International Law & Trade – Law Firms

Data Detours In Internal Investigations In EU Countries: Part I

Beryl A. Howell and Laura S. Wertheimer

STROZ FRIEDBERG LLC AND WILMERHALE

Beryl A. Howell

Laura S. Wertheimer

In today's regulatory climate, boards of directors of public companies are increasingly expected to act decisively when concerns of possible misconduct are raised, and are being held accountable for those actions. An internal investigation, whether conducted by the board or by a board committee, or by inside corporate counsel, is one approach frequently used by boards of directors to find the facts and then take prompt and appropriate remedial steps. As a matter of strong corporate governance, that approach protects the interests of the shareholders and positions the company to respond to any potential government enforcement action. Consequently, time is of the essence and there is no margin for error. Close scrutiny of any factual findings of the internal investigation from the board, company management (and their counsel), shareholders, and regulators, among others, should be expected and these findings are only as sound as the record on which they are based. Collecting the relevant documents, in electronic and paper form, requires diligence, thoroughness and dogged determination, as well as meticulous documentation of all such collection efforts. Regulators and prosecutors – who may agree to refrain from pursuing a parallel government investigation pending the outcome of the internal investigation – often expect detailed summaries of the records preservation protocol of the company and the collection efforts, review and analysis performed by the lawyers leading the inquiry. Among the factors U.S. prosecutors must consider in evaluating corporate cooperation and making charging decisions, is "the corporation's willingness to provide relevant evidence" and "incomplete or delayed production of records."[1]

These substantive and time pressures are significant when lawyers seek to access electronic records and data in the United States on a company's network and from employee desktops, laptops, BlackBerries, and PDAs. In the U.S., many public companies have adopted written policies, acknowledged by employees, in which employees are put on notice that they can have no expectation of privacy in information created and/or stored on the company's information technology platform, which permits lawyers to collect employee-generated data without any employee consent. The ever-increasing sophistication of networked environments presents numerous challenges to thorough document collection, including significant gaps between policy and reality in the operation of backup systems and storage of backup tapes; lax enforcement of records retention policies; incomplete asset control inventories and outsourced IT vendors. Generally, those challenges can be managed through a comprehensive protocol developed and applied by the lawyers and any discovery experts they may retain.

These challenges, however, are significantly greater when the inquiry requires counsel to collect records and data from companies with computer networks and servers in the European Union ("EU"). The EU Data Protection Directive provides that "information about a person is believed to belong to that individual and personal information is treated as intellectual property."[2] Broadly speaking, information about an employee residing on company property, including personal information in documents created by an employee that are maintained on company computers, servers and equipment, are considered to be personal data and access to such data is significantly constrained.[3]

In Part 1 of this article, we examine the requirements imposed by the 1995 EU Data Protection Directive respecting the collection, process and review of data located in an EU country[4] and for data created by employees on company property in the EU (whether or not they are EU citizens). In Part 2, which will be published next month, we discuss possible approaches that counsel can consider to navigate the legal thicket of the EU Data Protection Directive. As we will explain, none of the issues posed by the EU Data Protection Directive is insurmountable. Investigating counsel must simply anticipate them, recognize them when they arise, and determine an appropriate work-around.

EU Data Protection Directive. Although the EU adopted the Data Protection Directive in 1995 to harmonize data protection regulation in the EU, implementing legislation by the Member States is not uniform. The EU Data Protection Directive is comprised of a preamble and 34 articles divided into eight chapters. Member States were required to enact implementing legislation by 1998, and all have, although inconsistently. Moreover, the interpretation of identical requirements in the Directive and national legislation vary significantly from country to country. Consequently, familiarity with the Data Protection Directive is only a starting point. The specific laws of the country in which data is sought for an internal inquiry must be examined, both because the substance of the limitations as well as the penalties for violating the limitations, differ. For example, violations of the French data protection law carry both civil and criminal penalties,[5] while the UK data protection law does not, as yet, provide for criminal penalties.[6]

Key Terms. At the outset, understanding the terms used to describe key roles to which rights and duties apply in the Directive is helpful. A "data subject" is the natural person who can be identified, directly or indirectly, by the personal data.[7] EU data protection laws generally apply to all information processing activities that take place in the jurisdiction. Under the Directive, the definition of "data subject" is not limited to EU citizens – for example, U.S. citizens working in a EU country are "data subjects" and obtain all protections for data subjects under the Directive.[8] A "data controller" is a person or entity that determines the purposes and means of processing personal data,[9] and a "data processor" is a person who carries out the processing at the instructions of the controller.[10] "Processing" covers almost any handling of personal data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[11]

Lawyers retained to conduct an internal investigation (whether or not it involves an EU company or subsidiary) typically begin by collecting potentially relevant data. The collection effort ordinarily involves acquiring forensic copies of data from various media sources belonging to the company, including images of workstations, laptops, and handheld and removable data storage devices used by company employees, and backup tapes from company servers for the relevant time period. In light of the enormous differences in practices among companies regarding data sources and storage, many lawyers engage outside experts to assist in identifying potential data sources, coordinate with the internal IT function, and to participate in employee interviews regarding data sources and storage, and to handle the collection of data from each potential source. This document collection effort should be well documented, both to demonstrate the thoroughness of the data collection and to assure regulators that the collection has been performed in good faith. Where outside consultants are used, they can provide expert attestations to explain the collection and processing steps undertaken and respond to regulator inquiries.

That collection and processing effort is significantly complicated when undertaken in the EU. When a lawyer and/or an outside consultant (or an internal IT Department), working at counsel's direction, causes copies to be made of company data in the EU, for purposes of the internal inquiry, the EU Data Protection Directive is triggered, even if the copying occurs solely on the company's premises. Data processing that occurs after the collection – *e.g.*, applying specified filters to the data, converting the data into a format amenable to loading into a litigation review database, marking for privilege or other designation, and production – is almost always undertaken outside of the company. Moving company data to another location for processing and review by the investigating counsel may raise additional issues under the EU Data Protection Directive, particularly if the data is moved outside of the European Economic Area.[12]

Scope. The EU Data Protection Directive applies to "personal data," which is defined as data that "relat[es] to an identified person or identifiable natural person" (i.e., the "data subject"), who "can be identified, directly or indirectly," by reference to an identification number or "to his physical, physiological, mental, economic, cultural or social identity."[13] Each EU Member must implement the EU Directive as the floor of minimum protection, but is free to provide more stringent protections. This means that the scope of information covered by "personal data" varies among the EU Member States, and different types of personal data receive different levels of protection.[14] For example, do the protections for "personal data" extend broadly to include any information that can be retrieved by searching for an employee's name, such as any email or file with the employee's name on it or from which an employee may be identified, or any file connected to an employee, no matter the subject matter or focus of the email or file? Or, to qualify for these protections, must the information in the file more narrowly pertain or focus on the employee's personal activity, family or biographical information, or expressions of opinion or intention about the employee? EU Member States answer these questions

Please turn to page 31

***Ms. Howell** is the executive managing director and general counsel of Stroz Friedberg, a national consulting and technical services firm, and a Commissioner on the U.S. Sentencing Commission. **Ms. Wertheimer** is a partner in the Securities Department at Wilmer Hale 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 Wilmer Hale and Dana Lesemann, 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 30

differently, depending on their individual Data Protection Acts.

The scope of the definition of "personal data" in the UK's Data Protection Act was tested in a high-profile 2003 case brought by Michael Durant, who sought records from the Financial Services Authority (FSA), a banking regulatory authority, about the FSA's investigation of his complaints of allegedly fraudulent activity at Barclays Bank, where Durant had been a customer. Suspecting that this record request was "a misguided attempt to use the machinery of the [Date Protection] Act as a proxy for third party discovery with a view to litigation or further investigation," the UK Court of Appeal rejected the request and concluded that the definition of "personal data" should be applied narrowly, stating, in pertinent part:

> [N]ot all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser degree.[15]

From a business perspective, the UK's narrow interpretation of the information covered by "personal data" is good news, since the mere fact than an employee authored or was involved in documentation for a particular business transaction or event, and that authorship or participation is noted by the employee's name in the records, should not be sufficient to trigger the protections of the Data Protection Act and special handling for those corporate records.

Nevertheless, the UK Court of Appeal's *Durant* decision has apparently been controversial and prompted questions by the EU about UK compliance with the Data Protection Directive.[16] The UK's Information Commissioner's Office (ICO), which is responsible for providing guidance on the UK's implementation of the Data Protection Directive, issued clarifying guidance about how to determine whether information is "personal data."[17] This guidance suggests that reports of meetings that mention attendees, may, in fact, be personal data relating to those attendees since the information documents their "whereabouts at a particular time."[18]

The ICO guidance also provided:

> [w]here data about objects is not currently processed to provide information about an individual, but *could be processed to provide information* about an individual (for example, taxi location data), the data is likely to be personal data. What is being considered here is whether the processing of the information has or could have a resulting impact upon the individual even though the content of the data is not directly about that individual, nor is there any intention to process the data for the purpose of determining or influencing way that person is treated. (emphasis added)[19]

Taken literally, this guidance suggests that almost any corporate record could be deemed "personal data." The ICO acknowledged the difficulty created by its guidance: "There will be circumstances where it remains uncertain whether particular data is personal data. Where this is the case we consider that, as a matter of good practice, you should still treat the information with care and, in particular, ensure it is held and disposed of securely."[20] ICO guidance on employee monitoring similarly suggests that the UK data protection authority views the concept of personal data somewhat more expansively than the *Durant* Court.[21]

A 2001 French case underscores the difficulties in determining what is personal data under the Data Protection Directive, a task further complicated by the common use of workplace email systems, networks and computers for personal emails and online tasks. The commingling of personal activities with work-related activities on company resources that are assigned to particular employees, require that handling all data on these resources in EU countries is consistent with the EU Directive. Even when a company makes clear to its employees, including all EU employees, that there is no expectation of privacy for data on company resources and that all email sent or received on company equipment is subject to monitoring, the combination of EU Privacy Directive law, Europe's recognition of private communication as a fundamental human right[22] and various labor laws may trump the internal corporate policy and require special handling of the data. In France, an employee discharged for violating a non-compete agreement successfully sued his employer for violation of his privacy on the grounds that his employer reviewed his email – including emails marked "personal" – which confirmed that he was engaged in freelance work during working hours. Despite an express workplace policy forbidding employees to use company computers for personal use, the French Supreme Court held that the employer erred in reviewing the employee's email because that employee enjoyed a right to privacy during and at his place of work.[23]

General Restrictions. The EU Directive does not apply to data processing operations "concerning public security, defence, State security and criminal law enforcement" or "by a natural person in the course of a purely personal or household activity."[24] Eight general restrictions apply to the handling of personal data in other circumstances, including data located in the workplace:[25]

1. *Limited Purpose for Collection and Use*: Data should be processed for a specific purpose and subsequently used or communicated only in ways consistent with that purpose.[26]

2. *Integrity:* Data should be kept accurate, up-to-date and no longer than necessary for the purposes for which collected.[27]

3. *Notice*: Data subjects should be informed of the purpose of any data processing and the identity of the data controller, whether or not the personal data is collected or obtained from the data subject.[28]

4. *Access/Choice/Consent*: Data subjects have the right to obtain copies of personal data related to the subject, rectify inaccurate data and to object to processing in some situations, which will be discussed in more detail below.[29]

5. *Security*: Data controller and processors must take appropriate measures to protect the data.[30]

6. *Onward Transfer*: Data controllers may not send data to countries that do not afford "adequate" levels of protection for personal data.[31]

7. *Sensitive Data*: additional protections must be applied to special categories of data revealing the data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.[32]

8. *Enforcement:* Data subjects must have a remedy to redress violations.[33]

As we will discuss in Part 2 of this article, two of these restrictions, regarding consent and onward transfer, loom large in internal investigations when timely collection and processing of potentially relevant data for review is critical.

---

[1] *"Principles of Federal Prosecution of Business Organizations," Memorandum from Paul J. McNulty, Deputy Attorney General, to Heads of Department Components and United States Attorneys, undated but released December 12, 2006, ("McNulty Memorandum"), at pp. 7, 12. Note also that obligations to retain and produce corporate records may continue after an investigation is concluded.*

[2] *B. George, P. Lynch, S. Marsnik*, "U.S. Multinational Employers: Navigating Through the 'Safe Harbor' Principles to Comply with the EU Data Privacy Directive," *38 Am. Bus. L. J. 735, 742 (Summer, 2001).*

[3] *Directive 95/46EC 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*, available at URL*: http://ec.europa.eu/idabc/servlets/Doc?id=18534.*

[4] *The following 27 countries are Member States of the European Union (EU): Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.* See *http://europa.eu/abc/european_countries/index_en.htm.*

[5] *French Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data), Article 51, available at URL: http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf.*

[6] *UK proposal for addition of criminal penalties to data protection law, available at URL: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf.*

[7] *Directive, Art. 2(a) ("an identified or identifiable natural person ('data subject')").*

[8] *38 Am. Bus. L. J. at 752*, supra, *note 4.*

[9] *Directive, Art. 2(d).*

[10] *Directive, Art. 2(e) ("'processor'...processes personal data on behalf of the controller"), see also Art. 16 (processor, "who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law").*

[11] *Directive, Art. 2(b) ("'Processing of personal data' shall mean any operation or set of operations which is performed on personal data, whether or not by automatic means...").*

[12] *The EEA Agreement permits Norway, Liechtenstein, and Iceland to participate in the European single market without joining the European Union.*

[13] *Directive, Art. 2(a).*

[14] *For example, the EU Directive covers "personal data" only for individuals (Directive, Art. 2(a)), while the Swiss Federal Statute on Data Protection, which used the Directive as a model, defines "data subjects" to include both natural or "legal persons," which includes corporations.* See *Federal Act on Data Protection of 19 June 1992, the Federal Assembly of the Swiss Confederation, Art. 3(b), available at URL: http://www.edoeb.admin.ch/org/00828/index.html?lang=en.*

[15] Durant v Financial Services Authority, *2003 EWCA Civ 1746 (08 December 2003), at ¶ 28, available at URL: http://www.bailii.org/ew/cases/EWCA/ Civ/2003/1746.html.*

[16] *"Europe claims UK botched one third of Data Protection Directive," (Sept. 18, 2007), available at URL:http://www.theregister.co.uk/2007/09/18/ec_data_protection_act_objections/.* See also *S. Rempell, "Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute:* Durant v. Financial Service Authority *as a Paradigm of Data Protection Nuances and Emerging Dilemmas," 18 Fla. J. Int'l L. 807, 823 (December, 2006) ("The Court of Appeal interpretation of the DPA is inconsistent with the Directive... the Directive's all-encompassing definition of personal data is not subject to any limiting interpretation").*

[17] *UK Information Commissioner's Office, "Data Protection Technical Guidance Determining what is personal data" (August 21, ,2007), Preamble, available at URL: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf ("We have been aware for some time of the need to replace our guidance on the implications of the Durant judgment. Inevitably that guidance reflected the fact that the Court of Appeal was widely understood to have adopted a rather narrower interpretation of "personal data" and "relevant filing system" than most practitioners and experts had followed previously. We recognized the need to produce guidance with a greater emphasis on what is covered than what is not.").*

[18] Id., *at p. 12, ("Data may, for example, have personal connotations for an individual if it provides information about an individual's whereabouts or actions at a particular time. Example: Where an individual is listed as an attendee in the minutes of a meeting then the minutes will have biographical significance for the individual in that they record the individual's whereabouts at a particular time. The fact that an individual attended the meeting will be personal data about that person. However, this does not mean that everything in the minutes of that meeting is personal data about each of the attendees.")*

[19] Id., *at p. 17.*

[20] Id.

[21] *"Information about individuals, that is kept by an organisation on computer in the employment context, will fall within the scope of the Data Protection Act." ICO Employment Practices Code.*

[22] *"Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms.*

[23] Nikon France v. Onos, *Cass. Soc., Arrêt No. 41-64, October 2, 2001. Discussion of case available at URL: http://www.lawdit.co.uk/reading_room/room/view_article.asp?name=../articles/Nikon%20France%20vs%20Frederic%20Onos.htm.*

[24] *Directive, Art. 3, ¶ 2.*

[25] *V. Boyd, "Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization," 24 Berkeley J. Int'l L. 939, 958-59 (2006); F. Cate, "The Changing Face of Privacy Protection in the European Union and the United States," 33 Ind. L. Rev. 173,185-86 (1999).*

[26] *Directive, Art. 6, ¶ 1(b).*

[27] Id., *Art. 6, ¶ 1(d).*

[28] Id., *Arts. 10, 11.*

[29] Id., *Arts. 7, 12, 14.*

[30] Id., *Art. 17.*

[31] Id., *Arts. 25, 26.*

[32] Id., *Art. 8, ¶ 1.*

[33] Id., *Arts. 22-24.*