Data Detours In Internal Investigations In EU Countries: Part II

Beryl A. Howell and Laura S. Wertheimer

STROZ FRIEDBERG LLC AND WILMERHALE

In the first part of this article, which appeared last month, the authors discussed the European Union ("EU") Data Protection Directive and the challenges it creates in connection with the collection and review of electronic records and data for an internal investigation. This month, the authors conclude their analysis with a discussion of possible work-arounds to enable lawyers to collect records and data from companies with computer networks and servers in the EU.

As discussed previously, the EU Data Protection Directive contains eight general restrictions that apply to the handling of personal data, including data located in the workplace. Two of these restrictions, regarding consent and onward transfer, are significant for internal investigations when timely collection and processing of potentially relevant data for review is critical. We now discuss each of these two restrictions in turn.

Consent

The Directive requires that a data subject provide "unambiguous" consent to personal data processing, unless certain conditions apply, such as when the processing is necessary to:

- Perform a contract to which the data subject is a party (*e.g.*, an employment contract) or to protect vital interests of the subject;
- Comply with legal obligations of the controller;
- Perform tasks in the public interest or in the exercise of official authority vested in the controller or third party to whom the data is disclosed; or
- Pursue legitimate interests of the controller, except where those interests are overridden by the fundamental rights of the data subject.[1]

While an internal investigation authorized by a board of directors is plainly a legitimate interest of a "data controller" (*i.e.*, the company through its management or board), that investigation almost always implicates individual employees who are likely to complain that their rights have been compromised where any data that they have created, whether personal or related to the company, is collected without their consent. Even though such data may be stored on company computers and networks and the company may have an explicit policy, acknowledged by each employee, making clear that the company has a right to such data, the emphasis on employee protections in the Directive makes processing data without employee consent a somewhat risky proposition. As explained earlier, the definition of, and the exceptions to, "personal data" under the Directive are ambiguous. Obtaining employee consent provides the least risky path under the Directive (and most national laws of EU countries) for data collection and further processing. Before any decision is made to proceed down the path of obtaining employee consent, the client should be advised that resolving consent issues with current employees will likely take time, even when a board and/or senior management directs employees to cooperate fully with company counsel.

Beryl A. Howell

Laura S. Wertheimer

Should a decision be made to seek employee consent, lawyers should understand that the process of obtaining such consent is not an easy one. Many employees in the EU understand the protections for personal data and may refuse to provide consent until all "personal" items are removed, including photographs, files marked in a "personal" folder, e-mail with friends on non-work related topics, and/or until an employee's personal counsel is satisfied that all personal data has been removed. Technical protocols can be developed to address some employee concerns. The labor and employment laws of most EU countries are extremely protective of employees, and EU-based employees generally understand that their employment will not be jeopardized if they refuse to provide blanket consents. In addition, EU data protection authorities have cautioned against reliance on consent in an employment setting.[2] For example, employees should be given sufficient time to consider the proposed consent to avoid claims of coercion that might be used to nullify the consents at a later date. Counsel should be aware that it is fairly common for employees in the EU, when asked to review and sign data consents, to edit the consent and add their own terms, and, on occasion, retain counsel to negotiate the consent.[3] Employee consent may be withdrawn at any time, which may influence the timing of separation decisions for employees implicated by the fact-finding in an internal inquiry.[4] For U.S.-trained lawyers, it is a frustrating and time-consuming process to obtain employee consents and negotiate with individual employees (and their counsel). Complicating the already difficult landscape is that any imaging of company servers and backup tapes will likely produce personal data for current and former employees and others who may be peripheral to the investigation and from whom consent was not sought. While it plainly would not be feasible to seek consent from each current and former employee, counsel should understand the potential risks inherent in collecting such data.

Obtaining consents from former employees is thornier. Former employees may have no reason to cooperate and consent to the processing of their personal data stored by the company on servers, computers or back-up media. Depending on the circumstances of their separation, former employees may have every incentive to undermine, slow down or block the progress of an internal inquiry, and no amount of creative negotiation to address data processing concerns may overcome that incentive. Where current or former employee consents are sought and not obtained, counsel should consider whether to disclose the lack of consent to the appropriate regulators (so that the regulators can determine whether to seek the data under applicable treaties for mutual legal assistance).

In each investigation, counsel will need to make a strategic decision as to whether the company's need for such data overrides the privacy interest of the current and former employees in order to collect such data without consent. Special care must be taken to limit the processing of, and protect information about, the employee's personal activities, opinions and family, which is likely to be included in the data collected. In those circumstances, counsel may consider consultation with the supervising data protection agency regarding the scope of such protections.

While consent issues are being resolved, preserving the data is critical. Counsel should cause steps to be taken to suspend the recycling of back-up data, to avoid redeployment of old computers or upgrades to computers used by custodians of interest, and to remove deletion permissions on server data to preserve potentially relevant data for collection and further processing. In addition, clear instructions should be given to employees not to delete potentially relevant data or to use "wiping" programs that overwrite deleted data and may trigger concerns over compliance with preservation obligations.

Preserving data on a corporate network that may be relevant to a claim or defense in reasonably foreseeable litigation is standard operating procedure in the United States. In EU countries, however, the Data Protection Directive restricts the storage of data for "no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[5] The French Data Protection Authority, called the Commission Nationale de l'Informatique et des Libertes, or CNIL, which is in charge of overseeing the implementation and observance of the Directive in France, recently acknowledged the tension caused by the Directive and the preservation, collection and transfer of data to comply with American electronic discovery obligations. In a statement issued on January 15, 2008, the CNIL noted complaints by French companies stemming from their legal obligations under U.S. law to enforce litigation holds, collect data for pre-trial discovery, abide by injunctions by U.S. government agencies to retain personal data, and protect themselves from potential criminal liability for destruction of documents with the intention to hamper ongoing inquiries.[6] The CNIL, which now chairs the organization of EU data protection authorities created by the Directive (known as the Article 29 Working Party) announced that it would seek an EU-wide solution to these issues.[7]

Because of the significant employee protections contained in the Directive, collection efforts will likely be far slower than collection of data in the U.S. Counsel should initiate discussions with U.S. regulators to explain the difficulties and delays in collecting and producing such data to them.[8]

Onward Transfer

The Directive requires Member States to prohibit the transfer of personal data for processing to a third country that does not provide an "adequate" level of privacy protection.[9] No definition of "adequate" privacy protection is provided in the Directive. Shortly after the Directive became effective, the European Union evaluated the U.S. legal regime for privacy protection and found U.S. safeguards inadequate.[10] This finding has significant implications for U.S. lawyers and U.S. law firms hired to conduct internal investigations of companies with a EU presence, regardless as to whether or not the company is based solely in the EU, since EU restrictions govern the transportation of collected personal data, as well as where such data may be processed and reviewed.

Even if the data protection of a particular country is deemed to be inadequate, transfer may take place where consent is obtained from the employees, or data subjects, for movement out of the country.[11] As a practical matter, any consent sought from employees and former employees should provide that the individual authorizes the data controller to choose the venue for processing and review of the data. Structuring that consent with restrictions on confidentiality and security of the data may alleviate individual concerns.

Absent consent, several exceptions to the "onward transfer" prohibition in the EU Directive permit the movement of personal data out of the EU country of origin to a non-EU country, but those exceptions have little, if any, applicability to internal inquiries. For example, transfer is authorized when necessary for the performance of a contract with the data subject, including a contract "concluded in the interest of the data subject," and covers data transfers that may take place during employment contract negotiations or to protect "the vital interests of the data subject." An exception also permits data transfers that are "legally required on important public interest grounds or for the establishment, exercise or defence of legal claims."[12] Most internal investigations are conducted voluntarily and are not required by any regulator. Unless a regulator makes a formal demand, by subpoena or otherwise, for records maintained in the EU, it is likely to be difficult to establish the legal necessity of data transfers for fact finding in an internal inquiry. Moreover, considerable uncertainty exists regarding whether the public

Please turn to page 39

***Beryl A. Howell** is the Executive Managing Director and General Counsel of Stroz Friedberg LLC, a national consulting and technical services firm, and a Commissioner of the U.S. Sentencing Commission. **Laura S. Wertheimer** is a Partner in the Securities Department of WilmerHale whose practice focuses on counseling issuers, boards of directors and board committees on insider trading and other securities law issues, fiduciary duties, and corporate governance, and in connection with internal and governmental investigations and cross-border regulatory proceedings.* *The views expressed in this article are solely those of the authors. The authors thank for their assistance in the preparation of this article J. Beckwith Burr of WilmerHale and Dana Leseman, Jessica Smith and Stephen Lewis of Stroz Friedberg.*

Please email the authors at bhowell@strozllc.com or laura.wertheimer@wilmerhale.com with questions about this article.

Data Detours

Continued from page 38

interest exception applies to the interests of a country outside the EU. For example, the Article 29 Working Party asserted that the U.S. Center for Disease Control's effort to collect passenger data to prevent the spread of avian flu did not fall into that exception in the first instance, as the "processing is not necessary for the performance of a task carried out in the *public interest of a EU Member State*, but only in the interest of the US (emphasis added)." [13]

Onward transfers may take place if the data controller obtains adequate contractual safeguards for transferred data.[14] The European Commission has ratified three sets of "model clauses" deemed to provide adequate protection for data transferred between parties to the contract.[15]

In some cases, compliance may be simplified by transferring data to one EU State for initial processing. Relevant data can then be loaded onto an online litigation review database, and any subsequent transfer, for example to the U.S., would be governed by the rules in that jurisdiction. Under the EU Directive, "processing" includes the transmission of personal data. As with other terms in the Directive, the definition of a transfer is subject to varying interpretations by different EU states. For example, in 2001, the Swedish Data Protection Authority successfully sued a Swedish church member for posting on her website personal data about fellow parishioners on the grounds that it violated the Directive's notice, consent and onward transfer requirements.[16] On appeal, the European Court of Justice ("ECJ") was asked to interpret provisions of Article 25 in the Directive and, in particular, whether posting information online constituted a transfer of personal data to third countries that may lack adequate privacy protection. The ECJ held that a "transfer" under Article 25 of the EU Directive required more than the ability to access data from a third country and required that a transfer of personal data occur from one place and person to another place and person.[17] Uploading personal data to an Internet website when the person posting the information and the internet service provider hosting the site were both in an EU Member State, even though the information could be accessed in non-EU Member States, was not construed as "transferring" data to a third country.

The "church lady" case could be construed to mean that no "transfer" of personal data will be found to occur in the document review context, when "personal data" extracted from an EU company's equipment is loaded onto a secure litigation database server in an EU member state and accessible via the Internet for remote review in the United States. Support for this conclusion may be found in the reasoning of the ECJ that the Directive was not violated by the posting online in an EU country of personal data, which then could be widely shared with anyone who accessed the site. Yet, the technical configuration in the typical document review context is very different. In contrast to the situation in the ECJ case, data loaded onto a secure database would only be accessible by a limited group of defined individuals conducting the review. Thus, ironically, the steps taken to protect and restrict access to the data on a litigation database may be sufficient to satisfy the requirement of data transfer between specific people to fall within the coverage of the onward transfer provision of the Directive. Counsel must therefore evaluate the technical solution for conducting document review to ensure that it comports with the applicable data protection laws,

U.S. Department Of Commerce Safe Harbor

As noted earlier, the U.S. is not considered to provide "adequate" legal protection for personal data, potentially blocking all data transfers from Europe to the United States. In an effort to facilitate such transfers, the U.S. Department of Commerce ("DOC") and the European Commission agreed upon a mechanism, known as the Safe Harbor Framework.[18] Companies that publicly certify their compliance with the Safe Harbor Principles – and through such certification subject themselves to the enforcement authority of the Federal Trade Commission – are recognized by the European Commission as providing "adequate" legal protection for personal data. The European Commission's approval is binding, and EU Member States are not permitted to block data transfers to certified organizations within the United States based on the inadequacy of U.S. law. Nonetheless, the vagaries of national implementing laws for the Directive must still be checked since the Safe Harbor Framework is limited solely to the "adequacy" of the privacy protection for data transfer purposes.[19] The Safe Harbor Framework does not legitimize processing that would be barred under national law. The DOC maintains a list of over 1,300 U.S. companies from over 100 industry sectors that have registered and have been certified under the Safe Harbor Framework, including an increasing number of electronic discovery consultants.[20]

To obtain certification as compliant with the Safe Harbor Framework, an organization must satisfy seven data protection principles that track generally accepted concepts of "fair information practices" as embodied in the EU Directive, including requirements for notice, choice, onward transfer, security, data integrity, access and enforcement.[21] For example, certified organizations must provide security for personal data and take reasonable precautions to protect it from loss, misuse, unauthorized access, disclosure, alteration and destruction. They must also ensure data integrity and take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Notably, the notice and choice principles do not apply when "disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization."[22] Thus, a certified electronic discovery consultant that has been retained by counsel (or the client company) and receives personal data from an EU country, with directions to process that data in accordance with its client's instructions, acts as a third party agent and is not required to provide choice or notice to any individuals whose personal data may be included in the collection.[23] Any notice and choice obligations under national law rest with the data controller. Similarly, while generally organizations must, under the onward transfer prohibition, apply the Notice and Choice Principles of the Safe Harbor Framework, this prohibition does not apply to data transfers to a third party "that is acting as an agent" when the controller "ascertains that the third party subscribes to the Principles" or other applicable exceptions.[24]

Verification that a certified company is in compliance with the Safe Harbor Framework may be accomplished by either an outside compliance review or a "self-assessment" that the company's published privacy policies are accurate, comprehensive, prominently displayed, completely implemented and accessible. These published privacy policies must conform to the Safe Harbor Framework Principles by informing individuals of the in-house arrangements for handling complaints and of the independent mechanisms through which complaints may be pursued. In addition, the Safe Harbor-certified company must have in place procedures for training employees on complying with the privacy principles, disciplining employees for compliance failures, and periodic compliance reviews.[25] Certified companies must agree to submit to a binding resolution of complaints by a third-party dispute resolution program or choose to cooperate and comply with the European Data Protection Authorities ("DPAs").

Conclusion

With the ever-increasing expansion of multinational corporations and globalized business transactions, internal inquiries conducted by U.S. lawyers, in whole or in part, in EU countries, are likely to increase. Collecting and processing electronic documents is a complex, painstaking process in the U.S., and that process is further complicated by the EU Directive for protecting personal data resident on company equipment. Transferring properly collected personal data is yet another challenge under the EU Directive and the implementing regulations of separate EU Member States. While far from an impossible task, an understanding of the requirements contained in the EU Directive, as well as possible exceptions to these requirements, is necessary so that U.S. lawyers conducting an internal inquiry that involves data in the EU can collect, process and review the data, without exposing themselves or their clients to possible liability for violations of the EU Directive.

---

[1] *Directive, Art. 7.*

[2] *"The Article 29 Working Party [the organization of EU data protection authorities created by the Directive] has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment." 5062/01/ENFinal WO 48 Opinion 8/2001 on the processing of personal data in the employment context, Adopted on 13 September 2001.*

[3] *Variations in consent forms among employees at the same company may be useful to demonstrate the lack of coercion or pressure in obtaining the consent, should challenges be raised later.*

4 *Directive, Art. 14(a), 14(b) (Data subject has the right, in some circumstances, "to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him").*

[5] *Directive, Art. 6(e).*

[6] *CNIL,* Les entreprises inquiètes du dévelopement des règles leur imposant la communication de données personnelles aux Etats-Unis, *Jan. 15, 2008, available* at *http://www.cnil.fr/ index.php?id=2379&print=1. Note also that, in January 2008, the highest French court upheld a criminal conviction of a French lawyer, and a 10,000 Euro fine for violating of the blocking statute, French Penal Code Law No. 80-538. The French lawyer, who was hired by an American law firm representing the California insurance department that was investigating the French mutual insurance company, MAAF, had telephoned MAAF to seek information informally from it in connection with the inquiry. At the time of the call, MAAF was a defendant in the then-pending Executive Life litigation in U.S. federal court. Cour de Cassation [Cass, Crim.], Paris, Dec. 12, 2007, Juris-Data No. 2007-332254.* See also *http://www.cnil.fr/index.php?2464 (Discovery Case : Another Sensitive Issue With The USA).*

[7] *This issue is now listed as a high priority issue in the Working Party's 2008 – 2009 Work Programme. See EU Advisory Body on Data Protection and Privacy, supra note 38, available at http://www.cnpd.lu/objets/wp29/wp146_en.pdf. As of the writing of this article, no solution has been reached.*

[8] *In addition to EU Member States, other countries have data protection statutes that regulate access to employees' data and cross-border data transfers, with ramifications for the conduct of internal investigations by US law firms, including the European Economic Area (EEA)* (i.e., *Iceland, Liechtenstein, and Norway), neighboring countries* (e.g., *Albania, Andorra, Bosnia and Herzegovina, Croatia, Macedonia, and Switzerland), and the Russian Federation. M. Wugmeister, K. Retzer, C. Rich, "Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules," 38 Geo J. Int'l L. 449, 455 (Spring 2001).*

[9] *Directive, Art. 25.*

[10] Report on the Draft Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles, *(C5-0280/2000-2000/2144 (COS)), June 22, 2000.*

[11] *Directive, Art. 26(1) (a) (transfer "may take place on condition that: (a) the data subject has given his consent unambiguously to the proposed transfer").*

[12] *Directive, Art. 26(1)(d).*

[13] *http://www.cnil.fr/fileadmin/documents/approfondir/dossier/transport/avis_G_29_Communicable_diseases-PNR-_US_projet_NPRM_adopt_le_14_juin_2006_1014-06_EN_wp_121.pdf.*

[14] *Directive, Art. 26(2).*

[15] *Commission Decision 2001/16/EC of 27 December 2001 "on standard contractual clauses for the transfer of personal data to processors established in third countries, under the directive 95/46/EC," Commission Decision 2001/497/EC of 15 June 2001 under the directive 95/46/EC – O.J. L. 181/19 of 4.7.2001, and Commission Decision 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 (2004/915/EC).*

[16] Bodil Lindquist v. Sweden, , *Case C-101/01, 2003.*

[17] Id.

[18] *The Safe Harbor framework is comprised of a collection of documents negotiated between the DoC and the EU,* available at *http://www.export.gov/safeharbor/ SH_Overview.asp.*

[19] *Department of Commerce "SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE ON JULY 21, 2000," (The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States"),* available at *http://www.export.gov/safeharbor/ SHPRINCIPLES-FINAL.htm.*

[20] *http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/Search+by+Industry+Sector.*

[21] *Department of Commerce "SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE ON JULY 21, 2000,"* available at *http://www.export.gov/safeharbor/ SHPRINCIPLESFINAL.htm..*

[22] Id, *at endnote 1(note that while notice and choice principles do not apply to disclosures to third party agents, "[t]he Onward Transfer Principle, on the other hand, does not apply to such disclosures").*

[23] *Department of Commerce, Safe Harbor Workbook, Section II. Safe Harbor Principles, Notice ("Note that for a third party which is acting as an agent, notice and choice do not need to be provided"), available at URL: http://www.export.gov/safeharbor/SH_Workbook.asp.*

[24] *Department of Commerce,* supra *note 56,* available at *http://www.export.gov/safeharbor/ SHPRINCIPLESFINAL.htm. See also Safe Harbor Workbook, Section II. Safe Harbor Principles, Onward Transfer ("Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles"),* available at *http://www.export.gov/safeharbor/ SH_Workbook.asp.*

[25] *See Safe Harbor FAQ 7,* available at *http://www.export.gov/safeharbor/SH_FAQ7.asp.*