CROSS-BORDER FLOWS 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

What is a personal data?

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

- Controller : "means 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."

A person is identifiable as soon as he/she can be "identified, directly or indirectly, in particular by reference to an identification number or by one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity". Applying this criteria is far from easy; as an example, an IP address is considered by many courts (including the EU Court of justice and most Belgian case law) as a personal data, while other judges and legal systems are reluctant to go this way and try to infer from

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

the facts of the case that in a given situation, it should not be protected as a 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'.

It refers to *"any information relating to an identified or identifiable natural person"* (the so-called data subject). It is important to underline that such definition makes no difference between the professional or private life: a list of employees in a company is considered as a personal data because it relates to identified or identifiable natural persons. (Note: some EU countries – but not Belgium – have been one step further and do also protect *legal entities*).

The reason for a specific protection

The fear of European countries is that the data processor could circumvent the legal protection by, (i) either locating its activities outside the EU, or (ii) collecting data in the EU and sending it outside EU afterwards in order to process it in a more friendly location. The rules related to the applicable law are the answer to the first problem, while the protection of international data flow addresses the second issue.

The law provides that it applies in a situation where the controller is not established on the territory of the Community and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

In such circumstances, the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

There is no detailed definition of the *"equipment"* that the data controller must *"use"* on the *"territory"* in order to fall within the scope of the national law. The most delicate question is related to the collection of data related to a European data subject, on a website operated by a US company. Because the *"collection"* of such data is a *"process"* (see here above), it could mean that the national law of the data subject applies.

The so-called Group 29 (a Working-Party of all national European privacy Commissioners) has provided for additional details and made clear that examples of such equipment are personal computers, terminals and servers. When such equipment is used (for anything else than for the transit of information through the territory of the Community), the national law of the country where such equipment is used, shall apply. The same can occur when such equipment is in fact the computer of the European customer. Indeed, although the equipment should be *"used by"* the controller, *"it is not necessary that the controller exercise full control over [it]"*; neither is it needed that the controller has the ownership of the equipment. The Working-Party took the view that the necessary degree of disposal is given if *"the controller, (…) determines which data are collected, stored, transferred, altered etc., in which way and for which purpose"*.

The European directive also provides, in Recital 20, that *"the fact that the processing is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this directive; whereas in these cases, the processing should be governed by the law of the Member State, in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice"*. This is the corollary, which is necessary in order to reach the Directive's broader objective, which is *"to ensure that individuals are not deprived of the protection to which they are entitled under this Directive"*. As a consequence, one should be cautious when collecting data through a website targeting European customers, using cookies, java script, interactive banners, etc.

However the European Court of Justice has stated that "there is no 'transfer of personal data to a third country' where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which 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". (Case C-101-01, Bodil Lindqvist, ECR, 2003-Page I-12971)

Cross-border flows are forbidden

It is important to understand that in the situation described in the previous paragraph, the consequence is the fact the data subject may claim the pro-

tection of its national law and may, in most cases, claim such protection before its national judge. The situation is different with cross-border flows where the purpose is not to apply national law, but to make sure that no data is transferred outside the EU relevant country, to a recipient located in a less protective country.

The legal regime in all EU countries is harmonized in such a way that "*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*** *(...), the third country in question ensures an adequate level of protection*". (we underline) In other words, it is a "no, but" regime per default.

The Council and the European Parliament have given the Commission the power to determine, on the basis of Article 25(6) of Directive 95/46/EC whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. As of 2015, the list is limited to Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, USA (Safe Harbor - see below), and Eastern Republic of Uruguay).

Beside this list, businesses have three options to waive the prohibition: they may (i) adopt the Safe Harbor Principles system (USA), (ii) sign *ad hoc* contracts with the recipient (model clauses), or (iii) enforce binding corporate rules at a global level (BCR).

First and third solutions ensure more freedom for the processor because the latter is deemed to comply with European standards as far as privacy is concerned and is, therefore, largely in the same situation as a European business, including for the reutilization of the data. On the contrary, the second solution is easy to put in place but the processor is bound by the contract and may not do anything else than what is provided in the contract.

(Note: The Safe Harbor Principles system is specific to American businesses, while second and third solutions are opened to any data controller located outside the EU).

Exceptions to the prohibition

a) The Safe Harbor Principles

In consultation with the European Commission, the American Department of Commerce elaborated the Safe Harbor Principles, intended to facilitate the transfer of personal data from the European Union to the United States. The protection is organized around seven pillars (the principles):

a) Notice: Individuals must be informed that their data is being collected and about how it will be used.

b) Choice: Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.

c) Onward Transfer: Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.

d) Security: Reasonable efforts must be made to prevent loss of collected information.

e) Data Integrity: Data must be relevant and reliable for the purpose it was collected for.

f) Access: Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.

g) Enforcement: There must be effective means of enforcing these rules.

The way those requirements are met is largely in the hand of each company. It usually requires some organizational changes, technical means such as segregation of the data, and *ad hoc* documentation for internal and external use. A company who wants to qualify under those principles should make a statement to the American Department of Commerce in order to agree with the Principles and publicly declare that it is prepared to respect all of them (meaning, among other things, that the American Federal Trade Commission may check whether or not said company is respecting these principles). Each company must re-certify every 12 months. This can be done by a self-assessment or by a third-party assessment. There are also specific requirements in order to ensure appropriate employee training and an effective dispute mechanism.

b) *Ad hoc* contract and model clauses

The prohibition to transfer data outside the EU is waived if the sender and the recipient of the data sign an *ad hoc* contractual scheme ensuring that the fundamental principles arising from the European regulation are applied. Such principles include:

- Personal data should be collected only for specified, explicit and legitimate purposes;
- The persons concerned should be informed about such purposes and the identity of the data controller;
- Any person concerned should have a right of access to his/her data and the opportunity to change or delete data which is incorrect; and
- If something goes wrong, appropriate remedies must be available to put things right, including compensation or damages through the competent courts.

In order to facilitate the free circulation of data, the EU Commission has adopted pan-European standard model clauses. Companies may always rely on any different contract they'd draft themselves, provided that it is approved by the national privacy Commissioner of the country of the sender. But, if companies choose for the EU model clauses, all national Member States are under the obligation to recognize the standard contractual clauses as fulfilling the requirements laid down by the Data Protection Directive for the export of data to a third country, and consequently may not refuse the transfer. There are model clauses for a transfer from a controller to a controller, as well as for the transfer from a controller to a processor.

c) Binding corporate rules ("BCR")

Binding Corporate Rules are internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. It ensures that all transfers that are made within a group benefit from an adequate level of protection. This is an alternative to the company having to sign standard contractual clauses each time it needs to transfer data to a member of its group, and may be preferable where it becomes too burdensome to sign contractual clauses for each transfer made within a group. Once approved under the EU cooperation procedure, BCR provide a sufficient level of protection to companies to get authorization of transfers by national data protection authorities. It should be noted that the BCR do not provide a basis for transfers made outside the group. BCR must contain in particular: privacy principles (transparency, data quality, security, etc.); tools of effectiveness (audit, training, complaint handling system, etc.); and an element proving that BCR are binding.

Listed and/or large companies

In practice, a large number of multinational and/or listed companies start by qualifying under the Safe Harbor Principles in order to secure exchanges between the EU and the USA. Later on, they deploy those Principles within the group to harmonize the protection of data regardless the country where they are processed/sent/received. At the end, they get approval of the global system under the BCR system. Despite the fact that the whole process can prove to be quite heavy, those companies usually find it satisfactory at the end, notably because it considerably facilitate compliance with other legal requirements, such as whistle blowing procedures, e-discoveries, SOX Act and other financial regulations for listed companies.

Other exceptions

Very exceptionally, the national data protection authority of the sender of the data in the EU, may authorize a transfer that would normally not be

fully compliant; it will usually authorize it under other strict conditions and is usually reluctant to do so.

Also, the prohibition is waived in the following exceptional situations provided for in the European directive (please note it being exceptions, they should be interpreted restrictively and cannot constitute a normal framework for data transfers, especially when they are massive and repetitive):

- The data subject has unambiguously given his free and informed consent to the proposed transfer;
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;
- The transfer is necessary in order to protect the vital interests of the data subject;
- The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.