

DATA PROTECTION
IN THE
EUROPEAN UNION

TABLE OF CONTENTS

INTRODUCTION

THE EUROPEAN DIRECTIVE ON DATA PROTECTION

RULES DATA CONTROLLERS MUST ADHERE TO

YOUR RIGHTS AS A DATA SUBJECT

WHAT CAN YOU DO IF YOUR RIGHTS ARE VIOLATED

DATA TRANSFERS TO NON-EU COUNTRIES

USEFUL ADDRESSES AND NUMBERS

INTRODUCTION

Everyone has the right to respect for his private and family life, his home and his correspondence

- European Convention for the Protection of Human Rights and Fundamental freedoms

Information relating to individuals, called 'personal data', is collected and used in many aspects of everyday life. An individual gives personal data when he/she, for example, registers for a library card, signs up for gym membership, opens a bank account, etc. Personal data can be collected directly from the individual or from existing data base. These data may subsequently be used for other purposes and/or shared with other parties. Personal data can be any data that identifies an individual, such as a name, a telephone number, or a photo.

Advancement in computer technology along with new telecommunications networks is allowing personal data to travel across borders with greater ease.. As a result, data concerning the citizens of one Member State are sometimes processed in other Member States of the EU. Therefore, as personal data is collected and exchanged more frequently, regulation on data transfers becomes necessary.

In this context, national laws regarding data protection demanded good data management practices on the part of the entities who process data, called 'data controllers'. These included the obligation to process data fairly and in a secure manner and to use personal data for explicit and legitimate purposes. National laws also guaranteed a series of rights for individuals, such as the right to be informed when personal data was processed and the reason for this processing, the right to access the data and if necessary, the right to have the data amended or deleted.

Although national laws on data protection aimed to guarantee the same rights, some differences existed. These differences could create potential obstacles to the free flow of information and additional burdens for economic operators and citizens. Some of these were: the need to register or be authorised to process data by supervisory authorities in several Member States, the need to comply with different standards and the possibility to be restricted from transferring data to other Member States of the EU. Additionally, some Member States did not have laws on data protection.

For these reasons, there was a need for action at European level, and this took the form of EC Directives.

THE EUROPEAN LEGISLATION ON DATA PROTECTION

In order to remove the obstacles to the free movement of data without diminishing the protection of personal data, Directive 95/46/EC (the data protection Directive) was developed to harmonise national provisions in this field.

As a result, the personal data of all citizens will have equivalent protection across the Union. The fifteen Member States of the EU were required to bring their national legislation in line with the provisions of the Directive by 24th October 1998.

A Directive is a piece of European legislation which is addressed to Member States. Once such legislation is passed at the European level, each Member State must ensure that it is effectively applied in their legal system. The Directive prescribes an end result. The form and methods of the application is a matter for each Member State to decide for itself. In principle, a Directive takes effect through national implementing measures (national legislation). However, it is possible that even where a Member State has not yet implemented a Directive some of its provisions could have direct effect. This means that if a Directive confers direct rights to individuals, then individuals could rely on the directive before a judge without having to wait for national legislation to implement it. Furthermore, if the individuals feel that losses have been incurred because national authorities failed to implement directive correctly, then they may be able to sue for damages. Such damages can only be obtained in national courts.

The data protection Directive applies to 'any operation or set of operations which is performed upon personal data,' called 'processing' of data. Such operations include the collection of personal data, its storage, disclosure, etc. The Directive applies to data processed by automated means (e.g. a computer database of customers) and to data that are part of or intended to be part of non automated 'filing systems' in which they are accessible according to specific criteria. (For example, the traditional paper files, such as a card file with details of clients ordered according to the alphabetic order of the names).

The data protection Directive does not apply to data processed for purely personal reasons or household activities (e.g. an electronic personal diary or a file with details of family and friends).

It also does not apply to areas such as public security, defence or criminal law enforcement, which are outside the competence of the EC and remain a national prerogative. National legislation generally provides protection for individuals in these areas.

In addition, there is a separate Directive, Directive 97/66/EC, that deals specifically with the protection of privacy in telecommunications. This Directive states that Member States must guarantee the confidentiality of communication through national regulations. This means that any unauthorised listening, tapping, storage or other kinds of interception or surveillance of communications is illegal. Where calling-line identification is offered, users must be given the possibility to not subscribe to this service or not having their identification revealed when making a telephone call. Conversely, subscribers to this service must have the possibility to reject incoming calls from individuals who have blocked their calling-line identification. Additionally, the Directive states that where printed or electronic telecommunication directories exist, individuals are entitled to omission from the list, in principle, at no cost.

**WHO CAN BE A DATA SUBJECT?
WE ARE ALL DATA SUBJECTS.**

**WHENEVER YOU BOOK A FLIGHT, APPLY FOR A JOB,
USE A CREDIT CARD, OR BROWSE ON THE INTERNET,
-- YOU DISCLOSE SOME PERSONAL DATA.**

RULES DATA CONTROLLERS MUST ADHERE TO

Who can be a data controller?

Data controllers are the people or body, 'which determines the purposes and the means of the processing,' both in the public and in the private sector. A medical practitioner would usually be the controller of the data processed on his clients; a company would be the controller of the data processed on its clients and employees; a sports club would control the data processed on its members and a public library controls the data processed on its users.

Data controllers are required to observe several principles. These principles not only aim to protect the data subjects but also are a statement of good business practices that contribute to reliable and efficient data processing.

Each data controller must adhere to the data processing rules of the Member State where he or she is established even if the data processed belongs to an individual residing in another State. When the data controller is not established in the Community (e.g. a foreign company), he or she has to comply with the laws of the Member State(s) if the processing equipment (e.g. a computing centre) is located within the European Community.

THE RULES ARE:

- Data must be processed fairly and lawfully.
- They must be collected for explicit and legitimate purposes and used accordingly.
- Data must be relevant and not excessive in relation to the purpose for which they are processed.
- Data must be accurate and where necessary, kept up to date.
- Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them.
- Data that identifies individuals must not be kept longer than necessary.
- The Directive states that each Member State must provide one or more supervisory authorities to monitor the application of the Directive. One responsibility of the supervisory authority is to maintain an updated public register so that the general public has access to the names of all data controllers and the type of processing they do.
- In principle, all data controllers must notify supervisory authorities when they process data. Member States may provide for simplification or exemption from notification for specific types of processing which do not entail particular risks. Exception and simplification can also be granted when, in conformity with national law, an independent officer in charge of data protection has been appointed by the controller.

Member States may require prior checking, to be carried out by the supervisory authority, before data processing operations that involve particular risks may be undertaken. Which types of processing operations involve particular risks is for the member states to determine.

When can personal data be processed?

Personal data can only be processed (e.g. collected and further used) if:

- * The data subject has unambiguously given his or her consent, i.e. if he or she has agreed freely and specifically after being adequately informed;
- * Data processing is necessary for the performance of a contract involving the data subject or in order to enter into a contract requested by the data subject, e.g. processing of data for billing purposes or processing of data relating to an applicant for a job or for a loan;
- * Processing is required by a legal obligation;
- * Processing of data is necessary to protect an interest that is essential for the data subject's life. An example is in the case of a car accident and the data subject is unconscious, emergency paramedics are allowed to give blood tests if it is deemed essential to save the data subject's life;
- * Processing is necessary to perform tasks of public interests or tasks carried out by official authorities (such as the government, the tax authorities, the police etc.);
- * Finally data can be processed whenever the controller or a third party has a legitimate interest in doing so. However, this interest cannot override the interests **or** fundamental rights of the data subject, particularly the right to privacy. This provision establishes the need to strike a reasonable balance, in practice, between the business interest of the data controllers and the privacy of data subjects. This balance is first evaluated by the data controllers under the supervision of the data protection authorities, although if required, the courts have the final decision.

Sensitive data

Very stringent rules apply to processing sensitive data: data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs trade union membership, data concerning health or sexual preference. In principle, such data cannot be processed. Derogation is tolerated under very specific circumstances. These circumstances include the data subject's explicit consent to process sensitive data, the processing of data mandated by employment law, where it may be impossible for the data subject to consent (e.g. blood test to the victim of a road accident), processing of data has been publicly announced by the data subject or processing of data about members by trade unions, political parties or churches. Member states may provide for additional exceptions for reasons of substantial public interest.

Does the Directive Apply to Data Transfers on the Internet?

It would be rather illogical and without legal justification to exempt such an important means of transfer as the Internet from the scope of the data protection Directive. On the contrary, the sheer volume and multiple nature of personal data transmitted through the Internet all over the world, including to countries with no adequate protection, require particular attention. The data protection Directive is therefore technologically neutral: its provisions apply, irrespective of the technological means used to process personal data. For example, the Directive applies to the invisible collection of personal data on the Internet (e.g.: the "cookies" which are used to track the individual surfing habits). On the other hand, if personal data are collected in a "visible" way, it might be argued that an individual transferring his own data has given his consent to such a transfer, provided that he is properly informed about the risks involved.

- | |
|---|
| <p>Q. An individual continually receives unsolicited e-mails. How can this be prevented, as these e-mails come from many sources?</p> <p>A. The individual has the right to object to the processing of his/her data for the purposes of direct marketing. In addition, the individual could request her internet service provider to install mail filters or contact one of the associations devoted to preventing junk e-mail (CAUCE, Privacy International, etc.). Other services exist to assist individuals to prevent junk e-mail, such as www.spamfree.org. If the problem persists, the individual can write to her/his national supervisory authority.</p> |
|---|

YOUR RIGHTS AS A DATA SUBJECT

You have the right to be informed of any data processing when you are the data subject.

Data controllers are required to inform you whenever they collect personal data concerning you, unless you have previously been informed. You have the right to be informed of: the identity of the controller, the purposes for the processing and any further information such as the recipients of the data and the specific rights that you, as data subject, are entitled to. You have the right to receive this information whether the data was obtained directly from or indirectly from third parties. Derogation may be allowed in the latter case if giving this information proves impossible or extremely difficult, or if its required by law.

You have the right of access data about you.

You are entitled to approach any data controller to know whether or not he is processing personal data that concern you, to receive a copy of the data in an intelligible form and to be given any available information about their sources. If the personal data are inaccurate, or if they were unlawfully processed, you are entitled to ask for the correction, block or erasure of the data. In such cases, the data subject may also require the data controller to notify third parties who had previously seen the incorrect data, unless this proves impossible. A reasonable fee for providing access may be charged in some cases.

You must also have access to the logic on which automated decisions are based.

Decisions, which significantly affect the data subject, such as the decision to grant a loan or issue insurance, might be taken on the sole basis of automated data processing. Therefore, the data controller must adopt suitable safeguards, such as giving the data subject the opportunity to discuss the rationale behind the data collected or to contest decisions based on inaccurate data.

Exceptions and limitations

The right to privacy may sometimes conflict with freedom of expression and in particular, freedom of the press and media. It is therefore up to the Member States to establish exceptions in their data protection laws in order to strike a balance between these different but equally fundamental rights.

National law might allow other exceptions to provisions of the Directive. (These include the obligation to inform the data subject; the publicising of data processing operations; the obligation to respect the basic principles of good data management practice.) Such exceptions are permitted if, among other things, it is necessary on grounds of national security, defence, crime detection, enforcement of criminal law, or to protect data subjects or the rights and freedom of others. Additionally, derogation from the right to access data may be granted for data processed for scientific or statistical purposes.

WHAT CAN YOU DO IF YOUR RIGHTS ARE VIOLATED?

Your first step, if you fear that your rights have been violated, is to contact the person who appears to be the source of the violation in order to find out who the Data Controller is. If you don't get a satisfactory result from this, you could contact your national data protection authority. According to the Directive, each Member State must provide one or more public authorities to ensure the proper application of the data protection law. This authority, often referred to as the supervisory authority, is competent to hear complaints lodged by any person or business. The supervisory authority must investigate the claim and may temporarily ban the processing. If the supervisory authority finds that the data protection law has been violated, then the supervisory authority could, among other things, order the erasure or destruction of the data and/or ban further processing.

Q. A telecommunications provider gave information about your telephone or e-mail account to another company. As a result, you receive unsolicited calls or e-mails. . What can you do ?

A. If personal data was collected for billing purposes only, and you did not consent to further transfer of your data, then you are entitled to object to the transfer of your data to any third parties. The first step should be to write to your provider, clearly stating your complaint. If you receive no satisfactory answer, then you should contact the national supervisory authority.

Q. You are denied a loan because of inaccuracies in a bank's file. You made an access request to your bank in order to know what information was recorded on the bank's computer about your credit record. However, the bank failed to respond to your access request. You made several telephone calls to the bank regarding this request but to no avail. What should you do next?

A. The Directive states that you have the right to obtain access "without excessive delay" to any personal data held about you. If the data are inaccurate, you have the right to rectify them. Therefore, if you do not receive an answer from the bank within reasonable time, you can complain directly to the national supervisory authority. According to the Directive, the national supervisory authority must investigate the claim and inform the complainant of the outcome.

To contact the supervisory authority, you should (preferably in writing) describe the problem and submit enough information so that the problem is well described. In some member states, the supervisory authority has standardised forms that you can fill out to make a complaint. If this is available, then you should use these forms because this will speed up the handling of your case and you will receive an answer more quickly. In some member states complaints may be submitted by e-mail. In others this is not yet possible.

If this doesn't lead to a satisfactory result, you may need to go to court. If this were the case, it would be a good idea to seek legal advice. Going to court may also be necessary if you have suffered damages because of the violation to your rights. You may be entitled to compensation.

Q. Your employer has shared your medical file with your bank without seeking your consent. The medical file included information, the content of which may explain why your bank is refusing to allow you a mortgage credit. Are you entitled to compensation?

A. You are entitled to compensation if you suffer damage as a result of the unlawful disclosure of your personal data. This may be the case if your medical data have been shared without your consent.

Any person or business may lodge a complaint with the Commission about an alleged violation of Community law by a Member State.

The European Commission is responsible for ensuring that Community law is applied properly in the Member States. If necessary, the Commission reminds Member States of their responsibilities for implementing Community law on time and for enforcing it properly. In some cases, if a Member State fails to fulfil these obligations, the Commission may need to initiate proceedings before the European Court of Justice, which decides whether or not Community law has been infringed.

You will not have to prove that you are directly affected by the infringement that you allege.

However, disputes between private parties cannot be settled by the Commission in this context.

You will not be charged for making a complaint and you do not have to seek the assistance of a lawyer. Remember to include relevant information and documentation (e.g. relevant national rules) when making your complaint.

You can complain to the Commission by writing to:

Commission of the European Communities (for the attention of the Secretary-General), Rue de la Loi 200, B- 1049 Brussels.

or by using the standard complaint form available on request from the Commission's offices in the Member States and from the Internet at <http://europa.eu.int/comm/sg/lexcomm>

DATA TRANSFERS TO NON-EU COUNTRIES

In cases of transfer of data to countries that are not members of the European Union, it may be necessary to take special precautions if the level of data protection in the third country is inconsistent with that provided by European Law. Without such rules, the high standards of data protection established by the Directive would quickly be undermined, given the ease with which data can be moved around in international networks.

The principle of the Directive is that personal data can only be transferred to countries outside the EU that guarantee an “adequate” level of protection. Analysis of data protection laws and dialogues with the EU’s more important trading partners is underway in order to decide which countries can be seen as offering adequate protection.

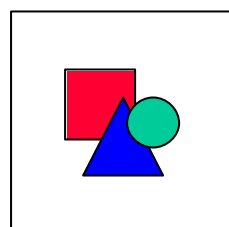
Where a non-EU country does not ensure an adequate level of protection, the Directive requires the blocking of specific transfers. Member States must inform the Commission of any such blocking measures, and this triggers a Community procedure to ensure that any Member State’s decision to block a particular transfer is either extended to the EU as a whole, or reversed.

What could non-EU Country Companies Do?

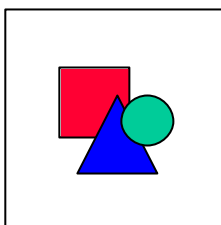
Blocking transfers of personal data is a solution of last resort. There are other ways to ensure that data continues to be adequately protected without causing disruption to international data flows and commercial transactions that the data is associated to. If EU firms are uncertain as to whether legislation or self-regulatory systems in a non-EU country provide adequate protection, they would be well advised to supply that protection themselves. This could be done by means of a contract between the company sending the data and the non-EU company receiving the data. The object of such a contract would be to provide for adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. Then, there should be no reason for an EU member state to block any transfer of data relating to its citizens.

USEFUL ADDRESSES AND NUMBERS

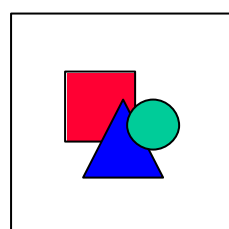
NATIONAL OFFICES OF THE DATA PROTECTION COMMISSIONERS



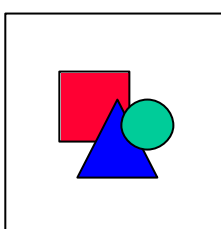
Austria:
 Österreichische
 Datenschutzkommission
 Ballhausplatz, 1
 A - 1014 WIEN
 Tel: +43/1/531.15.26.79
 Fax: +43/1/531 15 26 90
No web site



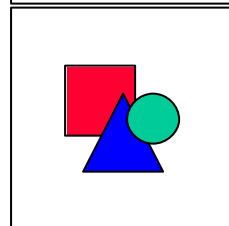
Belgium:
 Commission de la protection de la vie privée
 Adresse postale: Ministère de la Justice
 Bd. De Waterloo, 115
 B - 1000 BRUXELLES Bureaux:
 Avenue de la Porte de Hall, 5-8
 B - 1060 BRUXELLES
 Tel: +32 (0)2/542.72.00
 Fax: +32 (0)2/542.72.12
E-mail: privacy@euronet.be
<http://www.privacy.fgov.be/>



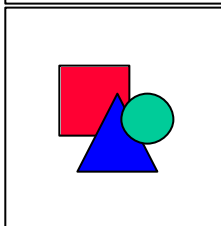
Denmark:
 Datatilsynet
 Christians Brygge, 28 - 4
 DK-1559 KØBENHAVN V
 Tel: + 45/33.14.38.44
<http://www.datatilsynet.dk/>
dt@datatilsynet.dk



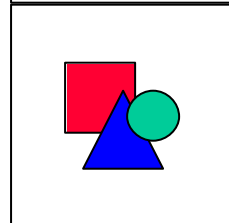
Finland:
 Office of the Data Protection Ombudsman
 P.O. Box 315
 FIN-00181 Helsinki
 Tel: +358/9/18251
<http://www.tietosuoja.fi/>



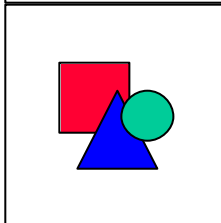
France:
 Commission Nationale de
 l'Informatique et des Libertés
 Rue Saint Guillaume, 21
 F - 75340 PARIS CEDEX 7
 Tel: +33/1/53.73.22.22
<http://www.cnil.fr/>



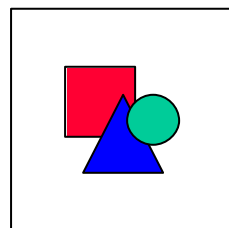
Germany:
 Der Bundesbeauftragte für den Datenschutz
 Postfach 20 01 12
 D - 53131 BONN (Bad Godesberg)
 Tel: +49/228/819.95.0
<http://www.bfd.bund.de/>



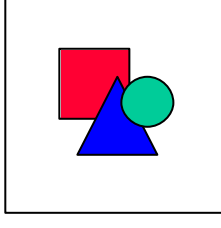
Greece:
 Hellenic Data Protection Authority
 8 Omirou Street
 10564 Athens, Greece
 Tel: +301/33.52.604-5
 Fax: +301/33.52.617
<http://www.dpa.gr>
contact@dpa.gr



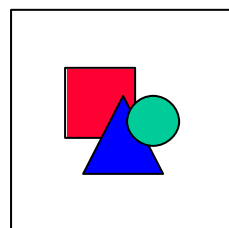
Ireland:
 Data Protection Commissioner
 Irish Life Centre, Block 4
 Talbot Street
 Dublin 1 - IRL
 Tel: +353/1/874.85.44
No web site



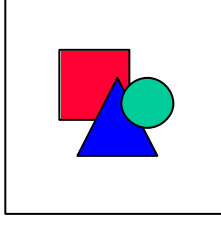
Italy:
 Garante per la protezione dei dati
 personali
 Largo del Teatro Valle, 6
 I - 00186 ROMA
 Tel: +39/06/68.18.61
No web site



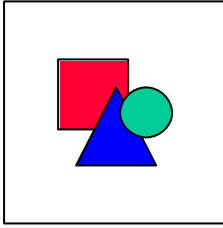
Luxembourg:
 Commission à la Protection des Données
 Nominatives
 Ministère de la Justice
 Boulevard Royal, 15
 L - 2934 LUXEMBOURG
 Tel: +352/478.45.46
No web site



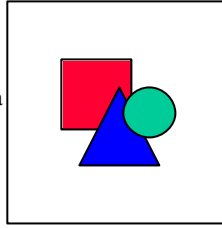
Netherlands:
 College Bescherming Persoonsgegevens
 Prins Clauslaan 20
 Postbus 93374
 NL - 2509 AJ 's-GRAVENHAGE
 Tel: +31/70/381.13.00
<http://www.cbppweb.nl/>



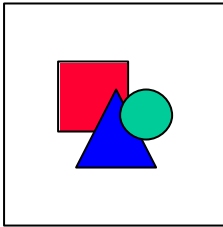
Portugal:
 Comissão Nacional de Protecção de Dados
 Pessoais Informatizados
 R. de S. Bento, 148 - 3º
 P - 1200-821 LISBOA
 Tel: +(351) 21.392 84 00
<http://www.cnpd.pt>



Spain:
Agencia de Protección de Datos
Paseo de la Castellana, N 41, 5a planta
E - 28046 MADRID
Tel: +34/91/308.40.17
<http://www.ag-protecciondatos.es/>



Sweden:
Datainspektionen
Fleminggatan, 14
9th Floor
Box 8114
S - 104 20 STOCKHOLM
Tel: +46/8/657.61.00
<http://www.datainspektionen.se/>



United Kingdom:
Data Protection Commissioner
Water Lane
Wycliffe House
UK – WILMSLOW - CHESHIRE
SK9 5AF
Tel: +44/1625/54.57.45
<http://www.dataprotection.gov.uk>

k

EFTA Countries

Iceland:
Ministry of Justice Data Protection Commission
Arnarhvoll
IS – 150 REYKJAVIK
Tel: +354/560.90.10
No web site

Norway:
Datatilsynet
The Data Inspectorate
P.B. 8177 Dep
N – 0034 OSLO
Tel: +47/22/42.19.10
<http://www.datatilsynet.no/>

EUROPEAN COMMISSION OFFICES IN THE UK

Jean Monnet House, 8 Storey's Gate, London SW1P 3AT
Tel: +44 (0)171 973 1992
<http://www.cec.org.uk>

4 Cathedral Road, Cardiff CF1 9SG
Tel: +44(0)1222 371631

9 Alva Street, Edinburgh EH2 4PH
Tel: +44(0)131 225 2058

Windsor House, 9/15 Bedford Street, Belfast BT2 7EG
Tel: +44(0)1232 240708

http://europa.eu.int/comm/represent_en.htm

NATIONAL SINGLE MARKET CONTACT POINTS

For citizens and businesses:

Julie Evans
Single Market Unit
Department of Trade and Industry
Bay 208 - Kingsgate House
London SW1E 6SW
Tel: (+44) (0) 171 215 44 90
Fax: (+44) (0) 171 215 47 20
E-mail: julie.evans@eirv.dti.gov.uk

DIALOGUE WITH CITIZENS AND BUSINESS

Europe Direct free phone number : 0800 581 591

Internet: <http://europa.eu.int/citizens>
<http://europa.eu.int/business>

By dialling this number, or through the websites, you can also put questions to the ‘Signpost Service’, which helps you to overcome practical problems in exercising your rights. Your question will be answered within three working days and you will be advised on the next step to take in terms of contacting the most appropriate body which can provide further help at an EU, national or local level.