly recommended that you submit your complaint in writing, giving a detailed explanation of the problem you have experienced.

4. GOING TO COURT

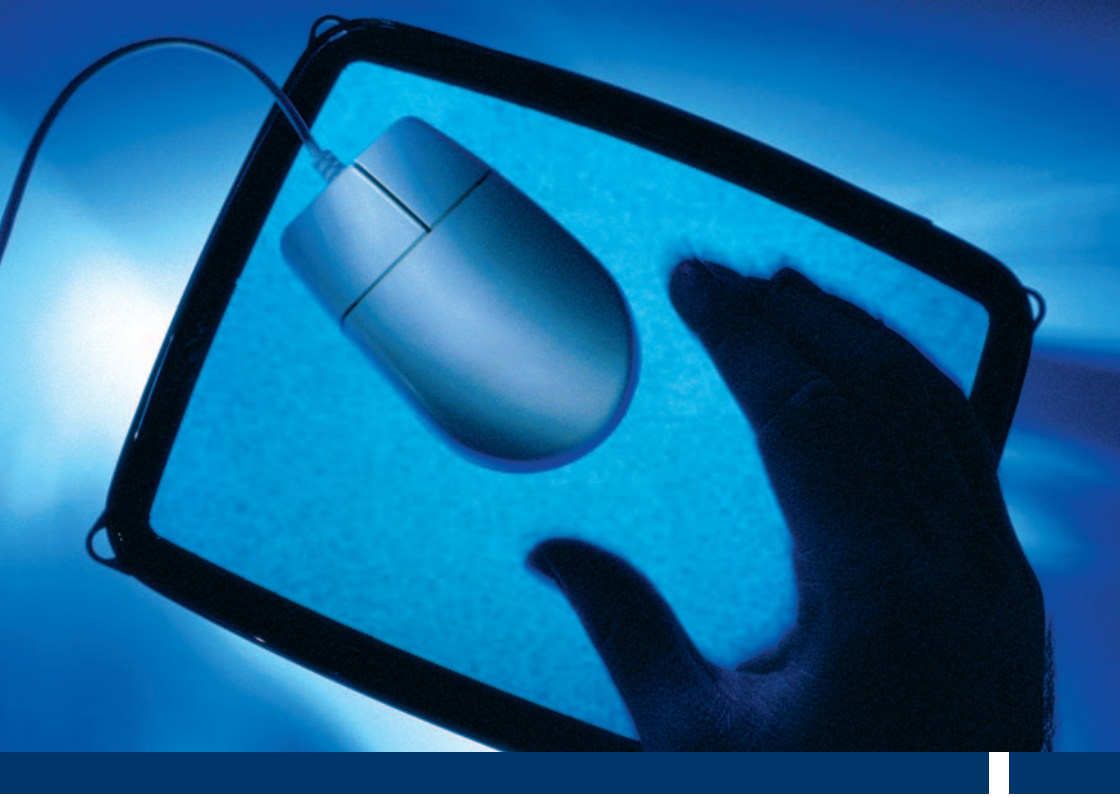
If the action taken by the C.N.P.D. does not seem to bring a satisfactory result, you still have the right to take the matter to court, in which case you will definitely need to contact a lawyer.

Legal action is also essential if you wish to claim compensation for the violation of your right to privacy and private life.

THE ROLE OF THE ***COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES***

Legislation relating to the protection of personal data aims to establish the correct balance between the information society and the protection of privacy.

If an equal balance is maintained between the interests of those who have a legitimate reason to obtain and use information about you, and your own natural expectation of being able to count on the respect of a certain anonymity and on the taking of special precautions in view of the intimate nature of certain data, this helps to establish a climate of trust between citizens and public or private persons or organisations holding such information, whether they operate in the commercial sector or not. This climate of trust also



encourages the development of economic activities involving modern technology (e-commerce), the modernisation of administration (e-government) and the free circulation of information.

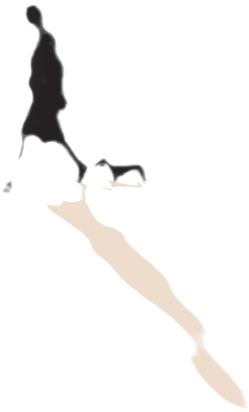
Harmonisation of national data protection legislation within the Member States is an essential step towards removing obstacles to the free circulation of data within the single market. The European Directive aims to establish, throughout Europe, the same level of protection of rights and freedoms of individuals with regard to the processing of personal data. The Directive has also lifted restrictions on the flow of personal data within the European Union, while imposing strict conditions limiting the circulation of information to countries which do not provide an adequate level of protection.

In Luxembourg, the *Commission nationale pour la protection des données* is the independent supervisory authority which upholds the rights of individuals and ensures these are respected by both private persons and public authorities.

Commission nationale
pour la protection des données

68, route de Luxembourg
L-4100 Esch-sur-Alzette
Tel: 26 10 60-1 / Fax: 26 10 60-29
info@cnpd.lu / www.cnpd.lu

DATA PROTECTION **GLOSSARY**



1. PERSONAL DATA

Any information of any kind, regardless of its form, including sound and image, relating to an identified or identifiable person. An identifiable natural person ("data subject") or legal person (company) is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, genetic, mental, cultural, social or economic identity.

2. PROCESSING OF PERSONAL DATA

Any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data.

3. PERSONAL DATA FILING SYSTEM

Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

4. CONTROLLER

The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

5. INTERCONNECTION

Any form of processing which involves connecting data processed for one purpose with data processed for identical or related purposes by one or more other controllers.

6. PURPOSE

The objective chosen before instigating the processing, which serves to determine the operations to be performed to achieve it (or try to achieve it) and to determine the data undergoing these operations. Several vague objectives may not be gathered under one purpose. Determination of the purpose or linked purposes of the processing is a key to evaluating the legitimacy of the processing.

7. DATA SUBJECT'S CONSENT

Any explicit, unequivocal, freely given, specific and informed expression of the data subject's will by which the data subject or his legal, judicial or statutory representative agrees to the personal data being processed.

EDITOR SIP **IN COLLABORATION WITH** CNPD **DATE** 08|2004 **LAYOUT** MV-CONCEPT.LU **PRINT** ?

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Service Information et Presse

33, BD ROOSEVELT L-2450 LUXEMBOURG
TEL: [+352] 478-2181 / **FAX:** [+352] 46 74 83
WWW.GOUVERNEMENT.LU

For further information, please contact:

Commission Nationale pour la Protection des Données

L-4100 ESCH-SUR-ALZETTE
TEL: [+352] 26 10 60-1 / **FAX:** [+352] 26 10 60-29
INFO@CNPD.LU / WWW.CNPD.LU