U.S. Subpoenas and European data protection legislation

Moerel, Lokke; Jansen, Nani; Koëter, Jeroen

Published in:
International Data Privacy Law

Document version:
Early version, also known as pre-print

Publication date:
2009

U.S. Subpoenas and European Data Protection Legislation

LOKKE MOEREL, JEROEN KOËTER, AND NANI JANSEN

Authors review the implications of the EU data protection rules when EU companies have to transfer personal data in order to comply with subpoenas issued by the U.S. authorities.

Following several press reports in June 2006,[1] it was revealed that the United States Department of Treasury had served administrative subpoenas on the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") in order to transfer personal data located on SWIFT's server in the United States for counter-terrorism purposes. SWIFT is a cooperative society under Belgian law that is owned by European financial institutions. It operates a worldwide financial messaging system in relation to financial transfers between financial institutions. The information processed by SWIFT concerns messages on the financial transactions of hundreds of thousands of EU citizens, amounting to more than 12 million messages on a daily basis. These messages contain without question personal data of EU citizens. The independent advisory body to the European Commission on data protection and privacy ("Article 29 Working Party") issued an opinion on the transfers of personal data by SWIFT based on the subpoenas issued by the U.S. Treasury Department.[2] The Article 29 Working Party concluded that SWIFT and the financial

Lokke Moerel (lokke.moerel@debrauw.com) is partner and head of the data protection practice at the ICT practice of De Brauw Blackstone Westbroek, Amsterdam, The Netherlands. Jeroen Koëter and Nani Jansen are associate and junior associate, respectively, at the firm's ICT practice.

Published in the July 2009 issue of Privacy & Data Security Law Journal.

institutions that use SWIFT's services had breached European data protection laws by transferring the personal data to the United States without ensuring adequate protection of such data and by failing to inform the individuals concerned about how their personal data was being (subsequently) processed. In hindsight, it is clear that SWIFT found itself in a conflict of law position between applicable U.S. laws (granting U.S. authorities certain powers to seize data) and European data protection requirements.

This Catch-22 situation SWIFT found itself in is not unique. To date, many European based companies have found themselves in similar positions where U.S. supervisory authorities such as the SEC, FTC, OFAC, the U.S. Department of Justice or the U.S. Department of Treasury (together the "U.S. Authorities") requested information from their U.S. group company, whether on a voluntary basis preliminary to such authority deciding whether to institute an official investigation based on a criminal or administrative subpoena, or on the grounds of various specific statutes.[3] Often, the information requested may involve handing over e-mail correspondence between the U.S. group company and its EU parent company, whose e-mail correspondence is often (centrally) stored on a server located at the parent company. European data protection laws apply to such data.

A company may also find itself facing similar dilemmas outside the realm of criminal or government investigations. This could be the case when a civil suit is filed in the U.S. and data originating from the EU has to be presented for pre-trial discovery.[4] Alternatively, a U.S. parent company might wish to institute its own internal investigation in case of reasonable anticipation of U.S. legal proceedings or government investigations, which internal investigation involves the transfer of personal data from its EU group companies to the U.S. However, this article focuses on data protection issues related to the submission of personal data either by complying with or trying to prevent the issuing of subpoenas by the U.S. Authorities.

There are two main questions in this respect:

1. Whether the processing of personal data within a company group in order to comply with the subpoena is in compliance with the EU data protection laws, and

2. Whether the transfer of such personal data to the U.S. Authorities is allowed under EU data protection laws.

THE EUROPEAN PRIVACY DIRECTIVE

The European Directive on the Protection of Personal Data[5] (the "Privacy Directive") aims to harmonize the level of protection for the processing of personal data within the European Union and stipulates the conditions under which such processing of personal data is lawful. "Personal data" is all data by which individuals can be identified, such as the name of a person, date of birth, telephone number, e-mail address, conditions of employment, etc. It includes both private and business-related data of a natural person. "Processing" means any operation which is performed upon personal data, such as the collection, storage, use, updating and transfer of such data. Since the Privacy Directive does not have direct effect, EU Member States have implemented the Privacy Directive in their respective national data protection laws.

LEGAL IMPEDIMENTS UNDER THE PRIVACY DIRECTIVE TO COMPLYING WITH U.S. SUBPOENAS

Pursuant to the Privacy Directive, personal data may be processed for specified and legitimate purposes only. To the extent data is transferred to countries outside the European Economic Area ("EEA") that do not provide an "adequate level of protection", additional criteria must be met. Furthermore, for the processing of "sensitive data" stricter rules apply than for other personal data. These requirements apply cumulatively although some criteria overlap to a great extent. In the following we discuss these requirements separately.

Regarding Legitimate Processing

A processing is legitimate if it fulfils one of the criteria provided by the Privacy Directive. This means that companies first have to determine whether there is a legal basis for a processing. In practice, only the follow-

ing three criteria listed in the Privacy Directive could serve as a basis for a processing of personal data in relation to a U.S. subpoena:

a. The individuals involved have provided their unambiguous consent;
b. The data processing is necessary for compliance with a legal obligation that applies to the company; and
c. The data processing is necessary for the legitimate interests of the company, unless the right of privacy of the individuals involved prevail.

The Individuals' Unambiguous Consent

Under the Privacy Directive, consent must relate to specific purposes, be based on clear, complete and correct information, and be given freely. The consent should therefore specifically relate to (in this case) the internal investigation at hand and the subsequent transfer of that data to the U.S. Authorities. The requirement that consent must be given freely entails that the individual should be able to refuse his or her consent without any consequences whatsoever. To the extent the personal data of employees is involved, the requirements for consent are even stricter. According to many EU Data Protection Authorities ("DPAs"), consent by an employee is deemed not to be given "freely" since there is a relationship of authority.[6] Employees' consent will only be considered valid if the employees are offered a realistic alternative (e.g., that the data of the individual is not part of the information to be provided to the U.S. Authorities, which usually is not an option). The relevant individuals should be explicitly informed that they may refuse their consent or withdraw it at any time afterwards. In practice this means that consent is often refused. In respect of individuals who refuse their consent, a company will then no longer be able to rely on one of the other possible grounds for processing (as discussed below). The personal data of the individuals who refused consent will then have to be excluded from the information submitted to the U.S. Authorities.

The route of requesting consent for an internal investigation (and subsequent submission of the findings to the U.S. Authorities, see below) will therefore in many cases not be a viable basis for companies to comply

with a request or subpoena from the U.S. Authorities. This may be different in individual cases where the submission of personal data is clearly in the interest of an individual concerned (for instance because he or she is involved in the litigation or if he or she will be granted immunity from prosecution if he or she cooperates).[7]

Compliance with a Legal Obligation

If a company submits information to the U.S. Authorities in order to comply with U.S. legislation, one could argue that the company is complying with a legal obligation to which it is subject and that it can therefore rely thereon as a basis for the processing of the personal data. However, this legal basis applies only if the processing serves the company's compliance with an EU formal statute. As the processing at hand would serve to comply with a U.S. law and not with an EU law or regulation, this cannot serve as a basis for the processing. However, in individual EU member states there may exist a legal obligation to comply with the order of a foreign court or a foreign authority or legislation that declares a violation of certain foreign laws also a violation of their national law.

The Legitimate Interests of the Company

This basis requires that a balancing of interests is made between the interests of the company possibly being charged under U.S. law and the interests of an individual possibly being incriminated under U.S. law, incurring liability under civil law or being identified as a witness. In balancing these interests, the principles of proportionality and subsidiarity have to be taken into account. In the present case this would mean the following. The principle of subsidiarity requires that if the interests of a company may be served in a way less harmful to the individuals, this way should be followed. This, for instance, implies that if the legitimate interests of the company are also properly served if only certain data are handed over, providing all data is prohibited. Under the principle of proportionality, insofar as it is possible to anonymize, pseudonymize or otherwise redact the information to be provided, this should be done.[12]

Further, any data filtering activity should be carried out locally in the

country in which the personal data was located.[9] In practice, companies may use this legal basis for the processing of personal data within the company for an internal investigation (question 1 from the introduction). It cannot, however, serve as a legal basis for the transfer of such data to the U.S. Authorities. In any event, for such transfer, additional criteria have to be met, as set out in the following section.

Regarding Transfer of Personal Data to Countries Outside the EU

The Privacy Directive prohibits the transfer of personal data to a third party located in a country that does not provide an "adequate level of protection" of personal data. The European Commission has established that the U.S. does not provide such adequate level of protection. Transfer of personal data to a third party located in the U.S. is therefore prohibited unless the recipient of the personal data is a U.S. established entity that adheres to the Safe Harbor principles. The Safe Harbor framework allows U.S. organizations to satisfy the Privacy Directive's requirements regarding, amongt other things, adequate protection. Until now, no U.S. Authority has adhered to the Safe Harbor principles. However, the Directive allows for the transfer of personal data to a country without an adequate level of protection on the following grounds (insofar as relevant here):

a. The unambiguous consent is obtained of all individuals whose personal data is transferred;
b. The transfer is necessary for the establishment, exercise or defense of legal claims; or
c. Adequate safeguards are provided for the transfer of the data.

Consent of the Individuals

The same applies as set out in the previous section. The route of requesting consent is therefore mostly not a viable basis for a company to transfer personal data to the U.S. Authorities.

The Establishment, Exercise, or Defense of Legal Claims

This ground applies to transfers in the context of *legal proceedings* only. In this regard, the Article 29 Working Party held that the transfer of data to comply with a subpoena issued prior to legal proceedings does not constitute a valid basis since a company often has then not yet become part of legal proceedings.[10] The foregoing applies *a fortiori* to any processing of personal data and subsequent transfer thereof by a company on a voluntary basis in order to prevent the issuing of subpoenas or to prevent investigations or legal proceedings.

Adequate Safeguards

One of the derogations to the EU transfer rules is that a member state may authorise a certain transfer of data to a third country that does not provide for an adequate level of data protection if the company transferring the data "adduces adequate safeguards with respect to the protection of such personal data". The European Commission has approved the use of so-called EC model agreements ("EC Model Agreement") for this purpose, which EU Model Agreement has to be entered into between the EU data exporting company and (in this case) the relevant U.S. Authority. Further, in many EU jurisdictions, a transfer on the basis of the EC Model Agreements requires authorization of the national DPA. To date the U.S Authorities have steadfastly refused to enter into an EC Model Agreement with European companies. The main reason the U.S. Authorities have so far refused to enter into an EC Model Agreement with European companies is that under the EC Model Agreements the parties involved are jointly liable for damages suffered by the individuals concerned as a result of a violation of the agreement. Without the conclusion of an EC Model Agreement, the transfer of personal data will be in violation of the Privacy Directive.

Regarding Sensitive Data

Stricter rules apply in respect of sensitive data than for other personal data. Sensitive data is personal data revealing racial or ethnic origin, polit-

ical opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life. Data related to criminal records, criminal proceedings or a strong suspicion that a certain person has committed a crime also qualify as sensitive data. As the European personal data covered by an (internal) investigation could very well lead to criminal prosecution of the individual concerned in the U.S., the subpoenaed information might also contain sensitive data. For example, if there is a suspicion of insider trading, violation of anti-trust laws or forgery of documents, the individuals involved could also be personally liable to prosecution and sanctions.

In principle, the processing of sensitive data is prohibited under the Privacy Directive. The Privacy Directive provides only two relevant grounds that could justify the processing of sensitive data in the case of a U.S. subpoena: (a) the explicit consent of the individuals concerned or (b) the necessity of the processing for the establishment, exercise or defense of legal claims. Some European Member States have laid down additional exemptions in national legislation. These grounds may provide additional legal basis to process sensitive data for an internal investigation. However, in any event they do not provide a legal basis to provide such sensitive data to the U.S. Authorities.

OTHER REQUIREMENTS UNDER THE PRIVACY DIRECTIVE

The Privacy Directive places a number of additional obligations upon a company wishing to transfer personal data pursuant to a U.S. subpoena. The company must inform all individuals concerned of the purposes of the processing and provide them with all other relevant information, such as the recipients of the data, the country to which the data is being transferred (U.S), and the level of protection of their personal data in the U.S. (inadequate). The individuals concerned also need to be informed of the manner in which they may exercise their right to access and any subsequent requests for correction or removal of incorrect or irrelevant data. The information should be provided before the investigation commences and before the data is submitted to the U.S. Authorities. Informing the individuals may only be delayed if (and for such time as) a substantial risk exists that such noti-

fication would jeopardize the ability of the company to investigate the case properly or gather the necessary evidence.[11] If other measures can be taken to safeguard evidence (e.g., copying of email files) such measures must be taken rather than delaying informing the individuals. The company transferring the data must take all reasonable technical and organizational measures to protect the data. The company should also impose requirements on external service providers (e.g., law firms, other companies providing litigation support services, accountants) involved in the review of the information as well as on the foreign authority receiving the data.[12]

Depending on local privacy laws, the local DPA may also need to be notified of the processing of personal data.

SANCTIONS

In the event of violations of local privacy laws, a company can incur a number of sanctions, depending on the local DPA's authorizations under national law. The local DPA may apply administrative enforcement, including penalties, or institute an investigatory audit into the compliance of a company with the local privacy laws. Often, DPAs are authorized to present their findings of violations of the local privacy laws to the press, which in practice has proven to be a very effective enforcement tool.

Criminal and civil proceedings are also an option. If non-compliance with privacy regulations constitutes an offense under the local criminal or administrative statutes, a penal fine can be incurred and sometimes even a prison sentence. In addition, the individuals concerned may initiate civil proceedings, such as claims for damages or requests for injunctions against the investigation or the surrender of their data to the U.S. Authorities.

CONCLUSION

Under current legislation compliance with a U.S. subpoena is impossible without simultaneous violation of European privacy laws which therefore poses a serious challenge for multinational companies. As circumstances vary markedly, the exact challenges and possible solutions will have to be evaluated on a case-by-case basis.

Published in the July 2009 issue of Privacy & Data Security Law Journal.

NOTES

[1] "U.S. Secretly Tracks Global Bank Data," Los Angeles Times, June 23, 2006; "Bank Data Is Sifted by U.S. in Secret to Block Terror," New York Times, June 23, 2006.

[2] Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Security for Worldwide Interbank Financial Telecommunication ("SWIFT") adopted on November 22, 2006, 01935/06/EN WP128.

[3] A subpoena could be issued on the grounds of various statutes, including the Patriot Act, Foreign Intelligence Surveillance Act, the Stored Communications Act, or on the basis of National Security Letters.

[4] The Hague Evidence Convention provides a standard procedure through which the court of one country can request assistance from the designated central authority of another in obtaining relevant information in civil and commercial matters. Please note that not all EU member states are a party to The Hague Evidence Convention and some contracting member states (like France, Spain, the Netherlands and Germany) have filed a reservation under article 23 thereof with the effect that pre-trial discovery of any information is not allowed in relation to foreign legislation. There are no multilateral treaties that regulate the cross-border exchange of information in regard to the type of subpoenas that fall within the scope of this article. However, arrangements can be made per sector. For example, the Dutch Financial Supervision Act allows for the Dutch National Bank to provide information on possible violations of certain U.S. and other laws to its U.S. counterparts.

[5] Directive 95/46/EC of the European Parliament and of the Council 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 of the European Communities of 23 November 1995 No L. 281 p. 31.

[6] Article 29 Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context, Sept. 13, 2001 (5062/01/EN/Final WP 48), p. 23.

[7] The Article 29 Working Party comes to the same conclusion in its recent Working Document on pre-trial discovery for cross-border litigation, Article 29 Working Party Working Document 1/2009 on pre-trial discovery for cross-border litigation adopted on February 11, 2009, 00339/09/EN WP158 ("Working Document on pre-trial discover"), p. 8-9. *See* further Working document on a common interpretation of Article 26(1) of Directive 95/46/EC

of 24 October 1995 (WP114), p.11.

[8] *See* Working Document on pre-trial discovery, loc cit, p. 10.

[9] *See* Working Document on pre-trial discovery, loc cit, p. 11.

[10] The Article 29 Working Party considered a subpoena of the United States Department of the Treasury ("UST") not to be a valid basis for a transfer by SWIFT of personal data to the UST, Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Security for Worldwide Interbank Financial Telecommunication ("SWIFT"), *supra* note 2, p. 24-25.

[11] *See* Working Document on pre-trial discovery, loc cit, p. 12. *See* further Opinion 1/2006 on the application of EU data protection rules to internal whistle blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117 00195/06/EN).

[12] *See also* Working Document on pre-trial discovery, loc cit p. 12, where the Article 29 Working Party requires the company to impose such security requirement also on the courts. Some U.S. Authorities (e.g. the SEC) have been willing to enter into confidentiality agreements prior to transfers of data.