Protection of personal data

Directive 95/46/EC is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision ofany activity linked to the processing of personal data.

ACT

European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Official Journal L 281 of 23.11.1995] [See amending acts].

SUMMARY

This Directive applies to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non automated filing systems (traditional paper files).

It does not apply to the processing of data:

- by a natural person in the course of purely personal or household activities;
- in the course of an activity which falls outside the scope of Community law, such as operations concerning public security, defence or State security.

The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down the key criteria for making processing lawful and the principles of data quality.

Data processing is only **lawful** if

- the data subject has unambiguously given his consent; or
- processing is necessary for the performance of a contract to which the data subject is party; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or
- processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

The **principles of data quality**, which must be implemented for all lawful data processing activities, are the following:

— personal data must be processed **fairly and lawfully**, and collected for specified, explicit and legitimate purposes. They must also be adequate, relevant and not excessive, accurate and, where necessary, kept up to date, must not be stored for longer than necessary and solely for the purposes for which they were collected;

— special **categories** of processing: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis.

The person whose data are processed, the data subject, can exercise the following rights:

— **right to obtain information**: the controller must provide the data subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data etc.);

— the data subject's **right of access** to data: every data subject should have the right to obtain from the controller;

— the **right to object** to the processing of data: the data subject should have the right to object, on legitimate grounds, to the processing of data relating to him/her. He/she should also have the right to object, on request and free of charge, to the processing of personal data that the controller anticipates being processed for the purposes of direct marketing. He/she should finally be informed before personal data are disclosed to third parties for the purposes of direct marketing, and be expressly offered the right to object to such disclosures;

Other relevant aspects for data processing:

— **exemptions and restrictions from data subject's rights**: the scope of the principles relating to the quality of the data, information to be given to the data subject, right of access and the publicising of processing may be restricted in order to safeguard aspects such as national security, defence, public security, the prosecution of criminal offences, an important economic or financial interest of a Member State or of the European Union or the protection of the data subject;

— **the confidentiality and security of processing**: any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller. In addition, the controller must implement appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access;

— the **notification** of processing to a supervisory authority: the controller must notify the national supervisory authority before carrying out any processing operation. Prior checks to determine specific risks to the rights and freedoms of data subjects are to be carried out by the supervisory authority following receipt of the notification. Measures are to be taken to ensure that processing operations are publicised and the supervisory authorities must keep a register of the processing operations notified.

Every person shall have the right to a **judicial remedy** for any breach of the rights guaranteed by national law applicable to the processing in question. In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered.

Transfers of personal data from a Member State **to a third country** with an adequate level of protection are authorised. However, although transfers may not take place when an adequate level of protection is not guaranteed, there are a number of exceptions to this rule listed in the Directive, e.g. the data subject himself

agrees to the transfer, in the event of the conclusion of a contract, it is necessary for public interest grounds, but also if Binding Corporate Rules or Standard Contractual Clauses have been authorised by the Member State.

The Directive aims to encourage the drawing up of national and Community codes of conduct intended to contribute to the proper implementation of the national and Community provisions.

Each Member State is to provide one or more independent public authorities responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to the Directive.

A Working Party on the Protection of Individuals with regard to the Processing of Personal Data is set up, composed of representatives of the national supervisory authorities, representatives of the supervisory authorities of the Community institutions and bodies, and a representative of the Commission.

REFERENCES

Act	Entry into force	Deadline for transposition in the Member States	Official Journal
Directive 95/46/EC	13.12.1995	24.10.1998	OJ L 281 of 23.11.1995
Amending act(s)	**Entry into force**	**Deadline for transposition in the Member States**	**Official Journal**
Regulation (EC) No 1882/2003	20.11.2003	-	OJ L 284 of 31.10.2003

Successive amendments and corrections to Directive 95/46/EC have been incorporated in the basic text. This consolidated version is for reference purpose only.

RELATED ACTS

IMPLEMENTATION REPORT

Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive [COM(2007) 87 final - Not published in the Official Journal].

This Communication examined the work done under the Work Programme for improved implementation of the Directive on data protection contained in the First report on the implementation of Directive 95/46/EC. The Commission highlighted improvements in that all Member States have transposed the Directive. It emphasised that the Directive should not undergo any amendments.

It also noted that:

- it will continue in its cooperation with the Member States and, if necessary, will launch official infringement proceedings;
- it will prepare an interpretative communication regarding certain provisions in the Directive;
- it will continue its implementation of the Work Programme
- it will present EU-level sectoral legislation if there are major technological developments in a specific area;
- it will continue cooperating with its external partners, in particular the US.

Report from the Commission of 15 May 2003 [COM(2003) 265 final - Not published in the Official Journal] First report on the implementation of the Data Protection Directive (95/46/EC)

The report took stock of the consultations carried out by the Commission to evaluate Directive 95/46/EC with governments, institutions, business and consumer associations, and individual citizens. The results of the consultations showed that few contributors advocated a revision of the Directive. Furthermore, after consulting the Member States, the Commission noted the fact that a majority of them and, also, of the national supervisory authorities, did not consider it necessary to amend the Directive at present.

Despite the delays and gaps in implementation, the Directive has fulfilled its principal objective of removing barriers to the free movement of personal data between the Member States. The Commission also believed that the objective of ensuring a high level of protection in the Community has been achieved since the Directive has set out some of the highest standards of data protection in the world.

Other Internal Market policy objectives have, however, been less well served. The divergences in data protection legislation are still too great between Member States, and these disparities prevent multinational organisations from developing pan-European policies on data protection. The Commission announced therefore that it would do what is required to remedy this situation whilst hoping, wherever possible, that it will not be necessary to proceed by way of formal action.

With regard to the general level of compliance with data protection law in the EU, there are three main problems:

— an under-resourced enforcement effort;

— very patchy compliance by data controllers;

— an apparently low level of knowledge of their rights among data subjects, which may be at the root of the previous phenomenon.

In order to ensure the better implementation of the Data Protection Directive, the Commission has adopted a work programme comprising a number of actions which need to be taken between the adoption of this report and the end of 2004. These actions are made up of the following initiatives:

— discussions with Member States and data protection authorities on the changes needed to bring national legislation fully in line with the requirements of the Directive;

— association of the candidate countries with efforts to achieve a better and more uniform implementation of the Directive;

— improving the notification of all legal acts transposing the Directive;

— simplification of the conditions for international transfers of data;

— promotion of privacy enhancing technologies;

— promotion of self-regulation and European Codes of Conducts.

PRIVACY AND ELECTRONIC COMMUNICATIONS DIRECTIVE

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Official Journal L 201 of 31.07.2002]

This Directive was adopted in 2002 at the same time as a new legislative framework designed to regulate the electronic communications sector. It contains provisions on a number of more or less sensitive topics, such as the

Member States keeping connection data for the purposes of police surveillance (the retention of data), the sending of unsolicited e-mail, the use of cookies and the inclusion of personal data in public directories.

Regulation (EU) No 611/2013 contains rules on the **notification of personal data breaches** by providers of publicly available electronic communications services in the event that their customers' personal data are lost, stolen or otherwise compromised.

Where a **personal data breach** occurs and personal data are compromised, providers are required by Directive 2002/58/EC to notify the competent national data protection authority (DPA) and also, in certain cases, the affected subscribers and individuals about the breach. Regulation (EU) 611/2013 introduces 'technical implementing measures' to clarify how these obligations should be met.

Among other things, providers should:

— inform the relevant DPA of the incident within 24 hours after detection of the breach, in order to maximise its confinement;

— take into account the type of data compromised when assessing whether to notify subscribers and individuals, e.g. where the data concerns financial information, email data, internet log files, web browsing histories, etc.;

— provide to the DPA and/or relevant subscribers or individuals the details of the incident, the type of data involved, and the measures taken to remedy the issue.

STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [Official Journal L 385 of 29.12.2004]

The European Commission has approved new standard contractual clauses which businesses can use to ensure adequate safeguards when personal data are transferred from the EU to third countries. These new clauses will be added to those which already exist under the Commission Decision of June 2001 (see below).

Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC [Official Journal L 181 of 04.07.2001]

This Decision sets out standard contractual clauses to ensure an adequate level of protection of personal data transferred from the EU to third countries. The Decision requires Member States to recognise that companies or bodies which use these standard clauses in contracts relating to the transfer of personal data to third countries ensure an 'adequate level of protection' of the data.

Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [Official Journal L 39 of 12.02.2010]

Commission Decisions attesting to the adequate level of protection of personal data to a number of third countries on the basis of Art. 25 (6): the Commission has so far recognized Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and the US Department of Commerce's Safe Harbour Privacy Principles as providing adequate protection.

PROTECTION OF DATA BY THE COMMUNITY INSTITUTIONS AND BODIES

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions

and bodies and on the free movement of such data [Official Journal L8 of 12.01.2001].

This Regulation aims at ensuring the protection of personal data within the institutions and bodies of the European Union. To this end:

- it includes provisions which guarantee a high level of protection of personal data processed by the Community institutions and bodies; and
- it provides for the establishment of an independent supervisory body to monitor the application of these provisions.

last update 08.03.2014