LEGAL PROTECTION OF PERSONAL DATA

Etienne WERY
Associé
Avocat au Barreau de Bruxelles
Avocat au Barreau de Paris (toque R 296)
etienne.wery@ulys.net

O. Ref. : 12/00146
Y. Ref. :

Date
26/01/2015

Legal framework

On the 25th of October 1995, the Directive 95/46/EC was adopted to harmonize the rules of data protection throughout the territory of the European Union. It describes the general system of protection of personal data and is the main European standard for the protection of personal data.

Two other main Directives regulate data protection in the EU:

- Directive 2002/58/EC, amended by the Directive 2009/136/EC concerning the processing of personal data and protection of privacy in the electronic communications sector.
- Directive 2006/24/EC on the retention of data generated of processed in connection with the provision of publicly available electronic communications services or of public communications networks.

In the Lindqvist case, the Court has ruled that the objective of the Directive is to maintain a balance between freedom of movement of personal data and the protection of private life.

BRUSSELS

224, av. de la Couronne
1050 Brussels
Tel. + 32 (0)2 340 88 10
Fax + 32 (0)2 345 35 80

Société civile à forme de SCRL
RPM Bruxelles
VAT : BE 0476.702.936

PARIS (succursale)

33, rue Galilée
75116 Paris
Tel. + 33 (0)1 40 70 90 11
Fax + 33 (0)1 40 70 01 38

In January 2012, the Commission considered it was time to give it an update and released a proposal of regulation which will replace the Directive 95/46. It is highly probable that the legal framework shall be substantially modified in the near future.

Supervisory authorities

Each Member State must provide that an independent administration monitors the application of the provisions of the Directive on its territory (art. 28 of the Directive 95/46). Those authorities must be independent as underlined by the Court in the C-614/10 case : "by failing to take all of the measures necessary to ensure that the legislation in force in Austria meets the requirement of independence with regard to the Datenschutzkommission (Data Protection Commission), (…) the Republic of Austria has failed to fulfil its obligations (…)". In the C-518/07 case, the court has ruled that, by making the authorities responsible for monitoring the processing of personal data by non-public bodies and undertakings governed by public law which compete on the market (öffentlich-rechtliche Wettbewerbsunternehmen) in the different Länder subject to State scrutiny, and by thus incorrectly transposing the requirement that those authorities perform their functions "with complete independence", the Federal Republic of Germany failed to fulfil its obligations.

The European Data Protection Supervisor (EDPS) is an independent supervisory authority charged with supervising the EU institutions on the application of data protection rules. It only has an advisory role on EU policies and legislation that affect privacy.

The Directive 95/46 provides at his article 29 that a Working party, the so-called "Article 29 Working Party" (or "29WP") should be in charge of the protection of individuals with regard to the processing of personal data. It is an EU-wide advisory body that is composed of a representative of each member state, the EDPS and the European Commission. His main tasks are the followings:

- Examining the national applications of legislation pursuant to EU data protection regulation;
- Issuing opinions and recommendations on the interpretation of core notions in data protection regulation and;
- Enhancing cooperation between national data protection authorities in the interest of joint procedures and enforcement actions.

The importance of the documents published by 29WP should not be underestimated. On the one hand, the fact that 29WP is interested in a subject means that there is a consensus among the authorities to consider this issue as an important one. On the other hand, since each national authority is a

members of this group, one can assess that the interpretation of the group will be reflected in national jurisprudence.

Definitions

Article 2 of the Directive 95/46 gives some key definitions about the main terms used to regulate the personal data legal framework.

- Personal data : "mean any information relating to an identified or identifiable natural person ("data object"); an identifiable person 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, mental, economic, cultural or social identity."

- Processing of personal data : "mean any operation or set or operations which is performed upon personal data, whether or not by automatic means."

- Controller : "mean 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."

In the Lindqvist case, the Court has ruled that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes "the processing of personal data wholly or partly by automatic means".

In the Tietosuojavaltuutettu case, it has ruled that an activity in which data on the earned and unearned income and the assets of natural persons are: (a) collected from documents in the public domain held by the tax authorities and processed for publication, (b) published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists, (c) transferred onward on CD-ROM to be used for commercial purposes, and (d) processed for the purposes of a text-messaging service whereby mobile telephone users can, by sending a text message containing details of an individual's name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person, must be considered as the "processing of personal data".

In the Worten case, it has ruled that a record of working time, such as that at issue in the main proceedings, which indicates, in relation to each worker, the times when working hours begin and end, as well as the corresponding breaks and intervals, is included within the concept of 'personal data'.

Main principles

Data must be:

a) processed fairly and lawfully;

b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

In addition, there must be a good cause for processing the data. The accepted good causes (this is a closed list) are :

a) the data subject has unambiguously given his consent; or

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

d) processing is necessary in order to protect the vital interests of the data subject; or

e) 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 to whom the data are disclosed; or

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) of the Directive (said article refers to the fundamental rights and freedoms of natu-

ral persons, and in particular their right to privacy with respect to the processing of personal data).

In some situations, the list of good causes is restricted. This is notably the case for the processing of 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.

As regards f) here above, the court has ruled, in the ASNEF case, that it (i) has a direct effect[1] and (ii) it must be interpreted as precluding national rules which, in the absence of the data subject's consent, require not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.

Finally the process of personal data is given in principle (there are exceptions, from country to country) prior declaration to the national authority. It means at least two things :

- a mere declaration is not a permission and the authority will not grant any sort of permission (there are however exceptions in specific cases);
- It is a prior declaration, that is to say the process cannot take place before this formality has been satisfied.

Rights of the data subject

a) Right to be informed

The controller or his representative must provide a data subject from whom data relating to him are collected with at least the following information, except where he already has it:

a) the identity of the controller and of his representative, if any;

b) the purposes of the processing for which the data are intended;

c) any further information such as:

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

[1] It may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions (see the chapter on interaction between EU and national norms).

- the existence of the right of access to and the right to rectify the data concerning him,

In so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

The regime is different where the data have not been obtained from the data subject.

b) Right to access and modify the data

Anyone may ask for any information regarding his personal data, "without constraint at reasonable intervals and without excessive delay or expense" (Art 12 of the Directive) from the controller, and has the right to modify or delete erroneous information "because of the incomplete or inaccurate nature of the date".

Third parties must get a notification of any of the rectifications disclosed "unless this proves impossible or involves a disproportionate effort".

In the C-486/12 case, the Court of Justice of the European Union has ruled that this must be interpreted as not precluding the levying of fees in respect of the communication of personal data by a public authority. In addition, the Court ruled that in order to ensure that fees levied when the right to access personal data is exercised are not excessive for the purposes of that provision; the level of those fees must not exceed the cost of communicating such data.

In the C553/07 case, the Court has ruled that the right to privacy with regard to the processing of personal data and on the free movement of such data, means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorized recipients. In order to carry out the necessary checks, the data subject must have a right of access to the data relating to him which are being processed. The right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past.

c) Right to object

Anyone has the right to oppose, for legitimate reasons that his personal data being processed.

In addition, the data subject has the right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be

expressly offered the right to object free of charge to such disclosures or uses.

Security

The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Security is a main concern in the proposal for a new legal framework (see here above). The regime will probably be substantially modified in the future. It could include an obligation to notify the data subject in case of a security breach.

Exceptions

There is a set of exceptions to some of the legal requirements, including when such a restriction constitutes a necessary measures to safeguard:

a) national security;

b) defence;

c) public security;

d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

g) the protection of the data subject or of the rights and freedoms of others.

In the IPI case, the Court has ruled that Member States have no obligation, but have the option, to transpose into their national law one or more of the exceptions which it lays down to the obligation to inform data subjects of the processing of their personal data.

Journalistic activities

The Directive creates large exemptions or derogations for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

In the Tietosuojavaltuutettu case, the Court has ruled that activities involving the processing of personal data carried out "solely for journalistic purposes", within the meaning of that provision, if the sole object of those activities is the disclosure to the public of information, opinions or ideas. Whether that is the case is a matter for the national court to determine.

Transfer of data to third-countries

The transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

In the Lindqvist case, the Court has ruled that there is no " transfer [of data] to a third country" within where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.

Please refer to the next chapter for more information.