



The Impact on U.S. Discovery of EU Data Protection and Discovery Blocking Statutes

January 2011

Hughes
Critical matters. Critical thinking.®
Hubbard

New York ■ Washington, D.C. ■ Los Angeles ■ Miami ■ Jersey City ■ Paris ■ Tokyo

This document is for informational purposes only and is not intended to be and should not be relied on for legal advice.

INTRODUCTION

Cross-border discovery is a significant litigation challenge for multinational companies. Unlike the United States, European nations view the privacy of personal information and data as a fundamental right. This approach has given rise to a complex web of privacy legislation and foreign discovery “blocking statutes” that greatly restrict the processing of data and the transfer of data from Europe to the United States. The countries comprising the European Economic Area (“EEA”)ⁱ adhere to the EU Data Protection Directive (the “EU Directive”)ⁱⁱ which sets forth principles that regulate data privacy protection. The broad scope of U.S. discovery is at odds with the civil law systems of most EEA countries, in which pre-trial discovery is extremely limited or non-existent. Practitioners who represent clients with a presence in the EEA need to be aware of country-specific privacy and discovery blocking legislation and the implications of these laws on U.S. discovery.

We prepared and presented the initial version of this paper in the summer of 2010. Since this is an evolving area of law and practice, we have updated it and are pleased to present this 2011 version.

The paper is organized into two parts. Part I provides an overview of the EU Directive and discovery blocking statutes, addresses their impact on U.S. discovery, and proposes guidelines for navigating the choppy waters of international discovery. Part II identifies, by EEA country, the applicable data privacy statute, commonly-encountered blocking statutes, and recent case law.

-
- i. The European Economic Area consists of the 27 Member States of the European Union plus Norway, Liechtenstein and Iceland (collectively, the “EEA” or “EEA countries”). The Member States of the EU are: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom (U.K.). See http://europa.eu/abc/european_countries/index_en.htm. The non-EU members of the EEA have agreed to enact legislation to implement the EU’s data protection policies.
 - ii. Council Directive No. 95/46/EC, O.J. L 281/31 (1995), http://ec.europa.eu/justice/policies/privacy/law/index_en.htm.

This paper provides an overview of a complex subject and is a starting point for additional, country-specific research. Hughes Hubbard wishes to thank the following members of its eDiscovery Practice Group for preparing the 2011 edition of this paper: Charles W. Cohen, Seth D. Rothman and Yohance Bowden. For more information about the matters discussed herein or our eDiscovery Practice generally, please contact our eDiscovery Practice Group Chairs:

Seth Rothman
(212) 837-6872
rothman@hugheshubbard.com

Charles Cohen
(212) 837-6856
cohen@hugheshubbard.com

TABLE OF CONTENTS

PART I

AN OVERVIEW OF THE EU DIRECTIVE AND BLOCKING STATUTES AND THEIR IMPACT ON U.S. DISCOVERY.....	1
A. The EU Directive	1
1. Scope, Implementation and Enforcement	1
2. Personal Data Defined	2
3. “Processing” Within the Meaning of the EU Directive	3
Principles Concerning Data Quality	4
Criteria for Legitimate Data Processing	4
4. Transfer of Personal Data to Third Countries.....	6
Country-Based Exceptions	6
Corporate-Based Exceptions.....	7
Condition-Based Derogations Under Article 26(1)	8
B. Working Party Opinion WP 158: Applying the EU Directive To U.S. Discovery Obligations	9
C. Blocking Statutes	13
D. Best Practices	14

PART II

DATA PROTECTION LAWS BY EEA COUNTRY	16
Austria	17
Belgium	17
Bulgaria	19
Cyprus	19
Czech Republic	20
Denmark	20
Estonia	21
Finland	21

France	22
Germany	24
Greece	26
Hungary	27
Iceland	27
Ireland	28
Italy	28
Latvia	29
Liechtenstein	30
Lithuania	30
Luxembourg	31
Malta	31
The Netherlands	32
Norway	33
Poland	33
Portugal	34
Romania	34
Slovakia	35
Slovenia	35
Spain	36
Sweden	37
United Kingdom	38
CONCLUSION	41

PART I

AN OVERVIEW OF THE EU DIRECTIVE AND BLOCKING STATUTES AND THEIR IMPACT ON U.S. DISCOVERY

A. The EU Directive

1. Scope, Implementation and Enforcement

The EU Directive was adopted by the European Commission on October 24, 1995, and took effect on October 25, 1998.¹ Its stated purpose was twofold: to harmonize divergent data protection regimes in the Member States in order to remove obstacles to the free flow of information and, to “protect fundamental rights and freedoms, notably the right to privacy”² by establishing minimum safeguards for the use of personal data. The EU Directive covers public and private sector employees³ and, importantly, protects their rights even when electronic data is transferred out of the EU. It does not apply to (i) “processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law”⁴ or (ii) processing by an individual engaged in a “purely personal or household activity.”⁵

The EU Directive obligates each EEA country to enact data protection laws that are at least as protective of personal privacy as the EU Directive itself. Each EEA country has made its own choices with respect to the definition of personal data (which, importantly for U.S. practitioners, includes much workplace data), the level of protection afforded personal data, and the penalties for privacy violations. Each EEA country has complied with the EU Directive and enacted data protection laws. Some countries, including Germany, France, and Italy, have chosen to enact data protection laws that are significantly stronger than the minimum required by the EU Directive.

The EU Directive also obligates each EEA country to create an independent data protection authority (“DPA”) to oversee the application of, and compliance with, the country’s data protection laws. Each DPA has the power to investigate, and intervene in, data processing operations.⁶ The various DPAs were quite active in 2010, although the European Commission believes several DPAs should be stronger. For example, the Commission referred Austria to the European Court of Justice for allegedly not having a DPA

1. Council Directive No. 95/46/EC, art. 32, O.J. L 281/49 (1995).

2. *Id.*, O.J. L 281/38, at ¶ 10 (1995).

3. *Id.*, art. 5-21, O.J. L 281/39 (1995).

4. *Id.*, art. 3, O.J. L 281/39 (1995).

5. *Id.*

6. *Id.*, art. 31, O.J. L 281/49 (1995). DPAs can order blocking, erasure or destruction of data; impose a ban; admonish a controller; engage in legal proceedings or notify judicial authorities where there have been violations. They may also hear claims lodged by any person who feels his or her rights have been violated.

that met EU independence requirements.⁷ In a high-profile referral, the Commission referred the UK to the European Court of Justice for “not fully implementing EU rules on the confidentiality of electronic communications such as e-mail or internet browsing.”⁸

Data privacy violators face multiple sources of sanctions. First, the country, through a DPA or judicial authority, can impose fines, imprison violators, or both.⁹ Second, EEA citizens who have suffered damage when protected data has been processed unlawfully have a private right of action and can sue civilly.¹⁰

The European Commission was active in 2010 in calling for modification and updating of the EU data protection laws and procedures. On November 4, 2010, the Commission announced that it would “propose in 2011 a new general legal framework for the protection of personal data in the EU covering data processing operations in all sectors and policies of the EU.” It released on the same day a document titled “A comprehensive strategy on data protection in the European Union,” in which it outlined areas that it felt could be improved.¹¹ The Commission took comments on its website until January 15, 2011.¹² The European Data Protection Supervisor (“EDPS”) issued an opinion on the Commission’s document on January 14, 2011.¹³ The EDPS listed a number of its own recommendations. *Id.*

2. Personal Data Defined

The EU Directive restricts access to and use of personal data created or received by an employee. “Personal data” in the EEA has a much broader scope than in the United States. The EU Directive defines “personal data” as “any information relating to an identified or identifiable natural person (‘data subject’).”¹⁴ Although the precise definition of personal data varies among the EEA countries, personal data is any data that permits the identification of an individual, either directly or indirectly, through means “likely reasonably” to be used by either the data controller or a third party.¹⁵ This includes information that is not considered “personal” in the United States, such as job titles, office locations and e-mail addresses, but which is considered “personal” in EEA countries because it can be linked to a

7. <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1430&format=HTML&aged=0&language=EN>.

8. <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215>.

9. *Id.*, art. 24, O.J. L 281/45 (1995).

10. *Id.*, art. 23(1), O.J. L 281/45 (1995).

11. http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm;
<http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/542&format=HTML&aged=0&language=EN&guiLanguage=fr>.

12. *Id.*

13. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

14. *Id.*, art. 2(a), O.J. L 281/38 (1995).

15. Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of Personal Data (012480/07/EN WP 136) (June 20, 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

person whom -- in the language of the Data Protection Directive -- "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."¹⁶

In the United States, we generally associate the phrase "personal data" with a limited set of data such as medical information and social security numbers. In Europe these types of data are considered "sensitive data," and are even more highly protected than "personal data." Sensitive data includes information of a highly personal nature, that reveals an individual's race, ethnicity, political opinion, religious or philosophical beliefs, trade union membership, mental or physical health, sex life, criminal convictions, civil judgments or sanctions.¹⁷ Under Article 8 of the EU Directive, Member States and data controllers are prohibited from processing sensitive personal data, subject to some very limited exceptions.¹⁸

3. "Processing" Within the Meaning of the EU Directive

The EU Directive applies to a wide range of activities, one of which is "processing." "Processing" is defined broadly as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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."¹⁹ This definition encompasses essentially every action taken in connection with U.S. discovery.²⁰ In the United States, "processing" is understood generally to relate to such technical actions as conversion from one format to another, de-duplication, culling, filtering, indexing and sampling.

Under the EU Directive, a "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" is a data controller.²¹ Data controllers can be entities or employees charged with making decisions regarding the processing of personal data. Data controllers must implement measures to protect personal data from accidental or unlawful

16. *Id.*

17. Council Directive No. 95/46/EC, art. 8(a) and 9(5)-(6), O.J. L 281/40, (1995).

18. Sensitive personal data may be processed where (i) the data subject has given explicit consent, (ii) the controller cannot meet its employment law obligations without doing so, (iii) it is necessary to the vital interests of a data subject (or another person), and the data subject is physically or legally incapable of giving consent, (iv) it is carried out by a non-profit organization whose aim is to advance an agenda related to one of the categories of sensitive data, (v) the data subject makes the data public, (vi) it is needed to establish or defend a legal claim, or (vii) it is required by a health professional in the course of managing treatment or health care services. *Id.*, art. 8, O.J. L 281/40 (1995).

19. *Id.*, art. 7(b), art. 2(b), O.J. L 281/40, 38 (1995).

20. See Working Document 1/2009 on pre-trial discovery for cross-border civil litigation ("WP 158"), at 8.

21. Council Directive No. 95/46/EC, art. 7(b), art. 2(d), O.J. L 281/1 (1995). See also Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (00264/10/EN WP 169) (Feb. 16, 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf).

destruction or loss, alteration or unlawful disclosure or access.²² Many key provisions of data privacy laws focus on the data controller's conduct and action. These are discussed below.

Principles Concerning Data Quality. Article 6 of the EU Directive articulates five data quality principles that govern processing of personal data.²³ Data controllers must take steps to ensure that the processing of personal data is:

- (a) Fair and Lawful – processed fairly and lawfully;
- (b) Purpose-Limited – “collected for a specific, explicit and legitimate purpose and not further processed in a way that is incompatible with those purposes”;
- (c) Relevant in Scope – deemed “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”;
- (d) Accurate and Current – personal data must be accurate and up-to-date, and every reasonable step must be taken to ensure that inaccurate or incomplete data (in terms of the purposes for which they are collected or processed) are erased or rectified; and
- (e) Time-Limited – “kept in a form that permits data subjects to be identified for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.”

In addition to the principles of finality, legitimacy and proportionality that the provisions embody, “transparency” is key to the proper handling of personal data. The EU Directive requires employers to notify employees that data about them is being collected, and provide them with (1) the identity of the controller and its representative, if any, (2) the intended purpose of the processing, and (3) any additional information, such as the recipients' identities, the need to respond to questions relating to the processing, and the rights to obtain updates from the controller on the processing, to make updates to the data being processed, and to have the controller notify third parties of those updates.²⁴ Importantly, employers must disclose if the data will be transferred outside the EEA.

Criteria for Legitimate Data Processing. The EU Directive prohibits processing of personal data except when one or more of the following conditions set forth in Article 7 are met.

- (a) Consent – Personal data can be processed if the data subjects “unambiguously” provide “informed” and “voluntary” consent.²⁵ It may be very difficult to

22. Barbara Crutchfield George, Patricia Lynch & Susan J. 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, n. 81 (2001).

23. Council Directive No. 95/46/EC, art. 6(1)(a)-(e), O.J. L 281/40 (1995).

24. *Id.*, art. 10, art. 11, O.J. L 281/41 (1995); Working Party, Opinion 8/2001 on the processing of personal data in the employment context (5062/01/EN WP 48), at 3 (Sept. 13, 2001), <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf>.

25. Council Directive No. 95/46/EC, art. 7(a), O.J. L 281/40 (1995).

obtain the consent of all the data subjects. For example, in order to process email, a data controller may need to obtain consent not only from the custodian of the email, but also from each and every sender or recipient of each email, including, perhaps, bcc addressees who may only be identified by the email's metadata. Even if the difficult identification hurdle can be overcome, another may prove insurmountable. This is because in certain countries employees may not be able to provide "unambiguous" consent as a matter of law.²⁶

(b) Performance of a Contract Involving a Data Subject – Personal data may be processed if "necessary to the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering a contract."²⁷ The provision applies to processing that is necessary to achieve the specific purpose of the contract.

(c) Compliance with Legal Obligations – Personal data may be processed when "necessary for compliance with legal obligations to which the controller is subject."²⁸ (As discussed below in section B, EEA countries generally do not recognize discovery obligations imposed by the United States or other non-EEA jurisdictions as "legal obligations" sufficient to allow the processing of personal data.)²⁹

(d) Protection of Data Subject's Vital Interests – Personal data may be processed when "necessary in order to protect the vital interests of the data subject."³⁰

(e) Tasks Carried Out in the Public Interest – Personal data may be processed "when necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the control or in a third party to whom the data are disclosed."³¹

(f) Controller or Third Party's Legitimate Interests – Personal data may be processed "when 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)."³² (Similar to the situation concerning compliance with legal obligations, EEA countries generally do not recognize

26. Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (2093/05/EN WP 114), at 11 (Nov. 25, 2005), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf.

27. Council Directive No. 95/46/EC, art. 7(b), O.J. L 281/40 (1995).

28. *Id.*, art. 7(c), O.J. L 281/40 (1995).

29. WP 158, at 9.

30. Council Directive No. 95/46/EC, art. 7(d), O.J. L 281/40 (1995).

31. *Id.*, art. 7(e), O.J. L 281/40 (1995).

32. *Id.*, art. 7(f), O.J. L 281/40 (1995).

discovery obligations imposed by United States or other non-EEA jurisdictions as “legitimate interests” of data controllers that would justify processing personal data.)³³

4. Transfer of Personal Data to Third Countries

Although the EU Directive does not actually define the term “transfer,” it is understood to be construed broadly to include any transmittal of personal data, whether paper or electronic, whether transmitted by post or electronically. To ensure that controllers do not circumvent the EU Directive’s protections by transferring data outside of the EU for processing, the EU Directive expressly prohibits the transfer of personal data to non-EEA countries, except in limited circumstances.³⁴

There are three categories of exceptions to the general prohibition against transfer of personal data outside of the EEA. It is useful to think of these as country-based, corporate-based and condition-based.

Country-Based Exceptions: There are two types of country-based exceptions. One arises when the European Commission has made a finding that a non-EEA country has adequate data privacy protections in place. (The European Commission has only made that finding with respect to a handful of countries.) The other arises from a program in place in the United States called the “Safe Harbor” program.

1. *Third Country Adequacy Findings.* Article 25 of the EU Directive permits transfers “where the third country in question ensures an adequate level of protection.”³⁵ The European Commission determines whether a particular non-EEA country provides an adequate level of protection. To date, the Commission has made adequacy findings (to which EEA countries are bound) with respect to only a handful of non-EEA countries: Switzerland (July 2000), Canada (December 2001 (for data subject to the Canadian Personal Information Protection and Electronic Documentation Act)), Argentina (June 2003), the Bailiwick of Guernsey (November 2003), the Isle of Man (April 2004) the Bailiwick of Jersey (2008), Andorra (2010), the Faroe Islands (2010).³⁶ The Commission does not view the United States as having adequate protections in place for the transfer of data. Thus, Article 25 does not provide a basis for the transfer of personal data to the United States for any purpose.

2. *United States Safe Harbor Program.* The European Commission permits transfers of personal data to the United States in accordance with the Safe Harbor Privacy Principles of the United States Department of Commerce (July 2000) (the “Safe Harbor Program”). The Safe Harbor Program was developed by the Commerce Department in consultation with the European Commission to permit the data transfer to U.S. entities

33. WP 158, at 9.

34. Data Protection Unit of the Directorate-General for Justice, Freedom and Security, *Frequently Asked Questions Relating to Transfers of Personal Data From The EU/EEA to Third Countries*, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf, at 18.

35. Council Directive No. 95/46/EC, art. 25, O.J. L 281/45 (1995).

36. http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm

that self-certify that they have implemented internal data practices consistent with the United States - EU Safe Harbor framework.³⁷ The seven Safe Harbor key principles are:

(1) Notice, which must be given to data subjects regarding the purpose and use of the collection;

(2) Choice, meaning data subjects must be able to opt out of the processing or use of personal data that is incompatible with the purpose for which it was originally collected;

(3) Onward transfer to third parties may occur only where the transferee is Safe Harbor-certified or executes a written agreement to provide at least the same level of privacy protection as is required by the relevant Safe Harbor principles, or where the transfer is otherwise allowed by the data privacy laws;

(4) Data subjects have the same "right to access" their data as they have under the EU Directive;

(5) Security measures are taken to protect data from loss, misuse or unauthorized access, disclosure, alteration or destruction;

(6) Data integrity is preserved (*i.e.*, personal data must be relevant to the purposes for which it is to be used and the organization must ensure the data's reliability); and

(7) Rigorous enforcement of the Safe Harbor requirements to ensure compliance by the organization.

The Safe Harbor program is recognized only by EU Member States and does not apply to Norway, Iceland and Lichtenstein. In addition, German data protection authorities have imposed additional requirements that must be met in order to transfer data to a Safe Harbor-certified entity in the United States.³⁸

Switzerland and the United States have entered into a Safe Harbor protocol for the transfers of certain types of data from Switzerland to the United States.³⁹ Only companies that fall within the jurisdiction of the Department of Commerce may participate, so telecommunication and financial companies are ineligible.

Corporate-Based Exceptions: Data transfers to third countries that do not provide an adequate level of protection are generally permitted if businesses adopt either standard contractual clauses or binding corporate rules.

1. *Standard Contractual Clauses (also referred to as "model contracts").* Pursuant to Article 26(4) of the EU Directive, the European Commission has promulgated

37. For a list of American companies that have been certified as safe harbor participants, see Safe Harbor List (2010), <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>.

38. See http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile (English translation not yet available).

39. See Safe Harbor Overview (2010), http://www.export.gov/safeharbor/eg_main_018236.asp.

approved contractual clauses permitting personal data transfer to processors in non-EEA countries.⁴⁰ In 2010, the European Commission revised these clauses to better reflect business realities,⁴¹ and published a set of frequently asked questions addressing the application of the new clauses.⁴² These clauses bind the parties to a set of rules that track the principles of the Safe Harbor framework. The clauses also provide that the contracting party is liable for any damage suffered by the data subject (who is deemed a third-party beneficiary to the contract) as a result of that party's breach. Despite the Commission's pre-approval of this method to allow transfer of data to non EEA countries, some DPAs may still require companies to obtain specific approval of the contract from the relevant DPA before the company may effect the transfer.⁴³

2. *Binding Corporate Rules.* Multinational companies may make intra-company data transfers from an EEA country to the United States using binding corporate rules ("BCRs"). BCRs are similar to Safe Harbor provisions, but rather than governing external transfers to a particular organization, the rules govern internal transfers within an organization, such as between corporate groups within a company or between parents, subsidiaries, and sister companies in the same corporate group.⁴⁴ To ensure that a company's BCRs provide an adequate level of privacy, most DPAs typically require that the company submit its BCRs to the DPA for approval, a process that can take some time. Once approved, personal data may transfer freely throughout an organization. Although several European countries appear receptive to the use of binding corporate rules, their use is still relatively rare. For example, as of January 2011, only seven companies in the UK had BCRs approved, and generally in the context of the transfer of human resources and personnel data: General Electric, Koninklijke Philips Electronics NV, The Amtel Corporation, Accenture Limited, the Hyatt Hotel Corporation, JP Morgan Chase & Co. and British Petroleum plc.⁴⁵

Condition-Based Derogations Under Article 26(1): There are six conditions which, if met, would permit the transfer of personal data outside of the EEA.

(a) Consent – Personal data transfers may occur when the data subject unambiguously consents;⁴⁶

(b) Performance of a Contract Involving a Data Subject – Personal data may be transferred if "necessary to the performance of a contract between the data subject

40. http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm.

41. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF>.

42. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_en.pdf.

43. http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm.

44. See Brandon Cook, *Why Cross-Border Litigation is a Compliance Concern*, Sarbanes-Oxley Compliance Journal, May 21, 2009, http://www.s-ox.com/dsp_getNewsDetails.cfm?CID=2599.

45. See the Information Commissioner's Office, http://www.ico.gov.uk/for_organisations/data_protection/overseas/binding_corporate_rules.aspx.

46. Council Directive No. 95/46/EC, art. 26(a), O.J. L 281/46 (1995).

and the controller or the implementation of precontractual measures taken in response to the data subject's request;⁴⁷

(c) Conclusion of the Performance of a Contract – Personal data may be transferred if it “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;”⁴⁸

(d) Public Interest or Legal Claims – Personal data may be transferred when “necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;”⁴⁹

(e) Data Subject's Vital Interests – Personal data may be transferred “in order to protect the vital interests of the data subject;”⁵⁰ or

(f) Transfer from Public Register – Personal data may be transferred 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.”⁵¹

B. Working Party Opinion WP 158: Applying the EU Directive To U.S. Discovery Obligations

The Article 29 Working Party (the “Working Party”), issued in February 2009 the *Working Document 1/2009 on pre-trial discovery for cross-border civil litigation* (“WP 158”).⁵² WP 158 purports to address the issues of cross-border discovery head-on and to offer guidance to data controllers presented with conflicting discovery demands.⁵³ Notably, the Working Party suggests that there are three possible grounds to legitimize transfers to the U.S. of personal data for civil litigation purposes: consent; “compliance with a legal obligation” (Article 7(c)); and “furtherance of legitimate interest” under Article 7(f) -- a significant departure from prior views. The Working Party also suggests that data may be transferred to the United States for litigation purposes via BCRs and the Safe Harbor provisions. While the Working Party document is welcome and important, it does not eliminate the difficulties U.S. litigants face in producing European personal data. Key points of WP 158 are summarized below.

47. *Id.*, art. 26(b), O.J. L 281/46 (1995).

48. *Id.*, art. 26(c), O.J. L 281/46 (1995).

49. *Id.*, art. 26(d), O.J. L 281/46 (1995).

50. *Id.*, art. 26(e), O.J. L 281/46 (1995).

51. *Id.*, art. 26(f), O.J. L 281/46 (1995).

52. The Working Party on the Protection of Individuals with regard to Processing of Personal Data is authorized by Article 29 of the EU Directive to oversee implementation of the EU Directive in the EEA, to address data protection issues and to issue recommendations, non-binding opinions and working documents to provide guidance in formulating appropriate and consistent data protection practices. It is comprised of, among others, representatives of the data protection authorities that oversee compliance with privacy legislation in the EEA countries. Council Directive No. 94/46/EC, art. 29, O.J. L 281/47 (1995).

53. WP 158, at 1-7.

With respect to the legitimate “processing” of personal data (Article 7), the Working Party:

- Observed that each “stage” of discovery (retention, disclosure, onward transfer, and secondary use) constitutes processing of personal data within the meaning of the EU Directive and that each stage must meet a condition under Article 7 in order to legitimize the processing of personal data. This includes suspending document retention policies pursuant to a litigation hold.⁵⁴
- Noted that data controllers are not legally obligated to retain personal data for an unlimited time. If the controller has a clear policy that requires the retention of records for a short period of time, the failure to preserve this information will not be deemed to have violated United States law. If the personal data is relevant and to be used in a specific or imminent litigation process, it should be retained until the conclusion of the proceedings and any appeal period. Data retention for purposes of future litigation can only be justified under Article 7(c) or 7(f) of the EU Directive, but the Working Party declared that the “mere or unsubstantiated possibility that an action may be brought before the US courts is not sufficient.”⁵⁵
- Reiterated its prior view that a foreign legal obligation does not qualify under Article 7(c), adding that a foreign legal obligation might arise “in the Member States to comply with an order of a foreign court seeking discovery,” *e.g.*, under the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, 1970 T.I.A.S. 7444, codified at 28 U.S.C. § 1781 (“Hague Evidence Convention”), although it recognized the effect of Article 23 Reservations (in which the adopting country declares that the procedures set forth in the Hague Convention are applicable only to trial evidence, and not pre-trial discovery).⁵⁶
- Suggested that where a country has opted out of the Hague Evidence Convention, “compliance with the litigation process may be found to be necessary for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed under Article 7(f).” This basis is only acceptable where the controller’s legitimate interests do not override the data subject’s fundamental rights and freedoms, and where the controller employs a “balance of interest test based upon proportionality, the relevance of the personal data to the litigation and the consequence for the data subject” and ensures adequate safeguards to protect the data.⁵⁷
- Emphasized the data subject’s right to object under Article 14 of the EU Directive where processing is based on a data controller’s or third party’s legitimate interest under 7(f), in the absence of national legislation, by presenting compelling

54. *Id.* at 8.

55. *Id.* at 8.

56. *Id.* at 6.

57. *Id.* at 10.

legitimate grounds relating to his or her situation. If there is a justified objection, data processing must stop.⁵⁸

- Observed that consent waivers under Article 7(a) are problematic in the U.S. discovery context because consent must be “freely given, specific and informed”⁵⁹ and must be obtained not only from a custodian, but from any data subject whose personal information is contained within the custodian’s files. Thus, a data controller would have to show that it notified not only its own employees but also any third parties whose personal data was contained within the information sought.⁶⁰ Further, each data subject would have the right to object to the processing of data and, in some instances, block it.⁶¹ Consent too may be revoked at any time, which is not feasible in U.S. litigation.⁶² With respect to sensitive personal data, WP 158 states that consent is the only legal basis upon which processing may occur.

- Suggested as an initial step that data controllers “restrict disclosure if possible to anonymised or at least pseudonymised data. After filtering (‘culling’) the irrelevant data – possibly by a trusted third party in the European Union – a much more limited set of personal data may be disclosed as a second step.”⁶³ The Working Party acknowledged it might be difficult to identify a trusted third party.

With respect to the legitimate transfer of personal data, the Working Party:

- Suggested that the EU Directive “does not prevent transfers for litigation purposes,” but cautioned that controllers must comply with certain data protection requirements in such transfers.⁶⁴

- Urged litigants “to involve the data protection officers from the earliest stage,” although it is not clear from the opinion if this refers to company-appointed data protection officers, or those at the DPAs.⁶⁵

- Encouraged EU data controllers to approach U.S. courts and educate them regarding data protection requirements and request appropriate protective orders that comply with the data privacy laws.

- Suggested using Binding Corporate Rules or the Safe Harbor Program “[w]here a significant amount of data is to be transferred.”⁶⁶

58. *Id.* at 12.

59. Council Directive No. 95/46/EC, art. 2(h), O.J. L 281/39 (1995).

60. WP 158, at 8.

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.* at 7.

65. *Id.* at 11.

- Reiterated its earlier opinion that Art. 26(1)(d) (transfer is necessary for the defense of legal claims or on important public interest grounds) cannot be used to justify the transfer of all employee files to a group's parent company on the grounds of the possibility that legal proceedings may be brought one day in U.S. Courts.⁶⁷
- Recognized "that compliance with a request made under the Hague Convention would provide a formal basis for a transfer of personal data," acknowledging though that not all Member States are signatories, and those that are may have signed with an Article 23 Reservation.⁶⁸
- Stated that the Hague Evidence Convention is the preferred method of providing for transfer of information for litigation purposes even though the time associated with Hague procedures falls outside the normal timeframe for U.S. pretrial discovery.

The Working Party paper states that, even with a proper basis for the transfer of personal data, controllers must balance the basis against the data subject's rights and ensure the use of adequate safeguards for the processing of the data subject's personal data. This means compliance with Article 6's fair processing principles and the implementation of adequate safeguards, including all reasonable technical and organizational precautions relating to security of the data and the imposition of these precautions on anyone involved in the litigation who has access to the data. These are discussed throughout WP 158 and include:

- transparency, by notifying individuals in advance of the possible use of their data for litigation, and, where the personal data is actually processed for litigation, notifying the data subject of the identity of the recipients, the potential uses of the data, the categories of data concerned and the existence of the data subject's rights in connection with that processing;⁶⁹
- notice to the data subjects of their right to object to processing under Article 14, which means the data controller must also provide information concerning the right to object on compelling legitimate grounds, the existence, purpose and functioning of the data processing, and the data subject's right to access, rectify and erase personal data under Article 12;⁷⁰
- culling to separate relevant and irrelevant information in order to reduce the set of personal data that will be disclosed;⁷¹ and

66. *Id.* at 13.

67. *Id.* at 13, citing WP 114, at 15.

68. WP 158, at 13.

69. *Id.* at 11.

70. *Id.* at 10, 12, and 18.

71. *Id.* at 10.

- culling by a trusted EU third party to reduce further the number of personal records to be processed.⁷²

Notably, the Working Party opted not to address the “control of the use, for litigation purposes, of personal data which has already been properly transferred for example to the United States for other reasons under BCR or Safe Harbor.”⁷³

C. Blocking Statutes

Another obstacle to cross-border discovery, wholly separate from the data protection issues discussed above is the existence in some countries of “blocking statutes,” that restrict or prohibit the transfer of documents for use in foreign proceedings unless the transfer is the result of compliance with the Hague Evidence Convention.

Chapter 1 of the Hague Evidence Convention permits evidence to be transmitted to other countries via “letters of request” issued by the court where the action is pending to the “Central Authority” of the jurisdiction where the discovery is located, which then forwards the letters to domestic judicial authorities competent to execute them.⁷⁴ This process can be lengthy, and may be impractical in many cases. Chapter 2 of the Convention allows for a duly-appointed commissioner or other official to obtain a set of documents voluntarily agreed to by the parties and transfer them to a foreign jurisdiction for use in foreign proceedings. This process can be much shorter, and is increasingly being used by litigants in U.S. courts.

Even if parties in U.S. litigation agree to use the Hague Evidence Convention, however, there are limitations. For example, nearly three-quarters of the EEA signatories have exercised their rights under the Convention’s Article 23 provision not to execute letters of request that seek evidence in connection with pre-trial discovery in common law countries (known as an “Article 23 Reservation”),⁷⁵ or to limit the requests they will honor to only specifically-tailored requests that seek narrowly defined categories of information.⁷⁶

One well known blocking statute is France’s Law 80-538, enacted on July 6, 1980, which amended Law 68-678, enacted on July 26, 1968. That statute imposes criminal penalties, including imprisonment, on parties who, among other things, transmit outside of the Hague Evidence Convention process “documents or information relating to economic, commercial, industrial, financial or technical matters” for use in foreign judicial or administrative proceedings.

72. *Id.*

73. WP 158, at 7.

74. BUSINESS AND COMMERCIAL LITIGATION § 18:92 (2d ed. 2005 & Supp. 2009-2010).

75. EEA signatories that have made Article 23 Reservations include Bulgaria, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Lithuania, Luxembourg, Monaco, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, and the United Kingdom of Great Britain and Northern Ireland. See http://www.hcch.net/index_en.php?act=conventions.status&cid=82.

76. BUS. AND COMM. LIT., *supra* note 74, § 18:92, at n.19.

While on the books for decades, France had not enforced the blocking statute until recently. Partly for that reason, the United States Supreme Court held in *Société Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa* that the French blocking statute did not “deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute.” 482 U.S. 522 (1987). The Supreme Court stated that U.S. Courts should balance a number of factors in deciding whether to order cross-border discovery. *Id.* at 544-47. These factors include: (1) the importance of the documents or information requested to the litigation; (2) the degree of specificity of the request; (3) whether the information requested originated in the U.S.; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the U.S., or compliance with the requests would undermine important interests of the state where the information is located. *Id.* The U.S. Courts have overwhelmingly required production notwithstanding blocking statutes. (see e.g. *Accessdata Corp. v. ALSTE Tech. GMBH*, 2010 WL 3184777 (D. Utah Jan. 21, 2010), *In re Air Cargo Shipping Svcs. Antitrust Litig.*, No. 06-MD-1775, 2010 WL 1189341, at *5 (E.D.N.Y. Mar. 29, 2010), *In re Global Power Equip. Group, Inc.*, 418 B.R. 833 (Bankr. D. Del. 2009) and *Filler v. Lernout (In re Lernout & Hauspie Sec. Litig.)*, 218 F.R.D. 348 (D. Mass. 2003)) Many wondered whether U.S. courts would reach a different conclusion after the case of *In re Christopher X*, Cour de Cassation, Chambre Criminelle, Dec. 12, 2007, 07-83.228), where criminal sanctions were imposed on an attorney for asking an individual for substantive information in connection with U.S. discovery efforts. It appears that the Christopher X case has not had a dramatic impact on the reported decisions of U.S. courts.

D. Best Practices

Unfortunately, notwithstanding the suggestions of WP 158, the European Commission has yet to adopt a universal resolution to the EEA/United States discovery conflict. Until both sides of the Atlantic can agree on an approach that meets European privacy and U.S. discovery needs, we recommend the following best practices to help corporate entities, whether multinational or not, prepare for and handle the challenges of cross-border litigation.

Before a Legal Duty Arises

- ❖ Implement company-wide computer usage policies that appropriately shape employees’ privacy expectations (e.g., informing employees that work e-mail may be subject to preservation and collection in response to legal obligations and suggesting a non-work e-mail address be used for personal matters).
- ❖ Implement document retention policies that retain email and other electronic documents for only as long as the business determines is necessary.
- ❖ Consider whether the U.S. operations have access to European data that they do not need. Such data is more likely to be ordered produced in U.S. litigation because it may be found to already exist in the United States.
- ❖ Consider implementing a data management plan that addresses key mandates of the EU Directive and/or specific European privacy laws to minimize the possibility of personal data violations, by
 - (i) informing data subjects during their initial employment orientation of possible processing and transfer activity in connection with the

management of the company or compliance with U.S. legal obligations;

- (ii) creating a data storage system that segregates personal and sensitive personal data so that each can be readily identified as such; and
- (iii) setting up a system that allows personal data to be readily anonymised, pseudonymised or redacted in a way that is compatible with legal obligations.

- ❖ Facilitate a dialogue between the European employees responsible for privacy obligations and the U.S. legal department.

After a Legal Duty Arises

- ❖ Determine whether the information sought is available from a source that does not implicate EEA data protection issues.
- ❖ Engage experienced local counsel familiar with the data privacy and blocking statutes, as well as any other laws that might affect cross-border discovery.
- ❖ Identify and raise EEA privacy issues with your adversary or the agency requesting the data and work to narrow the scope of the request as much as possible.
- ❖ Raise potential discovery issues with the court early on. Memorialize agreements regarding the scope of the discovery request or requests in writing and have the court incorporate them into a discovery order.
- ❖ Involve a company-appointed data protection officer, if there is one, at the foreign entity.
- ❖ Consider using European in-house staff or vendors to assist with discovery-related activities in Europe, consistent with WP 158's suggestion that data controllers are on stronger ground when they have reduced the volume of personal data to be produced as much as possible and transfer only the producible subset of personal data to the United States.
- ❖ Consider using the model agreements for the transfer of data.
- ❖ Separate out personal data from non-personal and process the non-personal first so the court and/or the DPA can see your good faith effort to comply with the EU Directive.
- ❖ Suggest to your adversaries the use of anonymised and pseudonymised versions of the data.
- ❖ Seek protective orders to preserve the confidentiality of produced data.
- ❖ Consider using the Hague Convention Chapter 2 process.

PART II

DATA PROTECTION LAWS BY EEA COUNTRY⁷⁷

Part II identifies, by EEA country, the legislation that implements the EU Directive and other related resources. Importantly, the EU Directive is simply the “floor” below which protection may not fall. The degree of protection, the definition of personal data, the enforcement of violations and sanctions, and the notification requirements to Data Protection Authorities, among other things, vary from country to country. Although beyond the scope of this paper, U.S. discovery may also be limited by national laws called “blocking statutes,” which are designed to prevent the transfer of broadly-defined “nationally sensitive” information in order to protect the sovereignty, and economic and security interests, of the countries from which discovery is sought. Where known, we have indicated whether a country has a blocking statute, and have included related cases for context. Local counsel can be extremely helpful in identifying new and developing law in their countries.

The most current information regarding European data protection laws may be found on internet sites. The internet citations in this section are current as of 1 August 2010. Although these sites are updated periodically, the last revision date will usually be posted. Sometimes, too, a source’s web address will change, in which case the source can usually be located by using the search feature on the site’s home page. In many cases, the smaller European countries do not have English translations of their case law or data protection legislation (particularly blocking statutes).

The following two websites are particularly useful resources:

- Data Protection – European Commission:
http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm – This site includes a copy of the EU Directive, European Court of Justice case law, links to the data protection commissioner websites for each EU country, the Commission decision regarding Model Contracts, the Working Party Opinions regarding transfers to third countries, the status of implementation of the EU Directive in each of the EU countries and links to useful websites such as the United States Safe Harbor list.
- www.privacyinternational.org – This site provides a nation-specific overview of data protection laws.

77. The EEA is comprised of 27 Member States of the European Union as well as Norway, Liechtenstein and Iceland (collectively, the “EEA” or “EEA countries”). The Member States of the EU are: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom (U.K.). See http://europa.eu/abc/european_countries/index_en.htm.

Austria

Relevant Law

- Federal Act Concerning the Protection of Personal Data [1]⁷⁸

The EU Directive has been implemented into Austrian law by the Federal Act Concerning the Protection of Personal Data of 2000, which is enforced by the Austrian Data Protection Commission [1, 2]. Section 13 entitled “Transborder Transmission and Committing of Data Subject to Licensing” contains portions of the EU Directive relevant to cross-border discovery requests [1]. The transfer of personal data to non-EEA countries generally must be approved by the Data Protection Commission unless, for example, the data subject has given consent, the data is being transferred to a country that has guaranteed adequate legal protection, or the data is transferred to a safe harbor company.

For the transfer of data outside the EU, the Austrian Data Protection Commission has approved the use of both binding corporate rules and model contracts [1], although it is not clear whether such data transfers would be permitted for discovery purposes.

Note, too, that in addition to the Federal Act, all nine Austrian Länder (the Austrian federal states) have also adopted data protection laws that implement the EU Directive [3].

Sources

1. Federal Act Concerning the Protection of Personal Data,
<http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.AT> or
<http://www.legislationline.org/download/action/download/id/1501/file/1cb88090fb7b0609e71b35b5a79e.pdf>
2. Austrian Data Protection Commission,
<http://www.dsk.gv.at/site/6248/default.aspx>
3. Status of implementation of EU Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data,
http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm

Belgium

Relevant Laws

- Law on Privacy Protection in Relation to the Processing of Personal Data [1]
- Law of 27 March 1969, as amended on 21 June 1976 [2]

78. Citations in the form “[#]” are to the country-specific sources listed at the end of each country-specific section of this paper.

- Royal Decree of 6 February 1979 concerning the Regulation of Marine and Air Transport [2]
- Article 458 of the Belgium Criminal Code [5]

The EU Directive is incorporated into Belgian law by the Law on Privacy Protection in Relation to the Processing of Personal Data (the “Law on Privacy Protection”). This law, which was promulgated in 1992 and last amended in 2003, is enforced by the Commission for the Protection of Privacy. Most cross-border provisions mirror those of the EU Directive. For example, the Law on Privacy Protection allows parties to transfer protected data pursuant to a contract containing sufficient safeguards. However, if the contract does not track the language of the sample contractual clauses approved by the European Commission, then the contract must be approved by Belgium’s Commission for the Protection of Privacy and authorized by Royal Decree (Belgian law) [4]. Additionally, Belgium allows for data transfers pursuant to binding corporate rules, but the binding corporate rules must be approved by both the Commission for the Protection of Privacy and the Ministry of Justice [3].

In 2003, Belgium’s data protection law and a criminal blocking statute came under scrutiny in *Filler v. Lernout (In re Lernout & Hauspie Sec. Litig.)*, 218 F.R.D. 348 (D. Mass. 2003), when plaintiffs moved to compel defendant KPMG, a Belgian corporation, to produce audit-related papers and other documents located in Belgium. The defendant objected, arguing that producing the documents would violate Belgium’s Law on Privacy Protection and subject it to criminal penalties under Article 458 of Belgium’s Criminal Code. The United States District Court for the District of Massachusetts disagreed, finding Belgium’s data privacy law applied only to personal data, not audit manuals, and further, that the blocking statute would not be violated, because, under the statute, a violation cannot occur where there is a court order to produce documents. Accordingly, the court ordered production of the audit materials.

Sources

1. English translation located at <http://freespace.virgin.net/r.wong253/dpa.html>
2. A. V. Lowe, EXTRATERRITORIAL JURISDICTION 98 (1983)
3. What are the Belgian national conditions for the use of “Binding Corporate Rules” or “BCRs”?, <http://www.privacycommission.be/en/faq/grensoverschrijdende-doorgifte-van-persoonsgegevens/Index14.html>
4. “Cross-Border Transfers of Personal Data,” http://www.privacycommission.be/en/in_practice/grensoverschrijdende_doorgifte_van_persoonsgegevens/
5. *Filler v. Lernout (In re Lernout & Hauspie Sec. Litig.)*, 218 F.R.D. 348, 350 (D. Mass. 2003)
6. Hague Conference on Private International Law, Members of the Organisation, http://www.hcch.net/index_en.php?act=conventions.status&cid=82
7. *In re Vitamins Antitrust Litig.*, 120 F. Supp. 2d 45, 55 (D.D.C. 2000), *amended in part*, Misc. No. 99-197 (TFH), 2000 U.S. Dist. LEXIS 17412 (D.D.C. Nov. 22, 2000)

Bulgaria

Relevant Law

- Personal Data Protection Act [1]

The EU Directive was implemented into Bulgarian law by the Personal Data Protection Act, which was promulgated in 2002 [1]. The Act is regulated by the Bulgarian Commission for Personal Data Protection. Chapter Six of the Act, "Submission of Data to Third Persons," contains provisions governing cross-border data transfers, which mirror those of the EU Directive [1]. Before data may be transferred to a non-EEA country, the Commission for Personal Data Protection determines whether the recipient country provides an adequate level of privacy protection [1]. It is unclear whether data may be transferred out of Bulgaria pursuant to binding corporate rules, however, the use of model contracts appears to be permitted [1].

Sources

1. Law for Protection of the Personal Data, http://www.mvr.bg/NR/rdonlyres/A9C8D2F5-582E-4BED-9710-E175A9AA087F/0/08_Law_Protection_Personal_Data_EN.pdf
2. Bulgaria – Data Protection, www.privireal.org/content/dp/bulgaria.php
3. Privacy International – Bulgaria, <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559501>

Cyprus

Relevant Law

- Law on the Processing of Personal Data (Protection of the Individual) [1]

The EU Directive was implemented into Cyprus law by the Law on the Processing of Personal Data (Protection of the Individual). The law was passed in 2001 and amended in 2003. Section Nine, "Transmission of Data to Third Countries," relates to cross-border data transfers and mirrors the language of the EU Directive [1].

We located only one recent case in which Cyprus's data protection law was raised by a party in response to a document request. *Lasala v. Marfin Popular Bank Pub. Co.*, Civ. No. 09-968 (JAP), 2009 U.S. Dist. LEXIS 69039 (D.N.J. Aug. 7, 2009). In *Lasala*, a money laundering case, the U.S. District Court for the District of New Jersey rejected the defendant's argument that Cyprus's data protection law required a burdensome review of documents before they could be transferred to the United States. Instead, the court concluded there was a risk that the documents would be destroyed (some had already been destroyed) and thus ordered the defendant to preserve and transfer to its U.S. counsel all documents related to the plaintiff's company.

Sources

1. Law on the Processing of Personal Data (Protection of the Individual), as amended,

<http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/d1813d5911e138bdc2256cbd00313d1c/f8e24ef90a27f34fc2256eb4002854e7?OpenDocument>
(select 138-(I)2001_en.pdf and 37-(I)2003_en.pdf)

2. Privacy International -- Republic of Cyprus,
<http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559499>

Czech Republic

Relevant Law

- Personal Data Protection Act 101 [1]

The EU Directive was implemented into Czech law in 2001 by the Personal Data Protection Act 101. The Act is administered by the Office for Personal Data Protection. Chapter III, "Transfer of Personal Data to Other Countries," incorporates the provisions of the EU Directive relevant to cross-border data transfer [1].

Source

1. Consolidated Version of the Personal Data Protection Act,
http://ec.europa.eu/justice/policies/privacy/docs/implementation/czech_republic_act_101_en.pdf

Denmark

Relevant Laws

- Act on Processing of Personal Data [1]
- Act No. 254 of 8 June 1967 on Limitation of Danish Ship Owners' Freedom to Give Information to Authorities of Foreign Countries [2]

The EU Directive was implemented into Danish law by the Act on Processing of Personal Data (Act No. 429), which was passed on May 31, 2000. The Act is enforced by the Danish Data Protection Agency. Chapter Seven of the Act relates to the transfer of personal data to non-EEA countries [1].

Sources

1. Act on Processing of Personal Data, <http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/>
2. A. V. Lowe, EXTRATERRITORIAL JURISDICTION 114 (1983)
3. Privacy International – Kingdom of Denmark,
<http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559545>

Estonia

Relevant Law

- Personal Data Protection Act of 2007 [1]

The EU Directive has been implemented into Estonian law by the Personal Data Protection Act of 2007, which is regulated by the Data Protection Inspectorate. Section 18 of the Act governs personal data transfer to third countries [1]. The Inspectorate must approve transfers of data to non-EEA countries that do not offer adequate levels of protection and transfers generally require the data subject's consent [1]. Company-appointed data protection officers are not required by law, but entities that do appoint them may process *sensitive* personal data without registering with the Inspectorate [1].

Sources

1. Personal Data Protection Act, English translation located at <http://www.aki.ee/eng/?part=html&id=105> (select Personal Data Protection Act link) (unofficial)
2. Privacy International – Estonia, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559541](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559541)

Finland

Relevant Laws

- Finnish Personal Data Act [1]
- Law Prohibiting a Ship Owner in Certain Cases to Produce Documents, 4 January 1968 [2]

The EU Directive has been incorporated into Finnish law by the Finnish Personal Data Act (523/1999). The Act was passed in 1999 and is regulated by the Office of the Data Protection Ombudsman. Chapter Five, entitled "Transfer of Personal Data to Outside the European Union," contains language that mirrors the EU Directive provisions regarding data transfers to third countries [1]. The use of model contracts is permitted by the Finnish Data Protection Act [1].

Sources

1. Finnish Personal Data Act, English translation located at <http://www.tietosuoja.fi/uploads/hopxtvf.HTM>
2. A. V. Lowe, EXTRATERRITORIAL JURISDICTION 115 (1983)
3. Privacy International – Republic of Finland, <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559538>

France

Relevant Laws

- Law No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties as amended by Law 2004-801, of 6 August 2004 relating to the Protection of Data Subjects as Regards the Processing of Personal Data [1]
- Law No. 68-678 of 27 July 1968, amended by Law No. 80-538 (the “1980 Blocking Statute”) [2]

The EU Directive was incorporated into French law with Law No. 2004-801 of 6 August 2004 relating to the Protection of Data Subjects as Regards the Processing of Personal Data (Law 2004-801). Generally, before personal data may be transferred to a non-EEA country without adequate privacy protections, express authorization must be obtained from the Commission Nationale de l’Informatique et des Libertés (CNIL), the French Data Protection Agency (although a recent CNIL opinion suggests that a declaration may be sufficient, *see below*). Chapters VII and VIII of Law 2004-801 set out sanctions for breaches of the law, which include fines of up to 300,000 euros (although there is pending legislation to increase the fine to 600,000 euros, discussed below) and imprisonment. With respect to cross-border processing and transfers, Law 2004-801 appears to track the privacy protections set forth in the EU Directive.

Workplace Privacy. In France, the right to privacy in the workplace is grounded in French civil and labor laws and the Convention for the Protection of Human Rights and Fundamental Freedoms [7]. Criminal law too, prohibits any kind of tampering with a third party’s hard copy or electronic communications [7]. The French Supreme Labor Court recognized workplace privacy rights in the landmark case, *Nikon France v. Onof*, Cass. soc., Oct. 2, 2001, No. 99-42942, which held that an employee has a right to privacy at the workplace, with respect to his personal life, even during work, and the employer could not search the personal messages the employee had stored on the company’s computer without breaching that right. Since then the Court has refined the law regarding workplace privacy to include a requirement that employees identify as “personal” documents that they wanted treated as personal; otherwise, unidentified documents are presumptively professional in nature. *See Bruno B. v. Giraud et Migot*, Cass. soc., Dec. 15, 2009, 07-44264 (where the French Supreme Labor Court ruled that, notwithstanding the employee’s right to privacy, a French company was justified in accessing correspondence on an employee’s computer that was not clearly identified as personal).

Based upon *Bruno*, it has been suggested that unidentified documents would be more accessible to parties to U.S. litigation because an employer could review them without an employee’s consent. This conclusion, however, does not sufficiently take into account the differences between internal French employment disputes and cross-border discovery.

Transfers of Personal Data to the United States. With respect to personal data transfer, the first use of the CNIL’s enforcement power under Law 2004-801 occurred in 2007, when the CNIL fined Tyco Healthcare France – the local subsidiary of the U.S. Tyco – \$40,000 for unlawfully transferring human resources data to Tyco’s U.S. headquarters without adopting binding corporate rules or Safe Harbor certification.

With respect to U.S. discovery, any transfer of documents from France to the United States requires satisfaction of the EU Directive’s data privacy principles regarding

processing and transfer, and could be impeded by the 1980 blocking statute, discussed *infra*. A CNIL opinion issued in July 2009 (the “Opinion”) provides practical guidance for the discovery of material subject to French jurisdiction. Regarding processing and transfer of data, the Opinion reiterates the importance of complying with the Hague Convention and French data protection laws, but also articulates, among other considerations, the data controller’s responsibilities, the significance of applying legitimacy and proportionality principles to the processing and transfer of personal data, and the rights of the data subjects.

With respect to personal data transfers to the United States, the CNIL suggests designating a corporate data protection officer to assist in navigating French data protection laws [5], and consulting a third party to determine whether data requests are proportional to the needs of the litigation [5]. Where there is a significant amount of data at issue, pseudonyms or other procedures shall be used to render data anonymous, thereby avoiding disclosure of personal information that is not necessary for the litigation [5]. (This approach may be unnecessary if the data disclosure is limited [5]). Further, large and repeated transfers of data are permissible when the recipient of the data is a United States entity that adheres to the Safe Harbor principles of the United States-EU Safe Harbor framework, when the data recipient has signed a contract containing standard contractual clauses approved by the European Commission, or when the data recipient has set up binding corporate rules [5]. Although the use of standard contractual clauses and binding corporate rules are contemplated in the context of transfers that occur during an entity’s normal course of business, the July 2009 Opinion suggests they can be applied for U.S. litigation purposes as well [5].

The Blocking Statute. France’s data privacy statute is not the only obstacle to U.S. discovery in France. The Blocking Statute requires that foreign discovery proceed through applicable international conventions - usually the Hague Evidence Convention - and imposes fines or imprisonment for violations [2]. It is routinely raised in connection with U.S. pre-trial discovery requests of French-held documents, but federal courts most often order disclosure notwithstanding the Blocking Statute, citing the United States Supreme Court’s decision in *Société Nationale Indust. Aérospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522 (1987) (French blocking statute is not a bar to discovery because the Hague Evidence Convention is not the exclusive means of obtaining discovery and therefore does not preempt the Federal Rules of Civil Procedure in foreign discovery matters). Many wondered whether U.S. courts would reach a different conclusion after the case of *In re Christopher X*, Cour de Cassation, Chambre Criminelle, Dec. 12, 2007, 07-83.228), where criminal sanctions were imposed on an attorney for asking an individual for substantive information in connection with U.S. discovery efforts. It appears that the Christopher X case has not had a dramatic impact on the reported decisions of U.S. courts. See, e.g., *In re Global Power Equip. Group, Inc.*, No. 06-11045, 2009 WL 3464212 (Bankr. D. Del. Oct. 28, 2009).

Pending Legislation. It has been reported that the French Senate is currently considering legislation that would impose greater data privacy obligations on data controllers. The proposed law, entitled “Law to Better Guarantee Privacy in the Digital Age” would amend France’s data privacy law, Law No. 78-17 of 6 January 1978, as amended. Key provisions include, among others: 1) doubling the top fine for a data privacy violation to 600,000 euros (currently roughly \$808,000), 2) expanding the definition of “personal data” to include internet protocol addresses, 3) requiring companies with more than 50 employees that have access to and process personal data to appoint a data protection officer, and 4) making it clear that data subjects have the right to object to the collection or processing of data for commercial purposes and the right to delete their data at any time, even after collection and processing [6].

Sources

1. English translation located at <http://www.cnil.fr/english/> (select Official Text link)
2. Law No. 80-538 of July 16, 1980, Journal Officiel de la Republique Francaise, July 17, 1980
3. The Sedona Conference, International Overview of Discovery, Data Privacy and Disclosure Requirements, Sedona Conference Working Group Series (2009), at 88
4. Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, Internet Update 2.0/April 2008, <http://www.oup.com/uk/booksites/content/9780199283859/updates/1704200813>
5. CNIL, *Deliberation No. 2009-474 of 23 July 2009 concerning recommendations for the transfer of personal data in the context of American court proceedings known as 'Discovery'*, http://www.cnil.fr/fileadmin/documents/en/D-Discovery_EN.pdf
6. Rick Mitchell, *French Bill Proposes Breach Notification Requirement That Goes Beyond EU Measure*, Privacy Law Watch, <http://www.pdfchaser.com/Clippings---BNA-Privacy-Law-Watch---French-Bill-Proposes-Breach-....html>
7. Art. 6 of the French Civil Code, Art. L.1121-1 of the French Labor Code (former Art. L. 120.2), Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Articles 226-15 and 432-9 of the French Criminal Code

Germany

Relevant Laws

- Federal Data Protection Act (Bundesdatenschutzgesetz), as amended [1]
- Telecommunications Regulations (blocking statute) [3]
- Maritime Shipping Law, §§11 and 17 (blocking statute) [4]

Germany implemented the EU Directive with the Federal Data Protection Act, effective May 2001 and amended September 1, 2009. Germany has one of the strictest privacy policies in the world, and each of the sixteen Länder (federal states) has a unique policy. For example, German data protection authorities have imposed additional requirements that must be met in order to transfer data to a Safe Harbor-certified entity in the United States.⁷⁹

79. See http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile. (English translation not yet available).

In stark contrast to U.S. discovery rules, German law generally does not require litigants to disclose documents to the other party [4]. Litigants need only produce documents that support their claims, and if the documents are not contested the court will accept them as fact [6]. German authorities will permit very limited discovery of documents from third parties if the U.S. court sends a letter of request for specific documents that are needed to resolve an issue and the U.S. court proceeding is already pending [4].

The 2009 amendments to the Federal Data Protection Act require companies to report an abuse or loss of sensitive data to the relevant German supervising authority as well as the person(s) involved [5]. Fines for serious data privacy breaches were increased to 300,000 euros [5]. It is not yet clear whether these amendments permit employee personal data to be processed for discovery purposes. Binding corporate rules may be used as a means by which to guarantee adequate privacy protection [8].

Discovery of workplace e-mails in Germany is particularly challenging. The Federal Data Protection Act limits the use of nearly all employee personal data, defined to include many employee e-mails [4]. If an employer permits employees to use their computers at work for private communication then those communications are likely protected from discovery [4]. The distinction between private and employment-related is often difficult to make and it is unclear how much of an employee's e-mails would ultimately be filtered out for privacy reasons in a discovery proceeding [4].

Litigants in U.S. courts who have objected to producing documents on Federal Data Protection Act grounds have had mixed success. In two cases, U.S. courts declined to compel document production when defendants raised as an objection the Federal Data Protection Act, violation of which constitutes a criminal offense in Germany for which one can be fined (50,000 Euros to 300,000 euros per violation) or imprisoned [7]. *In re Vitamins Antitrust Litig.*, Misc. No. 99-197 (TFH), 2001 U.S. Dist. LEXIS 8904, at *52-54 (D.D.C. June 20, 2001) (where court found the Act presented legitimate privacy law concerns and stated that "individuals have a presumptively legitimate interest under German law in the nondisclosure of their personal information to residents of countries with non-equivalent personal data protection standards"); *Salerno v. Lecia, Inc.*, 97-CV-973S(H), 1999 U.S. Dist. LEXIS 7169, at *10-11 (W.D.N.Y. Mar. 23, 1999) (where court declined to compel the European defendants to produce severance package information because there were serious legal ramifications for violations of the EU Directive and the Federal Data Protection Act). However, in *Accessdata Corp. v. ALSTE Tech. GMBH*, 2010 WL 3184777 (D. Utah Jan. 21, 2010), the United States District Court for the District of Utah ordered defendant to produce German data after conducting its own "brief review" of the Federal Data Protection Act and concluding that (i) a provision of the Act permitted the production of personal data with the data subject's consent or "for the establishment, exercise or defence of legal claims" (*Id.* at 2.), and (ii) the defendant had not demonstrated that it had been unable to obtain, or even attempted to seek, consent, let alone addressed the provision or explained why it did not apply in this particular case.

Germany has at least one blocking statute, the Federal Maritime Shipping Act of May 24, 1965, which was enacted to frustrate attempts by the United States Federal Maritime Commission to gather information from shipping lines concerning allegations of anti-competitive practices [3].

Sources

1. English translation of Federal Data Protection Act (Bundesdatenschutzgesetz), http://www.bfdi.bund.de/clin_118/EN/DataProtectionActs/DataProtectionActs_nod

- [e.html](#), amendments located at <http://dip21.bundestag.de/dip21/brd/2009/0536-09.pdf> (English translation of amendments not yet available)
2. Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 Hastings L.J. 751, 770, n.110 (2003), citing the German Constitution, Article 10(1) §10 Nr. 1 GG
 3. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES, § 442, cmt. Reporter's note 4 (citing to Federal Republic of Germany: Federal Maritime Shipping Act of May 24, 1965, Art. 11, [1965] Bundesgesetzblatt pt. II 833, 835). The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts, Sedona Conference Working Group Series (2008), at 16
 4. The Sedona Conference, International Overview of Discovery, Data Privacy and Disclosure Requirements, Sedona Conference Working Group Series (2009)
 5. Germany Introduces Stricter Privacy Laws - Impact on Database Marketing, <http://www.biaa.com/library/German%20Data%20Protection%20Law%20Hits%20Direct%20Marketing.docx.pdf>
 6. Erica M. Davila, *International E-Discovery: Navigating the Maze*, http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=erica_davila
 7. HR European news roundup - September 2009, http://www.expatica.com/de/employment/employment_information/HR-European-news-roundup--September-2009_14706.html
 8. Christoph Klug, *Improving self-regulation through (law-based) Data Protection Officials*, Deputy Executive Director of the German Association for Data Protection and Data Security (GDD), at 5

Greece

Relevant Laws

- Law 2472/1997 on the Protection of Individuals with Regard to the Processing of Personal Data (Data Protection Act) [1]
- Law 3471 Protection of personal data and privacy in the electronic telecommunications sector and the amendment of law 2472/1997 [1]

The EU Directive was implemented into Greek law in 1997 by the Law on the Protection of Individuals with Regard to the Processing of Personal Data (Data Protection Act), which was most recently amended in 2009. The Act is enforced by the Data Protection Authority. The Act's relevant privacy provisions mirror those found in the EU Directive [1].

Sources

1. Data Protection Act and amendment, English translations located at http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL (select Download Law 2472/1997 and Download Law 3471/2006)

2. Privacy International -- Greece,
<http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559534>

Hungary

Relevant Laws

- Act No. LXIII of 1992 on Protection of Personal Data and Disclosure of Public Information [1]
- Act IV of 1978 on the Criminal Code (blocking statute) [2]

The EU Directive is incorporated into Hungarian law by Act No. LXIII of 1992 on the Protection of Personal Data and the Disclosure of Public Information. The Act is enforced by the Parliamentary Commissioner for Data Protection and the Freedom of Information. Act IV of 1978 on the Hungarian Criminal Code provides for sanctions and punishment for the misuse of personal data [2]. Transfers of data to non-EEA countries is permitted under Act No. LXIII of 1992 using binding corporate rules [3]. Company-appointed data protection officers are required only if an organization's data relates to a specified sector including public utility providers, telecommunications service providers, and others [1].

Sources

1. Act No. LXIII of 1992, <http://abiweb.obh.hu/adatved/indexek/AVTV-EN.htm>
2. Act IV of 1978 on the Criminal Code, Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information, http://abiweb.obh.hu/dpc/index.php?menu=gyoker/relevant/national/1978_IV
3. Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information, Binding Corporate Rules, <http://abiweb.obh.hu/dpc/index.php?menu=reports/2006/4/10>
4. Privacy International – Republic of Hungary, <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559531>

Iceland

Relevant Law

- Act No. LXIII of 1992 on Protection of Personal Data and Disclosure of Public Information [1]

Although Iceland is not a member of the EU, it is a member of the EEA and the EU has determined that, as an EEA state, Iceland provides adequate protection to data and permits the flow of information from Iceland without additional safeguards [2]. Iceland's Act No. 77/2000 on the Protection of Privacy, enacted January 1, 2001, implements the EU Directive in Iceland. The Act is enforced by the Icelandic Data Protection Authority ("IDPA"), and overseen by the Data Protection Commissioner [3].

Sources

1. <http://www.personuvernd.is/information-in-english/greinar//nr/438>
2. Commission Decisions on the Adequacy of Data Protection in Third Countries, European Commission, http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm
3. <http://www.personuvernd.is/information-in-english/greinar//nr/437>

Ireland

Relevant Law

- Data Protection Act 1988/ Data Protection Act Amendment 2003 [1]

The EU Directive was incorporated into Irish law by the 2003 amendment to the Data Protection Act 1988, the primary Irish law dealing with data protection. The Act is enforced by the Office of the Data Protection Commissioner. The provisions in Section Twelve of the amendment, entitled, "Restriction on Transfer of Personal Data Outside State," apply to cross-border data transfer and mirror the provisions of the EU Directive [1]. The Data Protection Commissioner recommends using model contracts when transferring data to a third country [2].

Sources

1. Data Protection Amendment (2003), <http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html>
2. Data Protection Commissioner, Model Contracts, <http://www.dataprotection.ie/viewdoc.asp?DocID=38>

Italy

Relevant Law

- Consolidation Act Regarding the Protection of Personal Data, Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code) [1]
- Law No. 488 of July 24, 1980 (prohibiting transfer of documents regarding maritime activities) (blocking statute) [2]

The EU Directive was implemented into Italian law by the Consolidation Act Regarding the Protection of Personal Data, Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code). The relevant parts of the Personal Data Protection Code do not differ substantially from the EU Directive. Title VII of the Personal Data Protection Code deals with "Transborder Data Flows" [1]. According to Section 43 of Title VII, "personal data" may be transferred out of Italy only when a) the data subject has given consent, b) "the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party," c) "to establish or defend a legal claim, provided that the data are transferred exclusively for said purposes and for no longer than is necessary therefore in compliance with the legislation in force applying to business and industrial secrecy," or d) "if the processing concerns data relating to legal persons, bodies or

associations" [1]. Additionally, Section 44 permits the transfer of processed personal data to a non-EU member state if such transfer has been authorized by the Italian regulatory agency, Garante per la protezione dei dati personali ("Garante"), whose authorization is contingent upon the Garante's finding that adequate contractual safeguards are in place or the non-member state provides sufficient privacy safeguards [1]. Such safeguards include binding corporate rules and model contracts [4]. Contractual clauses that differ from the European Commission model contracts can be used once the Garante has determined that they offer the data subject's rights of adequate protection [1]. Italy does not require the appointment of data protection officers [4].

Beyond the Personal Data Protection Code, Italy has reserved its right under Article 23 of the Hague Evidence Convention to refuse to issue Letters of Request in connection with pre-trial discovery in common law countries [5]. One U.S. court, however, held that the Federal Rules of Civil Procedure should apply where Italy refuses to comply with discovery based upon its Article 23 declaration. *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, Case No. 04 C 3109, 2005 U.S. Dist. LEXIS 20049, at *17 (N.D. Ill. Sept. 12, 2005). Another court has noted that Italy's Article 23 declaration does not bar all cross-border discovery requests, and that the Italian courts must decide whether sufficiently specific requests or those that have been deemed relevant by the requesting court would be permissible. *In re Baycol Prods. Litig.*, 348 F. Supp. 2d 1058 (D. Minn. 2004).

Sources

1. Italian Data Protection Code,
<http://www.garanteprivacy.it/garante/document?ID=311066>
2. ABA Section of Antitrust Law, *Obtaining Discovery Abroad* (2005), p. 169.
3. Privacy International – Italian Republic,
[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559525](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559525)
4. Authorisation for the Transfer of Personal Data to Third Countries in Compliance with Standard Contractual Clauses – 10 October 2001,
<http://www.garanteprivacy.it/garante/doc.jsp?ID=1669728>
5. The Sedona Conference, *Framework for Analysis of Cross-Border Discovery Conflicts*, Sedona Conference Working Group Series (2008)

Latvia

Relevant Law

- Personal Data Protection Law [1]

The EU Directive was implemented into Latvian law by the Personal Data Protection Law, which was last amended in 2009. The law is enforced by the Data State Inspectorate. Similar to the EU Directive, personal data may be transferred out of Latvia only if the recipient country provides adequate protection or: (i) if consent of the data subject is obtained; (ii) if the transfer of the data is necessary in order to fulfill an agreement between the data subject and the data controller; or (iii) if the transfer of the data is necessary and requested under the set procedure in accordance with significant national and public interests, or is necessary for litigation [1]. Since 2008, the Data State Inspectorate has allowed personal data to be processed without notifying it as long as the

data controller has a data protection officer [2]. Violations of the Personal Data Protection Law are punishable by fines of up to approximately 14,000 Euros (\$20,000) [2].

Sources

1. Personal Data Protection Law, English version located at <http://www.dvi.gov.lv/eng/legislation/pdp/>
2. Twelfth Annual Report of the Article 29 Working Party on Data Protection, European Commission, June 16, 2009, p. 60
3. Privacy International – Republic of Latvia, <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559521>

Liechtenstein

Relevant Laws

- Data Protection Act of 14 March, 2002 [1]
- Ordinance on the Data Protection Act [2]

Liechtenstein implemented the EU Directive with the Data Protection Act in March of 2002 and the Ordinance on the Data Protection Act in July of 2002. The Data Protection Commissioner (Datenschutzbeauftragter) (“DPC”) supervises compliance with the Data Protection Act. The DPC must be notified of any foreign data transfer if there is no legal obligation to disclose the data and the persons affected have no knowledge of the transmission [1]. Standard contractual clauses may be used for third country business-related transfers but the DPC must be notified [2]. Data controllers are exempt from registering with the Data Protection Commissioner if they appoint a data protection officer [2].

Sources

1. English translation located at <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.LI#transfer>
2. English translation located at www.llv.li/pdf-llv-dss-dpo-fl_en_2009-11-30.pdf

Lithuania

Relevant Law

- Law on Legal Protection of Personal Data [1]

Lithuania implemented the EU Directive during its efforts to secure EU membership with the Law on Legal Protection of Personal Data (“LPPD”), most recently amended in April 2004 [1]. The State Data Protection Inspectorate supervises and monitors compliance with the LPPD [2]. In most cases, authorization from the State Data Protection Inspectorate is required for data transfers to third countries that do not provide adequate levels of protection. Data may be transferred to a third country without adequate protection if the contract that governs the transfer specifies the requirements for the safeguarding of

personal data [1]. The State Data Protection Inspectorate has not officially recognized binding corporate rules, but when used, they are looked upon favorably [2].

Sources

1. Law on Legal Protection of Personal Data,
<http://www.ada.lt/images/cms/File/pers.data.prot.law.pdf>
2. Privacy International – Lithuania,
[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559520](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559520)

Luxembourg

Relevant Law

- Amended Act of 02 August 2002 concerning the protection of individuals with regard to the processing of “personal data” (“Data Protection Act”) [1]

Luxembourg implemented the EU Directive when it enacted the Data Protection Act of 2002 (“DPA”), which was amended by the Law of 27 July 2007 [1]. Administration of the DPA is handled by the Commission Nationale pour le Protection des Données (CNPD) [1]. Transfer of data out of Luxembourg is allowed if the CNPD determines that the data controller offers sufficient guarantees in respect to the protection of the privacy, freedoms and fundamental rights of the data subjects [1]. Transfers by model contracts must be authorized by the CNPD [1]. The CNPD has permitted the use of binding corporate rules for cross-border data transfers in the business context [1]. Violations of the third party personal data transfer provisions of the DPA are punishable by up to one year in prison and a fine of 125,000 Euros [1].

Sources

1. Amended Act of 02 August 2002 (“Data Protection Act”),
www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf
2. Privacy International – Luxembourg,
[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559519](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559519)

Malta

Relevant Law

- Data Protection Act (Act XXVI of 2001) [1]

Malta incorporated the EU Directive into its national laws by enacting the Data Protection Act of 2001 (DPA) [1]. The Office of the Data Protection Commissioner is charged with the supervision and enforcement of the DPA. The Commissioner recommends the use of model contracts and has approved the use of binding corporate rules [2].

Sources

1. Data Protection Act, <http://idpc.gov.mt/dbfile.aspx/DPAen.pdf>

2. Office of the Data Protection Commissioner, Transfer of data to a third country, <http://idpc.gov.mt/article.aspx?art=121>
3. Privacy International – Malta, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559516](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559516)

The Netherlands

Relevant Laws

- Personal Data Protection Act [1]

The Data Protection Directive is implemented in The Netherlands by (1) the Personal Data Protection Act of 2000 (“PDPA”). The PDPA is a revised and expanded version of the Data Registration Act of 1998 and regulates the disclosure of personal data to third countries. The Dutch Data Protection Authority (College Bescherming Persoonsgegevens or “CBP”) supervises and regulates compliance with the PDPA [2]. Under the PDPA, transfers can take place if the transfer satisfies general conditions for data processing, which track those found in the EU Directive [3]. Data export to third countries is permitted by model contracts with a permit from the Dutch Minister of Justice [3]. Data protection officers are not required, but if appointed, companies may be exempt from the general requirement to notify the CBP of data processing [4].

In *Columbia Pictures Indus. v. Bunnell*, CV 06-1093 FMC(JCx), 2007 U.S. Dist LEXIS 46364, at *59-60 (C.D. Cal. May 29, 2007), the court found that U.S. defendants intentionally placed their servers in The Netherlands essentially to benefit from the protections of the broad definition of “personal data” which they believed included server log data, including users’ internet protocol (IP) addresses. Plaintiffs moved for an order to preserve and produce this data and defendants objected on the grounds that the PDPA prohibited them from doing so. *Id.* at *48. The court disagreed noting that IP addresses identified computers, not the individuals using the computers, and thus might not be protected under the PDPA. The court further noted that PDPA did not deprive the court of its power to order the parties subject to its jurisdiction to produce or preserve evidence. *Id.* at *49. The court did caution, however, that the holding of this case was extremely fact specific.

Sources

1. Personal Data Protection Act, http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml (select “read the unofficial translation”)
2. Privacy International – Kingdom of The Netherlands, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559513](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559513)
3. Dutch DPA, Your Data Data Processing Activities and Transfer to Third Countries, http://www.dutchdpa.nl/Pages/en_inf_contr_Transfer_3d_Countries.aspx#1
4. Dutch DPA, the Data Protection Officer, http://www.dutchdpa.nl/Pages/en_inf_subj_Data_Prot_Officer.aspx#2

5. Marc J. Gottridge & Thomas Rouhette, *Blocking Statutes Bring Discovery Woes*, New York Law Journal, Apr. 30, 2008, <http://www.law.com/jsp/cc/PubArticleCC.jsp?id=900005634407>

Norway

Relevant Law

- Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act) [1]

Although Norway is not a member of the EU, it is an EEA country and thus has implemented the EU Directive by enacting the Personal Data Act of 2000 ("PDA"), which was amended in 2008. The amendment added a new chapter regarding monitoring of employee e-mail. Enforcement of the PDA is overseen by the Data Inspectorate (Datatilsynet) [2].

Sources

1. Personal Data Act, <http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf>
2. Privacy International – Norway, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559510](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559510)

Poland

Relevant Law

- Act of August 29, 1997 on the Protection of Personal Data [1]

Poland implemented the EU Directive by enacting the Act of August 29, 1997 on the Protection of Personal Data ("PDA") [1]. The amendments that came into force on May 1, 2004, the day of Poland's accession into the EU, brought the original 1997 PDA into full compliance with the EU Directive [2]. The Inspector General is charged with overseeing compliance with the PDA. Transfers to third countries may take place with prior consent from the Inspector General, provided that the data controller assures there will be adequate safeguards [1].

Sources

1. Act on the Protection of Personal Data, http://ec.europa.eu/justice/policies/privacy/docs/implementation/poland_en.pdf
2. Privacy International – Republic of Poland, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559594](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559594)
3. Privacy Law in Poland, <http://privacylaw-poland.com>
4. Poland: Data Protection, <http://www.privireal.org/content/dp/poland.php>

Portugal

Relevant Law

- EU Directive implemented by Law 67/98 of 26.10.1998 [1]

Portugal was one of the first countries in western Europe to incorporate the EU Directive when it implemented Law 67/98 in 1998 [2]. This law replaced the existing Portuguese data protection rules, which were set out in Law No. 10/91 of April 1991, as amended by Law No. 28/94 of August 1991. The National Data Protection Commission (Comissão Nacional de Protecção de Dados or “CNPD”) oversees compliance with the Act. With very limited exceptions, the CNPD must authorize all data transfers to countries outside the EEA unless they are made pursuant to model contracts [1].

Sources

1. Data Protection Act, <http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM>
2. Maria L. Lopes, *Portugal Adopts Data Protection Legislation*, Nov. 22, 2006, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1611
3. Privacy International – Republic of Portugal, <http://www.privacyinternational.org/survey/phr2000/countrieshp.html#Heading21>
4. eGovernment Factsheet: Portugal, <http://www.epractice.eu/en/document/288343>

Romania

Relevant Laws

- Law No. 677/2001 of 21st of November 2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data [1]
- Law No. 102/2005 Regarding the Setting Up, Organisation and Functioning of the National Supervisory Authority for Personal Data Processing [2]

Romania incorporated the principles embodied in the EU Directive into its national law in Law No. 677/2001 (“PDL”). Because the PDL was implemented when Romania was in the process of reforming its law to join the EU, the provisions of the PDL follow those of the EU Directive very closely [3]. Compliance with the PDL is ensured by an Ombudsman, also known as The People’s Advocate. Personal data processing is also monitored by the National Supervisory Authority for Personal Data Processing (“PDP”) [4]. Ombudsman Order No. 6 of January 29, 2003 provides a template for contractual agreements with countries that do not provide adequate privacy protection [5]. As recently as 2008, Romania was considering permitting the use of binding corporate rules in accordance with Article 29 Working Party guidelines although it is not yet clear that their use has been approved yet [6].

Sources

1. Law on Protection of Individuals with Regard to Processing of Personal Data, http://ec.europa.eu/justice/policies/privacy/docs/implementation/ro_law_677_2001_en_unofficial.pdf
2. Law Establishing Supervisory Authority, http://ec.europa.eu/justice/policies/privacy/docs/implementation/ro_law_102_2005_en_unofficial.pdf
3. eGovernment Factsheet: Romania, <http://www.epractice.eu/en/document/288406>
4. Central and Eastern Europe Data Protection Authorities Web Site, Romania, <http://www.ceecprivacy.org/main.php?s=2&k=romania>
5. Privacy International – Romania, <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83786>
6. National Supervisory Authority for Personal Data Processing Annual Report, 2008, www.dataprotection.ro/servlet/ViewDocument?id=550

Slovakia

Relevant Law

- Act No. 428/2002 Coll. on Protection of Personal Data [1]

Act No. 428/2002 Coll. on the Protection of Personal Data (“PPD”) implements the EU Directive in Slovakia. It was adopted in September of 2002 and amended in 2005 [2]. The language of the PPD closely tracks the language of the EU Directive with respect to processing and transfer to non-EEA countries [1]. The Commissioner for the Protection of Personal Data oversees compliance with the PPD [2]. It is unclear whether the PPD permits data controllers to rely on model contracts for transferring data to third countries, however data processing in third countries is permitted [1].

Sources

1. Act on Protection of Personal Data, http://ec.europa.eu/justice/policies/privacy/docs/implementation/slovakia_428_02_en.pdf
2. Slovakia – Data Protection, <http://www.privereal.org/content/dp/slovakia.php>
3. Privacy and Human Rights, <http://gilc.org/privacy/survey/survey1z.html>

Slovenia

Relevant Laws

- Personal Data Protection Act of the Republic of Slovenia [1]

- Information Commissioner Act [2]

The Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*, UL RS No. 86/2004 *et seq.*, "ZVOP-1"), which was adopted in July 2004 and effective in January 2005, implements the EU Directive [1]. Personal data transfers outside of the EEA are permitted where: (i) provided by statute or binding international treaty; (ii) made with the data subject's consent; (iii) necessary for the performance of a contract relating to the data subject; (iv) necessary to protect the vital interests of the data subject; or (v) made from a public register [1]. Personal data can also be transferred to a non-EEA country if Slovenia's National Supervisory Body for Personal Data Protection decides the receiving country offers an adequate level of protection [1]. The Information Commissioner is in charge of overseeing application of the Personal Data Protection Act and has the authority to levy fines in the case of any unauthorized disclosures [2]. There is not yet any official guidance on the use of corporate binding rules for personal data transfer to third countries.

Sources

1. Personal Data Protection Act,
http://ec.europa.eu/justice/policies/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf
2. Information Commissioner Act,
http://ec.europa.eu/justice/policies/privacy/docs/implementation/information_commissioner_act_2005.pdf
3. Privacy International – Slovenia,
<http://www.privacyinternational.org/survey/phr2003/countries/slovenia.htm>
4. eGovernment Factsheet: Slovenia,
<http://www.epractice.eu/en/document/288361>
5. Privacy and Human Rights – Slovenia,
<http://gilc.org/privacy/survey/survey1z.html>

Spain

Relevant Laws

- Ley Orgánica 15/99 de 13 de Diciembre 1999 (December 13, 1999) de Protección de Datos de Carácter Personal (translation: Organic Law 15/1999 of 13 December on the Protection of Personal Data) [1]
- Royal Decree 1720/2007 [2]

Spain incorporated the EU Directive into its law with the Organic Law 15/1999 of 13 December on the Protection of Personal Data ("LOPD") in 1999, effective January 14, 2000 and further refined by the Royal Decree 1720/2007. The new Act succeeded and amended the 1992 Data Protection Act, Spain's first privacy law. The *Agencia de Protección de Datos* ("APD") enforces the Data Protection Act and provides guidance to ensure compliance with it. If a model contract is used, then the parties must seek prior approval from the Director of the APD [2]. Spanish law classifies data as either "low", "medium" or "high" security depending on the nature of the data [2]. Companies are required by

Spanish data regulations to appoint a data protection officer when processing data classified as “medium” or “high” security data according to Spain’s national privacy legislation [2].

Although the provisions relating to cross-border transfer are analogous to those in the EU Directive, the Spanish courts have debated whether an employee’s e-mails belong to the employer (and are therefore discoverable) or to the employee (and not discoverable) [3].

Sources

1. Data Protection Act,
https://www.agpd.es/portalwebAGPD/english_resources/regulations/index-iden-idphp.php (select “ORGANIC LAW 15/1999”)
2. https://www.agpd.es/portalwebAGPD/english_resources/regulations/index-iden-idphp.php, (select “Royal Decree 1720/2007”)
3. Privacy International – Spain,
<http://www.privacyinternational.org/survey/phr2003/countries/spain.htm>
4. The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts, Sedona Conference Working Group Series (2008)

Sweden

Relevant Laws

- Personal Data Act SFS 1998:204 of 29.4.98 [1]
- Regulation SFS 1998:1191 of 03.09.98 [2]
- Ordinance Regarding Prohibition in Certain Cases for Ship Owners to Produce Documents Concerning the Swedish Shipping Industry (1966) (Svensk Forfattningssamling No. 156, at 411) (blocking statute) [5]

Sweden enacted the Personal Data Act (“PDA”) of 1998 to conform its privacy law to the EU Directive. Some portions of the PDA were enacted in October of 1998 and others were enacted in stages until October of 2001 when the law finally went into full effect. The PDA replaced the Data Act of 1973, which was the first comprehensive national act on privacy in the world [3]. Section 33 of the PDA was amended in 1999 to adopt the EU Directive standards on the transfer of personal data to third countries. The amendment facilitates transfer of data through international communication networks, like the Internet [3]. The Data Inspection Board (Datainspektionen or DIB) oversees enforcement of the PDA. The DIB permits use of model contracts [1]. Although data protection officers are not required, companies that appoint them do not need to notify the DIB of their data transfers [1].

Sweden has implemented a set of rules governing the processing of what’s known as unstructured material [6]. Under these rules most of the provisions of the PDA do not apply when processing personal data in unstructured material, *i.e.*, data that is not included in or intended to be included in a document or case management system or any other database [6]. This can include personal data in e-mails, as well as word processing documents, sounds, images, etc. For example, lists of names, such as pupils in a class or

the names of board members may be handled without adherence to the Personal Data Act [7]. These regulations are intended to prevent misuse of data processing [3]. Such processing is permitted so long as it does not violate the integrity of the data subject's privacy [6]. In 2007, the rule was amended to address criticism that Sweden's data protection laws were too complicated for anyone to follow [7]. It remains to be seen whether the unstructured material rule will succeed in simplifying Sweden's data protection laws.

Additionally, Sweden has enacted blocking statutes to prohibit compliance with extraterritorial discovery demands if compliance may harm a domestic industry [5]. The Ordinance Regarding Prohibition in Certain Cases for Ship Owners to Produce Documents Concerning the Swedish Shipping Industry (1966) (Svensk Forfattningssamling No. 156, at 411) was enacted by Sweden in response to a United States investigation of alleged anticompetitive practices in the global shipping industry [5].

Sources

1. Personal Data Act, <http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/> (select Personal Data Act and Personal Data Ordinance pdf links)
2. SFS 1998:1191 of 03.09.98, <http://www.sweden.gov.se/sb/d/574/a/25633> (select "Personal Data Ordinance")
3. Privacy International – Sweden, <http://www.privacyinternational.org/survey/phr2003/countries/sweden.htm>
4. "Blocking Statutes Bring Discovery Woes," <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1209459934853>
5. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES, § 442, cmt. Reporter's note 4
6. Personal Data Protection: Information on the Personal Data Act, Ministry of Justice, Sweden, www.regeringen.se/content/1/c6/07/43/63/0ea2c0eb.pdf
7. Privacy International, PHR2006 - Kingdom of Sweden, <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559487>

United Kingdom

Relevant Laws

- Data Protection Act 1998 [1]
- United Kingdom's Protection of Trading Interests Act 1980 (c. 11) (blocking statute) [2]
- Privacy and Electronic Communications Regulations 2003 [3]

The U.K.'s Data Protection Act of 1998 ("DPA") incorporates the EU Directive into its national law. The DPA, like the EU Directive, adheres to the processing principles found in the EU Directive. Despite the DPA regulations, however, the U.K.'s broad discovery

rules more closely mirror U.S. rules and thus, in certain respects, conflict with the EU Directive's restrictive approach. For example, pursuant to Civil Procedure Rule 31.6, a U.K. litigant must disclose: (1) documents relied upon, (2) documents that adversely affect or support the litigant's own case or another party's case, and (3) documents that are required to be produced by a Practice Direction (Practice Directions are instructions that compliment the Civil Procedure Rules and are meant to achieve uniformity in the practice of U.K. law) [4]. Further, Rule 31 was amended in 2005 to include within the definition of "document," electronic documents, including e-mail and other communications, word-processed documents and databases, documents stored on servers and back-up systems, deleted documents, and metadata [4]. However, under the Practice Directions to U.K. Civil Procedures, disclosure requests must be reasonable, which depends on such considerations as the breadth of the requests, the complexity of the proceeding, and the accessibility of the documents [4]. Notably, in 2008, in *Digicel v. Cable and Wireless*, [2008] EWHC 2522 (CH), ¶¶ 40-43, 56-69, the U.K. court took note of discovery standards found in recent U.S. case law in resolving a discovery dispute involving electronic data located in Europe and the Caribbean. In doing so, it redefined the scope of what is reasonable and greatly expanded the amount of electronic material that is considered reasonably discoverable.

Personal data, too, is defined more narrowly in the U.K. than in other European countries. Recently, a U.K. court defined as personal data, data that "affect[s] the [data subject's] privacy, whether in his personal or family life, business or professional capacity." *Durant v. Fin. Servs. Auth.*, [2003] EWCA 1746 (Civ). This definition excludes, however, insignificant biographical data such as the incidental presence of a data subject's name in board minutes or the mere presence of a data subject's name in an address line of an e-mail [5], which falls within the definition of personal data under the EU Directive.

The European Commission has questioned the U.K.'s implementation of the EU Directive and is pressuring it to increase its privacy protections [6]. In April 2009, the European Commission formally warned the U.K. that it had breached the EU Directive after receiving complaints from U.K. internet users about British Telecom's ("BT") use of a targeted advertising program that tracked the internet activities of some of BT's customers on a trial basis without their consent [7]. This warning followed an earlier warning regarding the definition of "consent" in the U.K.'s Privacy and Electronic Communications Directive (EC Directive) Regulations 2003 (PECR) and the Regulatory and Investigatory Powers Act (2000). In October 2009, the Commission moved to the second stage of the procedure by issuing a letter to the U.K. government [7]. In 2010, the Commission referred the UK to the European Court of Justice for "not fully implementing EU rules on the confidentiality of electronic communications such as e-mail or internet browsing." [8]. The U.K. also applies the Hague Evidence Convention differently from most European signatories. Most countries entertain pre-trial discovery requests under the Convention after the filing of a claim and up to a final hearing on the merits [9]. Under U.K. law, litigants may begin requesting information using the Hague Evidence Convention when the filing of a claim is merely likely, and do not have to wait until a claim has actually been filed, thereby broadening the scope of data that can be discovered in the U.K. beyond the scope allowed by other EEA states [9]. In 2010, the fine for data protection breaches increased one hundredfold, from £5,000 to £500,000 [10].

In the U.K., although there are no blanket provisions prohibiting discovery, the U.K. Secretary of State has the authority under the Protection of Trading Interests Act 1980 (c. 11), a U.K. blocking statute, to give instructions precluding discovery in certain instances if it conflicts with the U.K.'s trading interests or infringes upon U.K. sovereignty [2].

Sources

1. Data Protection Act 1998,
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
2. http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1980/cukpga_19800011_en_1
3. <http://www.opsi.gov.uk/si/si2003/20032426.htm>
4. The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts, Sedona Conference Working Group Series (2008)
5. "The 'Durant' case, and its impact in the interpretation of the Data Protection Act 1998, Information Commissioner's Office,"
http://docs.google.com/viewer?a=v&q=cache:ya-N3cx2oEgJ:www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf+The+%E2%80%98Durant%E2%80%99+case,+and+its+impact+in+the+interpretation+of+the+Data+Protection+Act+1998,+Information+Commissioner%E2%80%99s+Office&hl=en&gl=us&sig=AHIEtbS8NaFi5-o5YzKbF1fTk2vrtImhyQ
6. Clare Dyer, ed. "Europe's Concern over the UK Data Protection Revealed," The Guardian (2007), <http://www.guardian.co.uk/uk/2007/oct/01/eu.humanrights>
7. EU deems UK privacy laws inadequate, takes legal action, Nov. 1, 2009
http://en.wikinews.org/wiki/EU_deems_UK_privacy_laws_inadequate,_takes_legal_action
8. See <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215>.
9. Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery on cross-border civil litigation (00339/09/EN WP 158) (Feb. 11, 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf, at 6
10. See http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf

CONCLUSION

For now, multinational businesses may face a “Catch-22,” *i.e.*, comply with one set of rules while possibly violating another. The realities of international business, however, are forcing policymakers and practitioners on both sides of the Atlantic to look closely at these issues in search of a solution, one that will likely require some sort of multi-lateral treaty for the collection of electronic evidence abroad. Currently, a dialog is underway between members of the Sedona Conference’s Working Group 6 on International Electronic Information Management, Discovery and Disclosure and the Working Party. Until a viable solution is reached, corporations with a presence in both the United States and an EEA country should review current records management policies and corporate IT structures for potential exposure, and work with key members of IT, Legal and Human Resource departments to develop and implement practices that mitigate the risks associated with processing and transferring foreign personal data, both in the business and litigation contexts.

hugheshubbard.com

Hughes Hubbard & Reed LLP | One Battery Park Plaza | New York, New York 10004-1482 | 212-837-6000

Ethics rules require this to be labeled attorney advertising. Readers are advised that prior results do not guarantee a similar outcome.

© 2011 Hughes Hubbard & Reed LLP