

white paper

communicate

When Worlds Collide:

**Suggested Best Practices for
Navigating European Data Protection Laws in
U.S. Litigation**

July 2009

Introduction

With the rise of globalization, the multinational corporation is now a well-established fixture on the corporate landscape. Whether the corporation is based in the United States, with operations abroad, or headquartered overseas with a presence in the United States, there is an ever-growing likelihood that counsel and their corporate clients will have to respond to an action that, although arising in the United States, will require the collection, review, and possible production of materials located abroad.

For example, an internal investigation triggered by the Sarbanes-Oxley Act¹ or Foreign Corrupt Practices Act² might require cross-border information gathering. Similarly, a company might need to review information maintained abroad in an effort to respond to an antitrust investigation or grand jury proceeding. Or a company might need to access and produce materials kept in a foreign location to respond to discovery in a U.S.-based action. Managing the complexities associated with these types of matters can always pose a challenge, but grappling with these kinds of challenges can be especially problematic if the information needed is kept in Europe, where various rules and regulations can greatly restrict access to and the use of employee and company data.

To address these issues, this White Paper examines in detail the European Union Data Protection Directive³ and in the process provides an overview of related national enabling legislation. In addition, this paper broadly outlines other potentially relevant sources of law, including nationally enacted blocking statutes and other rules and regulations that should be considered by U.S. counsel when seeking to obtain information housed in a company's European facilities.⁴ As part of that examination, this paper addresses the issues raised when in-house or outside counsel seeks to obtain and use data that resides in Europe so that he or she can (1) respond to U.S. discovery or governmental investigatory demands; (2) manage an internal company investigation; or (3) have access to records for use in the ordinary course of business or to meet business needs.

Little published case law or official guidance exists directly addressing these issues, especially with respect to accessing data located overseas in the context of an adversarial proceeding in the United States. Moreover, the relevant laws of foreign nations, and official interpretations of those laws by either courts or state-sanctioned bodies known as Data Protection Authorities, remain works in progress. As a result, there are few definitive, bright-line rules that can be applied.

In examining questions pertaining to the application and scope of European data protection laws, three overarching issues need to be kept in mind as we discuss the

1 15 U.S.C. §§ 7201-66 and 15 U.S.C. § 78m(k).

2 15 U.S.C. §§ 78dd-1 et seq.

3 Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personnel Data and on the Free Movement of Such Data (O.J. 95/L281) (the EU Directive).

4 Because of the number of possible sources of rules affecting discovery in the United States of data residing in Europe, we recommend that local counsel be consulted in any such circumstances.

issues examined in this paper and recommend how to create the strongest case possible for accessing data abroad for use in the United States:

- **Whether the EU Directive and the related enabling legislation would consider business records stored in Europe to be “personal data.”** To address this issue, we have examined the definition of key terms found in the relevant statutory materials. We conclude that although some room may remain to argue that certain types of records are not “personal data,” there is a significant likelihood that most business records, including email communications, would be considered “personal data” under the EU Directive as enacted in the various national Data Protection Acts (the DPAs).
- **If the EU Directive applies, which state’s personal data protection law governs?** Answering this question will likely require identifying the location of the “data controller” and/or “data processor,” possibly various “data subjects,” as well as the location of the data at issue—e.g., in the case of emails, the location(s) of the email server(s). As a result, this effort will involve an examination of the rules in effect in the “home” nation of the controller, and possibly those of the data processor and data subject.
- **If data at issue is subject to local data protection laws, what steps can be taken to meet the need for the data in the United States while complying with local European laws?** In order to access and retrieve the employee data for any of the three reasons noted above, it is highly probable that terms and conditions found in the EU Directive and the state DPAs regarding the “processing” of “personal data” and its subsequent onward transfer would apply. As described in more detail below, the mandates and rules found in the EU Directive and the state DPAs restrict what can be done to data, at least in the absence of some other applicable exception to their application.

Because of the complexities associated with this issue and the time that could be required to resolve the many issues associated with the lawful processing and onward transfer of personal data, a company with data residing in Europe that might be used in or transferred to the United States should consider taking the following data protection “readiness” steps to position itself to best address the dictates of the EU Directive:

- Implement audited and certified data management policies and procedures designed to minimize the potential for privacy infringement. These measures should include:
 - Structuring or segregating data to facilitate the ready identification of personal data, especially data of a highly personal or sensitive nature.
 - Deploying technologies that can be used to anonymize or redact data (to the extent the use of such technology is otherwise consistent with discovery or other legal obligations).
 - Informing data subjects and their representatives, through their respective European employers of any further transfer of their

personal data, for company management purposes and/or compliance with U.S. mandatory laws.

- Implementing computer systems and email usage policies that clearly define acceptable usage of computers and networks and the ownership of that equipment and data on that equipment, and that set users' expectations of privacy for the data stored on the machine or device they use.
- Obtaining, when necessary, general and matter-specific consent from employees/data custodians.⁵
- The company should consider taking steps to familiarize itself with the nuances of the applicable legislation and with existing means that can be used to facilitate the flow of data between Europe and the United States. For example, the company might:
 - Designate an employee or select counsel to liaise with local data protection officials in an effort to make sure any local authorization or certification is received for transfers of data; and/or
 - Take advantage of existing mechanisms for the transfer of data from the European Economic Area (EEA) to the United States. These mechanisms include enrolling in the Safe Harbor certification program sponsored by the U.S. Department of Commerce, the use of Standard Contractual Clauses, and/or the implementation of Binding Corporate Rules (BCRs) governing intracompany data transfers.⁶
- In the context of responding specifically to U.S. discovery requests, a company should consider the following options:
 - Carefully consider the nature of the discovery request to determine if some portion of the information sought resides in the United States or is otherwise available from a source that does not implicate EU data protection issues
 - Work closely with third-party service providers resident in the member nation or where appropriate, with local in-house IT staff to filter or cull the data (e.g., by the use of key terms) so that extraneous information is eliminated before it is used in or transferred to the United States.
 - Consider enlisting the help of custodians to self-select data for future processing and transfer.

5 As discussed in more detail below, while consent in itself may be of limited value, it may have the practical effect of making complaints less likely.

6 As discussed in more detail *infra*, each of the possible transfer methods requires adherence to strict rules that may severely limit their application to a situation in which information is being gathered in Europe and then transferred to the United States for disclosure to a third party, such as a federal investigating agency or an adverse party in a litigation matter.

- Alert the U.S. court or agency to the data protection issues and seek a protective order or confidentiality agreement pertaining to the materials.
- Work with opposing counsel or the agency requesting the data in an effort to narrow the scope of the request as much as possible.
- Consider the use of Standard Contractual Clauses to facilitate the onward transfer of data to third parties.
- Carefully consider whether there are any additional national laws and rules, especially those aimed at thwarting “foreign” discovery, that might come into play.

Data Privacy in the European Union

Historical Background

An analysis of the EU Directive and its implementation by individual EU and EEA nations requires a brief examination of the EU’s historical approach to employee-created or -received workplace information and the emphasis placed on the privacy of employees regarding the information they create or receive in the workplace.⁷ Moreover, the application of the EU Directive and member nation DPAs to so-called personal data will influence the extent to which a company can access some types of employee-generated or -received data, and once accessed, the uses to which the data can be put, including the transfer of such data to the United States or another jurisdiction outside the EEA.

Furthermore, although provisions found in the EU Directive and national DPAs permit the transfer of personal data among EEA member nations and contemplate the transfer of data to a country outside the EEA, such transfers are only lawful if that receiving country provides an “adequa[te] level of protection” for personal data or if a limited exception to the general bar to the onward transfer of data can be found.⁸ At the present time, Switzerland, Canada, Argentina, Jersey, Guernsey, and the Isle of Man have been certified as affording an appropriate level of protection.⁹ The United States has not been found by the European Commission (EC) to provide adequate protection.¹⁰

The data protection scheme now in place in Europe, which emphasizes an individual’s right to privacy in his or her personal data, can trace its lineage to Article 8 of the 1950 European Convention on Human Rights, which provides that

7 Broadly, the EEA is made up of the 27 members of the European Union along with Norway, Iceland, and Liechtenstein. 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. See http://europa.eu/abc/european_countries/index_en.htm.

8 See EU Directive Ch. IV, arts. 25, 26.

9 The EU Directive does not define the term “adequate.” Instead, determinations of the adequacy of data protection afforded by a nation are assessed by the European Commission.

10 See http://ec.europa.eu/justice_home/fsi/privacy/thridcountries/index_en.htm.

everyone has the right to respect for his private and family life, his home and his correspondence. . . . There shall be no interference by a public authority with his exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.¹¹

The EU Directive, which was published on October 24, 1995, echoes the importance of the individual's fundamental right to privacy:

Article 1—Objective of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.¹²

The terms of the EU Directive were intended to guide the 30 separate states that make up the EEA in their establishment of their own separate national data protection regulatory regimens, and although the various data privacy schemes share many common components of the EU Directive, a great deal of inconsistency in approach is evident at the Member State level. As a result, the laws of each member nation must be examined to determine the impact of local regulation on personal data, including workplace data, as well as to address other important issues, such as those pertaining to penalties for violating data protection proscriptions. For example, violations of the French data privacy act (DPA)¹³ can result in civil, administrative, or criminal charges being lodged against the violator or the “Data Controller” legally responsible for the violator, while violations of the UK DPA have not been criminalized.

To complicate matters even further, Article 29 of the EU Directive authorized the creation of independent data protection authorities to supervise compliance efforts pertaining to data protection. The heads of each office meet as a group—referred to as the Article 29 Data Protection Working Party—to address data protection issues and to provide guidance concerning the interpretation of data protection rules.¹⁴

11 European Convention on Human Rights (English), available at <http://www.echr.coe.int/ECHR>.

12 European Union Data Protection Directive, Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (O.J. 95/L281); see also *The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery* at 11 (Public Comment Version Aug. 2008) (Sedona Framework).

13 French Act no. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data), Article 51, available at <http://www.cnil.fr/fileadmin/documents/uk78-17VA.pdf>.

14 See Fred H. Cate & Margaret P. Eisenhauer, *Between a Rock and a Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements*, 6 Privacy & Security L. Rep. (BNA) 229 (Feb. 5, 2007).

Although the views of the Article 29 Data Protection Working Party are advisory in nature and do not carry the force of law, they provide helpful insight into the prevailing opinion of member nations about data

Key Terms

An understanding of several key terms found in the EU Directive and echoed in member nation DPAs is critical to analyzing their possible reach because although they employ terms that have a familiar ring to them, many of these terms have precise meanings that are often very different and more expansive than might be presumed. For example, this can be seen in an examination of Articles 3 and 4 of the EU Directive, which define the Directive's scope and outline the responsibilities of member states in protecting data privacy, as well as provide for the establishment of national data protection laws within the EU:

Article 3—Scope

- (1) This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

....

Article 4—National law applicable

- (1) Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
 - a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable
 - b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law
 - c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community
- (2) In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.¹⁵

privacy issues, especially when one considers the lack of case law or more official commentary on many of these issues.

15 EU Directive arts. 3, 4.

As indicated above, the terms “processing,” “controller,” “processor,” and “personal data” all take on special meanings under the EU Directive.¹⁶ Understanding these terms is critical to understanding the reach of the EU Directive, as well as the statutes passed by individual member States.

Processing

Processing “mean[s] 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.”¹⁷

The definition of the term “processing” is critical to developing a sense of the reach of the EU Directive and the local state statutes enacted in its wake. As defined in Articles 2 and 3 of the Directive, almost any activity undertaken by a so-called controller or processor regarding personal data, including the mere storage of electronic data and electronic data preservation (e.g., in response to a litigation hold directive), would be covered by the applicable legislation so long as the processing is undertaken wholly or in part through automatic means. Furthermore, the term “processing”—and thus the admonitions of the EU Directive—can apply to nonelectronic files, such as card indices or paper files that are part of an organized filing system. Thus, many activities that are typically associated with discovery compliance, whether electronic or not, or with conducting an internal investigation in general, such as the collection, preservation and organization of data belonging to selected company personnel, applying search terms, and the review of selected data, would all fall within the broad definition of “processing.”¹⁸

Data Controller

A data controller is “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.”¹⁹

Many of the key provisions found in the data protection legislation are focused on the conduct and actions of the data controller. Moreover, “the law of the EEA country where the ‘data controller’ is established will apply to the question of whether the relevant personal data [defined and discussed below] can be legitimately ‘processed’ under the EU Directive and the local laws which implement the [EU] Directive.”²⁰ Furthermore, if separate companies in a corporate group are established in different countries having

16 The EU Directive does not have the force of law as such, but serves as the basis for the laws enacted by Member States to meet the concerns expressed in the EU Directive.

17 EU Directive art. 2(b).

18 A UK Court of Appeal decision from March 2007 gives some hope that not every activity involving the examination of information amounts to the processing of personal data. In *David Paul Johnson v. The Medical Defence Union Limited* [2007] EWCA Civ. 262, the majority of the Court of Appeal held that the defendant had not processed data by its review of 14 paper files and three computer files recording incidents and complaints relating to the plaintiff over a 10-year period because the selection of information had been carried out by employees exercising their individual judgment as risk managers, not through “automatic means” or by the “processing of materials in a relevant filing system.” Given the somewhat unusual facts in this case, as well as the observation that UK data protection decisions do not always follow the leanings of continental enforcers, see *infra* discussions pertaining to the definition of “personal data,” parties will need to consider the effect, if any, of this opinion on their particular situation.

19 EU Directive art. 2(d).

20 Sedona Framework at 12.

laws pertaining to the processing of personal data, the laws of each country in which the data controllers are established could apply to the processing of personal data.²¹

Another interesting, and yet unresolved, feature of the term “controller” is whether it applies to a law firm (and possibly other professionals) assisting a party with its data processing needs. Arguably, there might be circumstances in which counsel could be said to be acting “jointly” with clients in determining the “purposes and means” of processing personal data, especially in the context of today’s eDiscovery environment in which lawyers are called upon to provide advice on how to collect and review copious amounts of data. Because many of the guidelines promulgated by the EU Directive, as well as laws enacted by member nations, focus on the data controller, counsel would be well-advised to consider this possibility.²²

Processor

A “processor” is a “natural or legal person . . . or any other body which processes personal data on behalf of the controller.”²³

As was the case with “processing,” the term “processor” has a much broader meaning than how the term is often used in eDiscovery compliance in the United States, where it is typically used to refer to a technology service provider that assists in preparing electronically stored information for review or production. In the context of the EU Directive and of various state legislative schemes, the term can include an entity that merely stores or processes data in the ordinary course of its business.

Personal Data

“Personal data” means “any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”²⁴

The processing of personal data at the request of a data controller triggers the provisions of the EU Directive and those of member States. Because “processing” includes almost all activities associated with handling data, especially in the eDiscovery context, ascertaining whether information is “personal data” is important to determining whether the data protection act applies to the data at issue.

What constitutes personal data for data protection purposes varies among EEA member nations.

For example, in a 2003 UK decision, the UK Court of Appeal observed that “not all information retrieved from a computer search against an individual’s name or unique identifier is personal data within the [meaning of the UK Data Protection] Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data.”²⁵ Thus, under *Durant*, a record that merely identified its

21 See *id.*

22 Law firms might also be deemed to be data processors while acting on behalf of their clients.

23 EU Directive art. 2(e).

24 EU Directive rt. 2(a).

25 *Durant v. Financial Services Authority*, [2003] EWCA (Civ.) 1746 (Dec. 8, 2003), ¶ 28, available at <http://www.hmcourts-service.gov.uk/judgmentsfiles/2136/durant-v-fsa.htm>.

author or recipients without revealing more information about their status or condition could arguably be found to fall outside the definition of “personal data” and the provisions of the data protection act would not apply. Of course, if the record did provide more information—for example, if the record addressed employment status or provided salary or date-of-hire information—then even under *Durant* the record would likely fall within the protections afforded by the relevant data protection legislation.

Furthermore, the *Durant* decision has been criticized by the UK’s Information Commissioner’s Office (ICO) and does not appear to have been followed (at least by citation) in other EEA jurisdictions. Moreover, the ICO, in a report issued to provide “technical guidance on determining what is personal data,” observed that “[w]here data about objects is not currently processed to provide information about an individual, but could be processed to provide information about an individual (for example, taxi location data), the data is likely to be personal data [within the meaning of the statute]. What is being considered here is whether the processing of the information has or could have a resulting impact upon the individual even though the content of the data is not directly about the individual UK Information Commissioner’s Office.”²⁶

The ICO continued in the report to note the potential reach of its interpretation. For example, in a hypothetical contained in the same report, the ICO opined that a document that listed the attendees at a meeting would be treated as personal data because it provided biographical information about data subjects in that it indicated what those persons were doing at a particular time and their location.²⁷

In some jurisdictions, the data need not directly identify a data subject for it to be classified as personal data. For example, the French data protection authority has found that the IP address of a computer should be deemed “personal data” because it could allow the identification of a particular computer, thus indirectly permitting the identification by a third party (the Internet access provider) of an individual holding an Internet subscription. This interpretation results from the drafting of the definition of “personal data” under French law. Indeed, when implementing the EU Directive, France expressed the concept of “indirect identification” not only by reference to an identification number, but also when the identification of an individual could be reasonably made by a third party to the data controller. By doing so, France included the provisions of Recital 26 of the preamble to the EU Directive in the legal definition of personal data. Moreover, Recital 26 of the EU Directive states that “to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.” (Emphasis added.)²⁸

Thus it would appear that, at least as far as the Article 29 Data Protection Working Party is concerned, the concept of “personal data” includes any data allowing the identification of an individual, either directly or indirectly, through means “likely reasonably” to be used either by the data controller or by any third party.

26 *Data Protection Technical Guidance Determining what is personal Data* (Aug. 21, 2007), available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf.

27 *Id.* at 13.

28 This interpretation has been confirmed by the Article 29 Data Protection Working Party in two opinions: Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (June 20, 2007) (01248/07/EN WP 136) (WP 136), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf, and Article 29 Data Protection Working Party, Opinion 1/2008 on Data Protection Issues Related to Search Engines (April 4, 2008) (00737/EN WP 148) (WP 148), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf.

Territorial Considerations

Given the definitional breadth of the terms used in the EU Directive and that of national DPAs, it is important to address the potential extraterritorial reach of those bodies of rules. The *Sedona Framework* provides that in those situations where the data controller is located outside the EEA—for example, a situation in which the data controller is located in the United States, but personal data is processed in an EEA country—“then personal data will be subject to the law of the EEA member country where the equipment is used to process the data.”²⁹

By way of example, the *Sedona Framework* states that “if a company in the USA transfers data to an eDiscovery vendor in the UK, then it will be subject to UK local data privacy laws.”³⁰ Although this example is unclear about the location of the data before the transfer, i.e., whether the data is located in the United States or Europe before its transfer to the UK, another example found in the same publication suggests that the treatment of U.S. domestic data kept in a European location as part of a company’s ordinary course of business—from the perspective of data protection—should be analyzed in terms of international comity with respect to that data being made available in the United States in response to an otherwise legitimate document request in civil litigation.³¹ Interestingly, no direct citation is provided for this proposition.

This potentially expansive view is arguably supported by language found in the EU Directive and the laws of member nations. For example, the reach of the EU Directive is not limited to citizens of the EU, and would include non-European workers seconded to a facility located in an EU Member State.³² Thus, privacy protections could extend to data subjects regardless of their nationality or residence, so long as data is being “processed” in a country governed by the EU Directive or by or on behalf of a “data controller” located within the EU.

An examination of the applicable national laws tends to support this expansive notion. For example, the DPA for the Czech Republic³³ expressly applies to “all personal data processing” in the Czech Republic.³⁴

Furthermore, the Czech DPA applies to personal data processing even if the controller is not established in the Czech Republic “if the law of the Czech Republic is applicable preferentially on the basis of the international public law” or “if the controller who is established outside the territory of the European Union carries out processing on the territory of the Czech Republic.” And similarly, “[i]f the controller carries out processing through its organization units established in the territory of the European Union, [the controller] must ensure that those organization units will process personal data in accordance with national law of a respective member State of the European Union.”³⁵

29 *Sedona Framework* at 12.

30 *Id.*

31 *See id.*, Appendix C: Application of the Framework for Cross-Border Discovery Conflicts to Selected Hypothetical Case Studies, Hypothetical Case Study No. 2.

32 Barbara Crutchfield George, Patricia Lynch & Susan F. 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, 752 (Summer 2001).

33 *See Act on Protection of Personal Data and on Amendments to Some Related Acts (2000)*, available at <http://www.privireal.org/content/dp/czechrepublic.php>.

34 Czech Office for Personal Data Protection (DPA) art. 3(2).

35 Czech DPA art. 3(5)(a), (b).

Similar sentiments can be found in a number of other statutory schemes for EEA nations, including those of France,³⁶ Germany,³⁷ and the UK.³⁸

It is important for counsel to consider the language found in the EU Directive and national DPAs and the published information pertaining to the interpretation of that language. A European Data Protection Authority would likely conclude that data stored in the EEA is subject to the terms of the EU Directive and the mandates of the applicable national DPA, regardless of its point of origin. If such were the case, it is important to consider the available options for processing and accessing the data stored in the EEA in the event that a company is called upon to access that data as part of discovery compliance. The Sedona Conference provides some guidance on this point.³⁹

The Sedona Conference authors suggest a “balancing of the needs, costs and burdens between the parties [in litigation] and the interests of each jurisdiction in protecting the privacy rights and welfare of its citizens affected by the litigation.”⁴⁰ The proposed balancing approach advocated by the Sedona Conference requires the weighing and assessment of seven factors:

- i. The nature of data privacy obligations in the jurisdictions where the responding party is established
- ii. The obligations of the responding party to preserve relevant information related to the litigation in both the jurisdiction where the litigation is filed and the jurisdictions where the responding party is established
- iii. The purpose and degree of control of the responding party in maintaining the sought-after information in the jurisdiction where the information is located
- iv. The nature and complexity of the proceedings
- v. The amount in controversy
- vi. The importance of the discovery to resolving critical issues in the matter
- vii. The ease and expense of collecting, processing, reviewing, and producing relevant electronic documents, taking into account:
 - a. The accessibility of the electronic documents
 - b. The quantity of electronic documents

36 See French Data Protection Act and related regulatory provisions on the Protection of Personal Data, available at <http://www.cnil.fr/index.php?id=300> (French language) or, for an unofficial translation into English language, <http://www.cnil.fr/index.php?id=4>.

37 See Federal Data Protection Act, Bundesdatenschutzgesetz § 1 (¶ 2) (3), (¶ 5) (2006), available (in English) at http://www.bfdi.bund.de/cln_007/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf.

38 See Data Protection Act ch. 29 § 5 (1998).

39 See *The Sedona Conference—Cross-Border Transfers of Electronically Stored Information: Best Practices for Avoiding and Resolving Conflicts* (Draft dated Oct. 28, 2007) (Cross-Border Best Practices).

40 *Id.* at 27.

- c. The location of the electronic documents
- d. The likelihood that the integrity and authenticity of electronic documents will be impaired by the discovery process
- e. The ability to identify documents subject to foreign privilege.⁴¹

The arguments that can be made based on these factors will depend, at least in part, on the nature of the litigation at hand.

Issues Pertaining to Data Processing and the Onward Transfer of Personal Data

The EU Directive and member nation DPAs contain provisions that, from a U.S. perspective, can be seen as designed to impede access to so-called personal data located in Europe. The first hurdle to clear concerns the steps that must be taken before personal data can be “processed.” The second concerns how data, once processed, can be transferred to a geographic location outside the EEA. Both hurdles must be overcome in order for data to leave a member of the EEA and come to the United States.

Processing

To the extent the records prepared by a company’s employees fall within the definition of “personal data,” then any “processing” of that data must be “lawful” and in accord with the EU Directive and the national DPA. Moreover, Article 6 of the EU Directive requires that data controllers ensure that personal data is:

- (i) Processed fairly and lawfully
- (ii) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical, or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards
- (iii) Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- (iv) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified
- (v) Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member states

⁴¹ *Id.* at 27-28.

shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical, or scientific use.

The requirement that data must be processed “lawfully” has been examined in detail by the Article 29 Data Protection Working Party. According to that group, the lawful processing of data must address the principles of finality, legitimacy, proportionality, and transparency.⁴² In this context, “finality” refers to the fact that personal data “must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.”⁴³ “Legitimacy” requires that data only be processed for legitimate purposes and in accord with the provisions of Article 7 of the EU Directive.⁴⁴ “Proportionality” forbids the processing of data for a purpose beyond that for which it was collected and requires that the processing of personal data so collected “still [be] fair to the worker.”

Finally, “transparency” requires that employers notify employees of the data they are collecting about them, give employees access to and as the case may be, update such data upon request, and inform employees of why the data is being processed, the categories of entities to which the data may be disclosed, and the eventual transfer/disclosure of their personal data outside of the EU.

Although Article 6 of the EU Directive spells out what a controller must consider when it is permitted to process personal data, Article 7 enumerates the circumstances in which processing can take place at all.⁴⁵ Moreover, it provides that personal data can be processed only if:

- (a) The data subject has unambiguously given his consent; or
- (b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- (d) Processing is necessary in order to protect the vital interests of the data subject; or

42 See Article 29 Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context (Sept. 13, 2001) (5062/01/EN/Final WP 48) (WP 48) at 3, *available at* http://ec.europa.eu/justice_home/fsi/privacy/docs/wpdocs/2001/wp48en.pdf.

43 *Id.*

44 *Id.*

45 The processing of so-called “sensitive” personal data—personal data revealing the data subject’s racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or pertaining to the subject’s health or sex life—is even more tightly controlled and is generally prohibited by Article 8 of the EU Directive unless specific, enumerated exceptions are present. Article 8’s prohibitions do not apply if the data subject gives explicit consent to the processing of the data or where the processing is necessary to meet the obligations of the controller in the field of employment law or to protect the vital interests of the data subject or another person where the data subject is incapable of giving his or her consent. EU Directive art. 8(2)(a)-(c). Similarly, processing by certain types of foundations or trade unions may be excepted from the general proscriptions of the directive, as is the processing of data made public by the data subject. *Id.* art. 8(2)(d), (e). Other exceptions exist in the context of medical treatment and law enforcement. See *id.* art. 8(3)-(7).

- (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) Processing is 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 or fundamental rights and freedoms of the data subject which require protection under Article 1(1).⁴⁶

The statutes for member nations generally track these general provisions.⁴⁷

1. Article 7(a): Consent—A “False Good” Solution?

The plain language of the provisions found in EU Directive Article 7 pertaining to consent (Art. 7(a)), compliance with a legal obligation (Art. 7(c), and/or legitimate interests (Art. 7(f)) would appear to provide sufficient bases for processing employee data in the context of an internal investigation or as part of discovery *compliance*.

These provisions, however, have been construed narrowly by data protection authorities. For example, the Article 29 Data Protection Working Party has opined that “consent” must be freely given and that it must be capable of being revoked by the employee/custodian at any time, i.e., at will.⁴⁸ Furthermore, fully informed consent is required.⁴⁹ Thus, if a controller seeks consent from a data subject regarding the processing of his or her personal data, the controller will need to specify the purpose for which the data is to be processed and the means and manner of the data processing.⁵⁰ Furthermore, the controller can process the data only in accordance with the purpose for which the data was collected and may not commingle the data with other data collected for some other purpose.⁵¹

Clearly, the strings attached to obtaining “consent” to personal data processing can be substantial and problematic. Moreover, in some matters there may be strategic or tactical reasons for not informing an employee that his or her data is going to be collected and subsequently reviewed by company personnel or counsel. In such situations, consent to processing by the data subject is a nonstarter. Furthermore, even in those matters where consent is at least a theoretical possibility, the need to obtain consent from all data subjects—not just the custodians of the records being collected—and the right of data subjects to withdraw their consent at any time or to cure any incomplete or inaccurate information poses substantial hurdles for parties wishing to rely on consent as a basis for processing.⁵²

46 See EU Directive art. 7(a)-(f).

47 Although the legislation of member nations generally tracks Article 7’s admonitions, counsel and their clients should consult the particular Data Protection Act of the member nation at issue for any nuances that may be present.

48 See WP 48 at 23.

49 *Id.* Although the EU Directive does not expressly mandate that consent be in writing, some EEA jurisdictions, e.g., Germany, do require a writing for consent to be effective. Because of this possibility and due to the detail required for consent, we believe that a party using consent as a means for legitimizing the processing of personal data should seek to have the consent in writing.

50 See *id.*

51 See *id.*

52 See EU Directive art. 12(b) (data subject has the right to rectify incomplete or inaccurate data); *Id.* art. 14(a) (data subject’s right “to object at any time”).

The difficulties associated with relying on consent as a pathway to processing are further demonstrated in another Working Party paper that was recently published.⁵³ The issuance of this Working Party paper, devoted exclusively to cross-border discovery issues, reflects the complex issues associated with processing personal data in the context of a U.S.-based investigation or litigation matter and the subsequent transfer of that data—or some portion of that data—to the United States. The paper also serves as an “invitation to public consultation with interested parties, courts in other jurisdictions and others to enter a dialogue with the Working Party” on these issues.⁵⁴

In WP 158, the Article 29 Data Protection Working Party stated that it considers it “unlikely that in most cases consent would provide a good basis for processing.”⁵⁵ In reaching this conclusion, the Working Party first restated the need to get consent from third parties—such as customers—identified in the data and the practical difficulties with such an exercise.⁵⁶ The Working Party also noted the need for obtaining consent that is truly and freely given and that data subjects “must have a real opportunity to withhold . . . consent without suffering any penalty, or to withdraw it subsequently if [the data subject] changes his mind.”⁵⁷ For those reasons, the Working Party concluded its analysis of consent as a pathway to processing by repeating the text found in an earlier Working Party paper: “Relying on consent may . . . prove to be a ‘false good solution,’ simple at first glance but in reality complex and cumbersome.”⁵⁸

2. Article 7(c): Processing to Meet the Controller’s Legal Obligations

Processing undertaken to meet the legal obligations of the controller would seem to fit nicely within the context of a U.S. company conducting an internal investigation or responding to a subpoena in a criminal or civil matter. Unfortunately, looks can be deceiving. Concepts concerning what constitute the legal obligations of the controller have evolved narrowly and do not include the need to meet extraterritorial legal requirements, such as U.S. discovery or federal statutes, like Sarbanes-Oxley.⁵⁹

Interestingly, the processing of personal data to meet domestic or communitywide legal obligations would satisfy the requirements announced in Article 7(c). Thus, depending on the nature of the action and the existing national statutory or regulatory scheme in place, data required for a U.S.-based matter could feasibly be processed in response to a foreign legal action.⁶⁰ Of course, even if data were processed in this manner, the possible onward transfer of that data to the United States would still be an open issue, as examined in more detail below.

3. Article 7(f): Processing Deemed Necessary for the Purposes of Legitimate Interests Pursued by the Controller

53 See Article 29 Data Protection Working Party, Working Document 1/2009 on Pretrial Discovery for Cross Border Civil Litigation (Feb. 11, 2009) (00339/09/EN/WP 158) (WP 158).

54 WP 158 at 14.

55 *Id.* at 8.

56 *Id.*

57 *Id.* at 9.

58 *Id.* (quoting Article 29 Data Protection Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (Nov. 25, 2005), (2093/05/EN WP 114) (WP 114) at 11, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf).

59 See Article 29 Data Protection Working Party, Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime (Feb. 1, 2006), (00195/06EN WP 117) (WP 117) (finding that “any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC”).

60 See WP 117 at 7-8.

The Working Party's recent paper on pretrial discovery observes that "the requirements of 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)" and thus justify the processing of personal data.⁶¹ The authors also state, however, that "[t]his basis would only be acceptable where such legitimate interests are not overridden by the interests of fundamental rights and freedoms of the data subject."⁶²

Under the framework proposed by the Article 29 Data Protection Working Party in WP 158, several considerations must be weighed in determining the balancing of interests between the controller and the data subject. Those factors, in turn, involve an examination of concepts that are fundamental to the EU Directive: proportionality, transparency and notice, data access and the right to cure, and data security.

Proportionality

This factor is derived from Article 6 of the EU Directive, which requires the fair and lawful processing of data and that data be collected for "specified, explicit, and legitimate" purposes. According to the Working Party, proportionality requires "data controllers involved in litigation to take such steps as are appropriate . . . to limit the discovery of personal data to that which is *objectively relevant* to the issues being litigated."⁶³ To accomplish this, the Working Party recommends applying various filters to the data to limit the processing of data not called for in the litigation and suggests that various anonymization or redaction techniques be employed if at all possible.⁶⁴ The Working Party also observed that the filtering process should take place locally in the country in which the personal data is found before the personal data that is deemed to be relevant to the litigation is transferred to another, non-EEA jurisdiction.

In continuing its discussion of proportionality, the Working Party examined the question of who could make the objective determination of relevancy:

The Working Party recognises that this [i.e., filtering] may cause difficulties in determining who is the appropriate person to decide on the relevance of the information taking into account the strict time limits laid down in the US Federal Rules of Civil Procedure to disclose the information requested. Clearly it would have to be someone with sufficient knowledge of the litigation process in the relevant jurisdiction. It may be that this would require the services of a trusted third party in a Member State who does not have a role in the litigation but has the sufficient level of independence and trustworthiness to reach a proper determination on the relevance of the personal data.⁶⁵

Finally, the Working Party recommended that parties facing a need to process personal data approach the relevant U.S. court to explain the difficulties posed by a production request and seek a protective order to comply with EU and Member State rules.⁶⁶

61 See WP 158 at 9.

62 *Id.*

63 *Id.* at 10 (emphasis added).

64 *Id.* at 11.

65 *Id.* at 11.

66 *Id.*

Transparency and Notice

Under the rubric of transparency, the Working Party addresses the kind of information that must be provided to a data subject when his or her data is being processed in accord with Article 7(f) of the EU Directive, as well as the timing of such notice. Relying on Article 10 of the EU Directive, the Working Party opined that, in the context of pretrial discovery, data subjects should receive advance, general notice of the possibility of personal data being processed for litigation in the United States and that once personal data was processed for discovery purposes, data subjects should receive notice about the identity of any recipients of the data, the purposes of the processing, the categories of data at issue, and the existence of their rights (discussed below) with respect to that data.⁶⁷

Similarly, under Article 11, notice should be provided to data subjects “as soon as is reasonably practicable after the data is processed” in those situations where the data is collected from a third party (e.g., computer data off their employer’s network) and not directly from the subject.⁶⁸ Interestingly, the Working Party also observed that the timing of notice contemplated by Article 11 concerning data in the possession of a third party could be delayed if there is a risk that such notice would jeopardize the safety or integrity of the data and/or impede the company’s ability to investigate matters.⁶⁹ Of course, the Working Party cautioned that such an exception regarding notice “must be applied restrictively on a case by case basis.”⁷⁰

The notice envisioned by Articles 10 and 11 goes beyond serving as a mere informational tool. Such notice provides the data subject with an opportunity to exercise his or her “right to object at any time on compelling legitimate grounds to the processing of the data relating to them” under Article 14 of the EU Directive.⁷¹ Compelling legitimate grounds for such objection would include violations of the EU Directive’s principles of data quality and proportionality (as found in Article 6 of the EU Directive and discussed *supra*), notice (as addressed by Articles 10 and 11), rights of access, rectification, and erasure under Article 12, and the secure handling of data as required by Article 17.⁷²

Data Access and the Right to Cure

The data subject’s right to access his or her data and to cure inaccurate or incomplete data is another fundamental right that must be balanced when assessing the feasibility of processing data under Article 7(f) of the EU Directive. Moreover, Article 12 gives the data subject the right to have access to the data held about him or her in order to check its accuracy and rectify it if it is inaccurate, incomplete, or outdated. And, as noted by the Working Party, the right to access and to cure allows a data subject to check the personal data that has been processed and to satisfy himself or herself that the data to be transferred “is not excessive.”⁷³

Of all the rights examined thus far when considering whether the processing of personal data under Article 7(f) is a possibility, the right to data access and cure poses significant issues for counsel conducting an internal investigation or, worse yet, responding to a

67 *Id.*

68 *Id.*

69 *Id.* at 12.

70 *Id.*; see also WP 117 at 13 (discussion of Article 11 notice in the context of the establishment of whistleblower hotlines).

71 WP 158 at 12; see also WP 117 at 9.

72 See WP 117 at 9-15.

73 WP 158 at 12.

discovery demand or investigative subpoena. For example, giving document custodians the ability to winnow out “excessive” materials raises compliance concerns about the completeness of a production and could lead to the expenditure of a great deal of time, effort, and money validating the decisions made by custodians. Similarly, altering or removing data from a “production set” of materials could give rise to allegations of spoliation or obstruction. Indeed, the Working Party, with measured understatement, noted that “this right could give rise to a conflict with the requirements of the litigation process to retain data as at a particular date in time and changes (whilst only for correction purposes) would have the effect of altering the evidence in the litigation.”⁷⁴

Data Security

The final factor to be weighed concerns the need for the data controller to “take all reasonable technical and organisational precautions to preserve the security of the data to protect it from accidental or unlawful destruction or accidental loss and unauthorised disclosure or access” as mandated by Article 17 of the EU Directive.⁷⁵ The aforementioned precautions apply not only to the controller, but to other actors in the litigation drama, including the law firms involved in the matter, the court adjudicating the matter, and retained experts, who must also comply with the principles of the EU Directive.⁷⁶

Given the complexities associated with processing personal data, passage along the road to the lawful and fair processing of data subject to the rules established by the EU Directive and the laws enacted by EEA countries is neither easy nor quick. Because of this, companies and their counsel should begin assessing avenues for the processing of data in the EU before an immediate need arises, if at all possible. Nuances in the local statutory regime, nation-specific case law on the topic of personal data protection, formal and/or informal rulings or guidance offered by national data protection bodies, as well as the applicability of regulations outside the context of data protection,⁷⁷ must be considered by companies facing the data processing challenge posed by the European rules and regimes.

Assuming that a mechanism can be found to process personal data, a means must be found to facilitate the onward transfer of that data from its home to the United States so that it can be examined by counsel or produced in litigation. As was the case with processing, the onward transfer of personal data from the EEA to the United States has its own labyrinth of rules that must be negotiated.

Onward Transfer

A Concept in Search of a Definition

The EU Directive and national DPAs significantly restrict the transfer of personal data from Europe to locations outside the EEA. Moreover, with a few exceptions to be examined shortly, these rules prohibit the transfer of data to countries lacking an

⁷⁴ *See id.*

⁷⁵ *Id.*

⁷⁶ *Id.* at 12-13.

⁷⁷ Some of these, like “blocking statutes,” will be discussed below.

adequate level of protection for personal data and, as discussed earlier, the United States has been found lacking in that regard.⁷⁸

Although the concept of personal data transfer is at the heart of the EU Directive and member nation DPAs, none define the term “transfer.” The term has been interpreted, however, by the European Court of Justice (ECJ) in a matter that is sometimes referred to as the “Swedish church lady” case.⁷⁹

In that case, Mrs. Lindqvist created a webpage from her home computer that displayed certain information about her and her fellow parishioners, which included, *inter alia*, the names of the parishioners, employment details, telephone contact information, and in one case, health status. The defendant church lady did not inform the parishioners that she was creating the webpage and she also failed to notify the Swedish data protection authority that she was going to create the page. Although it is not clear from the opinion by what means the Swedish public prosecutor learned of the charges brought against Mrs. Lindqvist for violating Sweden’s Data Protection Act. The church lady admitted creating the page, but denied criminal wrongdoing. Nevertheless, she was fined SEK4000 by the prosecutor.

On appeal, the ECJ framed the issue as “whether there is any transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person (the hosting provider) who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.”⁸⁰ The EC and the governments of Sweden, the Netherlands, and the UK submitted briefs to the ECJ on this question.

The EC and Sweden argued that the loading of personal data onto an internet page, so that the data becomes accessible to nationals of third countries, constitutes a transfer of data to third countries within the meaning of Directive 95/46.⁸¹ The Netherlands, after observing that the term “transfer” was not defined, argued that the term referred to the act of intentionally transferring personal data from the territory of a member state to a third country and thus concluded that Mrs. Lindqvist’s actions should not be considered to be a transfer of personal data to a third country within the meaning of Article 25 of Directive 95/46.⁸² Similarly, the UK stated that the term connotes the transmission of personal data from one place and person to another place and person.⁸³

In examining the facts before it, the ECJ observed that in order for someone “to obtain the information appearing on the internet pages on which Mrs. Lindqvist had included information about her colleagues, an internet user would not only have to connect to the internet but also personally carry out the necessary actions to consult those pages. In other words, Mrs. Lindqvist’s internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages.”⁸⁴ Thus, according to the court, “personal data [that] appear on the computer of a

78 See EU Directive art. 25.

79 *Bodil Lindqvist v. Sweden*, C-101/01, Judgment of November 6, 2003, available at http://www.fim.uni-linz.ac.at/Lva/IT_Recht_Computerforensik/C-101_01%20-%20Bodil%20Lindqvist.pdf.

80 *Lindqvist* ¶ 52.

81 *Id.* ¶ 53.

82 *Id.* ¶ 54.

83 *Id.* ¶ 55.

84 *Id.* ¶ 60.

person in a third country, coming from a person who has loaded them onto an internet site, were not directly transferred between those two people but through the computer infrastructure of the hosting provider where the page is stored.”⁸⁵ As a result, the court concluded that there is no “transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.”⁸⁶

It is unclear how much reliance should be placed on the *Lindqvist* decision. On the one hand, it would seem to suggest that a company could consider hosting data in Europe (either on its own platform or through a service provider located within the EEA) that could then be accessed by counsel in the United States via a Web-based platform without there being a transfer of personal data. On the other hand, there are some troubling limits to the case. For example, the opinion does not address the situation in which a reader of the information would then take the information provided and pass it along to a third party, like a litigation adversary or government agency. Similarly, it is unclear how limiting the number of potential viewers to a discrete set of people—such as a document review team in a litigation matter—might have colored the court’s views on whether an impermissible transfer had taken place. Moreover, the court took care to distinguish the situation before it, in which information was passively made accessible, from situations in which information is transmitted to others automatically.

Interestingly, the EC, in the May 2009 version of its Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries, appears to have addressed the distinction suggested by the ECJ.⁸⁷ Moreover, the EC states that “all the cases where a controller takes action in order to make personal data available to a third party located in a third country” could be deemed a transfer of personal data.⁸⁸ Thus, the EC would appear to apply a broader definition of “onward transfer” than that applied by the *Lindqvist* court.⁸⁹

Possible Exceptions to the Bar Against Onward Transfer

The EU Directive generally bars the onward transfer of data from the EEA to a country lacking adequate protection of personal data.⁹⁰ Article 26 of the EU Directive addresses derogations to that general prohibition and lays out the following possibilities for the onward transfer of data from the EEA to another location, like the United States:

85 *Id.* ¶ 61.

86 *Id.* ¶ 71. The court expressly withheld judgment concerning the legality of the activities undertaken by the hosting provider. *Id.* ¶ 62.

87 Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries, available at http://ec.europa.eu/justice_home/fsi/privacy/docs/international_transfers_faq/international_transfers_faq.pdf, at 18 (Transfer FAQ).

88 To the extent the data controller is located in a Member State, the laws of that state will dictate whether and how personal data can be transferred outside the European Community. Transfer FAQ, at 19. If the data controller is located outside the Community, the laws of the Member State where the processing equipment is used will apply. *Id.*

89 No rationale is given for the EC’s stated view in the FAQ. To the extent the EC’s view prevails, the scope of EC authority over data transfers out of the EEA would be extensive.

90 See EU Directive art. 25.

- (a) The data subject provides unambiguous consent; or
- (b) The transfer is necessary for the performance of a contract between the data subject and the controller; or
- (c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- (d) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims [in court]; or
- (e) The transfer is necessary in order to protect the vital interests of the data subject; or
- (f) The transfer is made from a register that according to laws or regulations is intended to provide information to the public.

At first glance, the exceptions to the general bar on the onward transfer of personal data pertaining to consent by the data subject (Art. 26(1)(a)) and/or to onward transfers “legally required” (Art. 26(1)(d)) would appear to provide an easy and well-marked road for a company to follow with respect to data currently located in the EEA that is needed in the United States.

Unfortunately, both exceptions, like those relating to processing, carry unforeseen burdens and limitations. For example, consent in this context (as was the case with “processing personal data”) must be given prior to the transfer, and be unambiguous, specific to the transfer at issue, freely given, and informed.⁹¹ Furthermore, as was the case with respect to consent in the context of processing personal data, all identifiable data subjects—not just the custodian from whom data is data is taken—must consent to the transfer.

The conditions under which an onward transfer can be justified as being “legally required” have also been interpreted narrowly⁹² by the Article 29 Data Protection Working Party:

The Working Party emphasises that the concept of “establishment, safeguarding or defence of legal claims” must here again be subject to strict interpretation. Thus, for example, the parent company of a multinational group, established in a third country, might be sued by an employee of the group currently posted to one of its European subsidiaries. The exception in Article 26(1)(d) appears to allow the company to legally request the European subsidiary to transfer certain data relating to the employee if these data are necessary for its defence.

...

91 See *id.* arts. 2(h), 26(a).

92 Even if this exception could be used to justify the onward transfer of data to the United States, the Article 29 Data Protection Working Party has opined that “other relevant provisions of the Directive need to be respected.” Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 at 8, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/2005/2p114_en.pdf.

In addition, this exception can only be applied if the rules governing criminal or civil proceedings applicable to this type of international situation have been complied with, notably as they derive from the provisions of the Hague Conventions of 18 March 1970 (“Taking of Evidence” convention) and of 25 October 1980 (“Access to Justice” Convention).⁹³

Since the publication of WP 114 in 2005, the Working Party members recently revisited issues pertaining to the onward transfer of data from the EU to jurisdictions like the United States in WP 158. In the latter working paper, they stated that “[w]here the transfer of personal data for litigation purposes is likely to be a single transfer of all relevant information, then there would be a possible ground for processing under Article 26(1)(d) of the Directive where it is necessary or legally required for the establishment, exercise or defence of legal claims.”

At first glance, this view would seem to offer a glimmer of hope to those seeking to bring data into the United States for litigation or internal investigative purposes. A closer look reveals, however, the very narrowly circumscribed nature of the Working Party’s views.

First, the statement is cast in terms of “litigation,” thus the need to bring in data for compliance purposes or to conduct an internal investigation to avoid litigation or prosecution would not seem to satisfy this requirement. Indeed, the authors state that a transfer of files based on Article 26(1)(d) cannot be premised “on the grounds of the possibility that legal proceedings may be brought one day in U.S. courts.”⁹⁴

Second, a requirement that the transfer take place in a single delivery of data, although possible in some matters, would not appear to take into account the possible need for a supplemental production of data or the addition of other document custodians. Third, the reference to “relevant” information appears to presuppose that a relevancy review has taken place within the EEA member nation in which the data is located, a view that is consistent with the Working Party’s expressed view with respect to processing personal data,⁹⁵ but one that could certainly add to the time needed for and costs associated with discovery compliance.

Nevertheless, in what might be seen as a softening of its earlier position, the Working Party’s approach to the use of the Hague Convention⁹⁶ as a necessary step to using Article 26(1)(d) as a basis for the onward transfer of data appears to have changed somewhat from that stated in WP 114, which is quoted above. In the more recent publication, the Working Party authors recognize that resorting to the Hague Convention cannot be an absolute precondition for the onward transfer of personal data because some EEA member nations have not signed the Hague Convention and other members that have signed it did so with reservations under Article 23 of the treaty⁹⁷ with respect to

93 WP 114 at 15, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

94 WP 158 at 13 (citing WP 114 at 15).

95 See *id.* at 11 (discussed above).

96 Hague Evidence Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, 847 U.N.T.S. (1972).

97 For example, France limits discovery in that country to only those means referenced expressly in the treaty, i.e., letters rogatory, depositions before a diplomatic official, or depositions before a duly appointed commissioner. See ABA Section of Antitrust Law, *Obtaining Discovery Abroad* 112 (2d ed. 2005). Similarly, Germany does not appear to permit pretrial document discovery under the Hague Convention, *id.* at 137, while Italy limits pretrial discovery to only the tools afforded by the treaty and further limits discovery to those matters deemed “civil or commercial” under Italian law, *id.* at 158; see generally, Sedona Framework at 17 (citing Soiret, *The Foreign Defendant: Overview of Principles Governing*

compliance with discovery demands arising from foreign—i.e., U.S.—litigation. See WP 158 at 13. As a result of this recognition, the Working Party now notes that resorting to the treaty for data found in countries that (1) are signatories to the treaty and (2) have not signed with reservations about U.S. (or other foreign) discovery is an apparently independent basis for the onward transfer of personal data: “Where it is possible for the Hague Convention to be used, the Working Party urges that this approach should be considered first as a method of providing for the transfer of information for litigation purposes.”⁹⁸

Although a discussion of all the issues associated with reliance on the Hague Convention as a means of facilitating discovery is beyond the scope of this paper, the Working Party’s take on the efficacy of resort to the Hague—“[w]hilst there may be some concerns about the length of time such a procedure could take, the courts, for example in the U.S., are experienced in the use of the Hague and such timescales can be built into the litigation process”—seems optimistic. Moreover, U.S. courts take the view that the procedures afforded by the Hague Convention are but “one method of seeking evidence [abroad] that a court may elect to deploy.”⁹⁹ Indeed, the complexities associated with invoking the Hague Convention, the time frame associated with achieving results under the Hague, and the convention’s requirements for specificity with respect to how document requests must be made are among the reasons cited by U.S. litigants for proceeding abroad under the Federal Rules of Civil Procedure, without resort to the treaty. Furthermore, resort to the Hague treaty would not be an option in matters that had not yet ripened into an actual case.

Thus, for a company trying to review materials in order to meet regulatory obligations or to detect internal wrongdoing, compliance with Article 26(1)(d) or a handful of narrowly tailored alternative avenues for the onward transfer of data—discussed immediately below—are the only options available for now.

Alternative Means for Transferring Data to the United States from the EEA

There are three other options for the onward transfer of data to the United States aside from the exceptions found in the EU Directive: Department of Commerce Safe Harbor certification, Standard Contractual Clauses, and BCRs. As will be seen, although each provides a pathway for European data to enter the United States for delivery to a particular recipient, significant strings are attached. For example, although each option permits the flow of data out of Europe into the United States, none of the options readily provides for the onward transfer of data once in the United States to, for example, a government regulatory body in an effort to report wrongdoing and seek leniency or amnesty from prosecution.

Safe Harbor Certification

The first option is Safe Harbor certification, which exists between the United States and the 27 members of the European Union.¹⁰⁰ The U.S. Department of Commerce and the

Jurisdiction, Venue, Extraterritorial Service of Process and Extraterritorial Discovery in U.S. Courts, 28 Torts & Ins. L.J. 533 (1993)).

⁹⁸ WP 158 at 14.

⁹⁹ *Societe Nationale Industrielle Aerospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522, 541 (1987).

¹⁰⁰ See European Union Safe Harbor Overview, available at http://www.export.gov/safeharbor/eu/sh_en-overview.asp. The Safe Harbor program is limited to transfers of data from the EU Member States to the United States; transfers from Norway, Iceland, and Liechtenstein to the United States are not covered and

EC have developed a set of protocols that permit the flow of personal data into the United States from Europe to firms that self-certify on an annual basis that they provide adequate privacy protection of personal data.¹⁰¹

Through this process, certified firms are deemed adequate to receive data, and disputes arising over the conduct of U.S.-based Safe Harbor firms are heard in the United States.¹⁰² The Safe Harbor scheme is only available to firms that are subject to the jurisdiction of the Federal Trade Commission or Department of Commerce.¹⁰³ Furthermore, firms seeking Safe Harbor certification must comply with seven “safe harbor principles” that were established between the EU and the United States:

- **Notice:** Organizations must notify data subjects about the purposes for which the information is being collected and must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to whom disclosures of the data might be made, and the choices and means the organization offers for limiting its use and disclosure.
- **Choice:** Organizations must give individuals the opportunity to “opt out” of having their personal data disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, an explicit “opt-in” choice must be given by the data subject for his or her information to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.
- **Onward Transfer to Third Parties:** To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as its agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the EU Directive or another adequacy finding. In the alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.
- **Data Subject Access:** Individuals must have access to personal information about them that an organization holds and must be afforded the opportunity to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.¹⁰⁴

transfers from the EU to other another non-EU venue other than the United States are not covered by the EU Safe Harbor regimen. Similarly, Switzerland and the U.S. Department of Commerce have also entered into a Safe Harbor protocol for the transfer of certain types of data from Switzerland to the United States. See http://www.export.gov/safeharbor/swiss/doc_eg_safeharbor_swiss.asp.

101 U.S. Department of Commerce, Safe Harbor, available at <http://www.export.gov/safeharbor/index.html>.

102 The European data exporter could be subject to discipline by the national data protection authorities in the event of a data breach. See U.S. Department of Commerce, Safe Harbor Privacy Principles—FAQs (July 21, 2001), available at http://www.export.gov/safeharbor/SH_FAQ9.asp.

103 *Id.*

104 The FAQs provided by the Department of Commerce as a guide to interpreting the Safe Harbor process and the seven principles that guide that process make clear that access by data subjects to their data is

- **Security:** Organizations must take reasonable precautions to protect personal data from loss, misuse and unauthorized access, disclosure, alteration, and destruction.
- **Data integrity:** Personal data must be relevant to the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
- **Enforcement:** In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organizations. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

Through the Safe Harbor program, an organization can be deemed to provide "adequate safeguards" for personal data even though that organization is located in the United States. The very basis for this recognition—adherence to the seven principles—calls into question the efficacy of a company relying on the Safe Harbor regimen to conduct an internal investigation, pursue litigation, or respond to a subpoena. At the very least, the requirements for notice, custodial choice, access, and data integrity certainly could influence—and likely limit—the instances in which the Safe Harbor program could be used in the situations we have examined in this paper. Similarly, issues pertaining to the onward transfer of data by the U.S. recipient of the European data to another party, e.g., an adverse party or federal agency, would have to be addressed. This could be especially problematic if a European data subject chose to opt out once that subject's data was present in the United States and likely subject to the subpoena power of a U.S. court.

Standard Contractual Clauses

Standard Contractual Clauses are the second avenue for data to come into the United States.¹⁰⁵ Under this approach, data is permitted to enter the United States (or any other

not an absolute right. Moreover, access can be denied over specific concerns about, inter alia, interference with the execution or enforcement of the law; interference with private causes of action; disclosure of personal information pertaining to other individuals where such references cannot be redacted; the breach of a legal or other professional privilege or obligation, prejudicing the confidentiality that may be necessary in connection with monitoring, inspection, or regulatory functions connected with sound economic or financial management; or other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated. U.S. Department of Commerce, *Safe Harbor Privacy Principles—FAQs* (July 21, 2001), available at http://www.export.gov/safeharbor/SH_FAQ8.asp.

105 Like so many pieces in this puzzle, the current forms of Standard Contractual Clauses may be evolving to meet challenges posed by changing data processing business arrangements. In an Article 29 Data Protection Working Party paper issued on March 5, 2009, the Working Party provided comments to an EC proposal to amend the Standard Contracts to take into account the growing use of subprocessors by data importers. See Opinion 3/2009 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC (data controller to data processor) (Mar. 5, 2009), (00566/09/EN WP 161), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp161_en.pdf.

venue deemed inadequate from a data protection standpoint) where both parties agree to be bound by a set of clauses that comply with the principal provisions of the EU Directive.¹⁰⁶ Careful drafting is required because a breach can result in a claim for damages by the data subject and, unlike the Safe Harbor option, companies contemplating use of Standard Contractual Clauses will need to determine if the applicable data protection authority must be notified in advance of any onward transfer of data out of the EU to the another (non-EU) location.¹⁰⁷ National data protection authorities have the power to terminate transfers if the terms of the contracts are not being adhered to, and depending on the member nation at issue, can impose monetary fines or seek criminal penalties.

In practice, inasmuch as the jurisdictions of both the data protection authorities and the EC are limited to the national/European territories, their decisions may solely have any direct effect upon corporate entities located within these jurisdictions. Consequently, the law applicable to Standard Contractual Clauses, administrative, civil and criminal sanctions that may be pronounced on the basis of personal data transfers violating the EU Directive or the Standard Contractual Clauses are deprived of legal effect against any US counterpart.

The joint and several liability between the US and European counterparts in the Standard Contractual Clauses often deters US entities. However, such liability regime actually exonerates the US counterpart from any liability under DPAs or EU laws. This important issue must be considered by the corporate entities that must choose between Safe Harbor Certification procedures subject to the jurisdiction of the US Federal Trade Commission and Standard Contractual Clauses with no legal binding effect in the United States.

Binding Corporate Rules

BCRs are the third option available. BCRs are available only to companies within a corporate family group and only after the relevant data protection authority has approved the terms of the BCR.¹⁰⁸ The terms of the BCR, once approved, only protect onward transfers between affiliated companies, so any transfer outside the corporate group to a third party, like a federal agency conducting an investigation, would not be covered and would thus require resort to other means.¹⁰⁹ Of course, even when approved, BCRs do not trump the applicable data protection rules and regulations of the Member State or States at issue.

106 See Commission Decision 2001/497/EC (O.J. L181,15.6.2001), *available at* <http://www.datatilsynet.no/upload/Dokumenter/Temaartikler/plikter/2.pdf>; Commission Decision 2004/915/EC (O.J. L385, 27.12.2004), *available at* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF>.

107 See Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries, at 25 (FAQ B.2) *available at* http://ec.europa.eu/justice_home/fsi/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

108 See Article 29 Data Protection Working Party, Working Document: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (June 3, 2003), *available at* http://ec.europa.eu/justice_home/fsi/privacy/docs/wpdocs/2003/wp74_en.pdf.

109 Several EU member nations—along with Iceland, Liechtenstein, and Norway—have agreed to implement a protocol in which one member's data protection authority acts as the lead authority to investigate a company's BCR application. If the application is approved by the lead authority, the data protection authorities of the participating nations agree to use the lead authority's decision as the basis for their concurrent approval of the BCR application. The Czech Republic, Cyprus, France, Germany, Ireland, Italy, Latvia, Luxembourg, Malta, the Netherlands, Slovakia, Spain, and the United Kingdom have signed on to the mutual recognition procedure.

Other Potential Traps to Consider

The EU Directive and the national data protection laws enacted to meet the dictates of the EU Directive are not the only snares that await companies and counsel as they attempt to collect vital information kept abroad. Sticking to the European¹¹⁰ context of this paper, these traps could include blocking statutes, bank secrecy laws, rules pertaining to works councils, pre-transfer reporting obligations, and even telecommunications laws.

Although by no means exhaustive, the following overview provides a relevant sampling of some of these laws and rules and issues associated with them.

Blocking Statutes

Blocking statutes can generally be characterized as procedural, discretionary, or industrial in nature, or in some cases, a hybrid combination of these.¹¹¹ Procedural blocking statutes prohibit compliance with discovery orders unless procedures within the country in which discovery is sought are met.¹¹² Discretionary blocking statutes empower local government agencies with the ability to approve or deny discovery.¹¹³ Industrial blocking statutes, as the name would imply, seek to prohibit the discovery of information that pertains to a specific industry.¹¹⁴

France's blocking statute is one of the broadest in its procedural sweep and one of the most strict in that it raises the possibility of criminal sanctions for conducting discovery outside the confines of the Hague Convention.¹¹⁵ The French statute provides, in part: "Subject to international treaties or agreements [e.g., the Hague Convention] and laws and regulations in force [i.e., the laws of France], it is forbidden for any person to request, seek, or communicate, in writing, orally or in any other form, documents or information of an economic, financial or technical nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures." The statute applies to evidence sought by traditional discovery requests in U.S. litigation.¹¹⁶ The statute's prohibitions apply to "French nationals and directors, representatives, and employees of companies acting in France."¹¹⁷

Persons relying on the French statute as a basis for resisting discovery in U.S. matters have in the past found little comfort offered by U.S. courts, which have regularly rejected applying it so that French parties escape their discovery obligations.¹¹⁸ Although there

110 The EU Directive is currently being considered by members of the Asia Pacific Economic Cooperation (APEC) group as a model for its members as they craft legislation relating to the cross-border flow of data. APEC members include Australia, Canada, Chile, Hong Kong, China, Japan, South Korea, Mexico, New Zealand, Peru, Taiwan, Thailand, the Philippines, the United States, and Vietnam. See APEC Group Considers Privacy Framework for Regulation of Cross-Border Data Flows, Digital Discovery & e-Evidence (BNA) (Mar. 11, 2009), available at <http://ddee.bna.com/subscribers/News.And.Analysis.html?d=A0B8A0F9V6>.

111 See ABA Section of Antitrust Law, Obtaining Discovery Abroad 51 (2d ed. 2005).

112 *Id.*

113 *Id.*

114 *Id.*

115 See Law. No. 80-538 of July 16, 1980, J.O., July 17, 1980, at 1799, D.S.L., 1980, at 285; see also ABA Section of Antitrust Law, Obtaining Discovery Abroad (2d ed. 2005) at 109-13.

116 Obtaining Discovery Abroad, at 110.

117 *Id.*

118 See *Valois of America, Inc. v. Risdon Corp.*, 183 F.R.D. 344, 348 (D. Conn. 1997).

could be several reasons for this rejection, one possible basis is that until very recently no one had been prosecuted in France for violating the statute's provisions.

That changed, however, in *In re Advocat "Christopher X,"* Cour de Cassation, French Supreme Court, December 12, 2007, Appeal no. 07-83228. In this decision by the French Supreme Court, the French court clearly confirmed that the Hague Convention is the exclusive means for gaining discovery of French nationals or French residents. In its decision, which was the first interpreting the 1980 law, the court found that the actions of a French lawyer, retained by a U.S. party, in collecting oral statements from an *adversary's* employee violated the criminal provisions of the statute, which impose imprisonment of up to six months, a fine of €18,000, or both. In this case, the lawyer was fined €10,000.¹¹⁹ "The significance of this French decision is that it suggests that U.S. litigants may need to reconsider using the Hague Convention as the first, if not exclusive, means of discovery abroad."¹²⁰

Switzerland provides a similar example. Indeed, two statutes,¹²¹ one protecting Swiss sovereignty and the other addressing industrial espionage concerns, are particularly relevant to conducting U.S. discovery. The first, Article 271 of the SPC, captioned "Protection of Swiss Sovereignty Against Unauthorized Acts for a Foreign Authority," generally prohibits obtaining evidence in Switzerland for use in a foreign proceeding without judicial assistance as provided under the Hague Convention on Taking Evidence Abroad. Article 271 prohibits performing acts on behalf of a foreign state on Swiss territory that, under Swiss law, lie within the competence of a Swiss public authority. Offenders need not be actual officials; it is enough that their actions have an official nature. Private collection of material intended for use as evidence in foreign proceedings falls within Article 271's scope. In particular, the gathering of documents (and also taking depositions) by foreign attorneys in Switzerland, or in connection with a foreign subpoena, is considered to be an unauthorized act for a foreign authority. Because Article 271 not only prohibits engaging in unauthorized acts on Swiss territory but also facilitating them, criminal liability could potentially extend to those who facilitate such acts, including deponents and document holders.

Article 273 of the SPC—Protection Against Economic Espionage—prohibits nonconsensual disclosure of so-called business secrets of third parties residing in Switzerland to foreign states and entities (including foreign affiliates and parent companies), unless endorsed by competent Swiss authority. Specifically, a foreign authority's order does not justify disclosure. Moreover, Article 273 prohibits the investigation and disclosure of industrial and business secrets for and to foreign authorities, foreign organizations or foreign private companies. The focus of this provision is on the protection of Swiss economic interests. Article 273 prohibits not only the illicit investigation of business secrets, but also disclosure of legally obtained information where the concerned person has a legitimate interest in keeping the information secret.

119 Accessing employee data in the context of an internal investigation or as part of a U.S. litigation is especially problematic given the EU Directive, France's adaptation of the EU Directive's tenets in its national data protection act, see Decree No. 2005-1309 of 20 October 2005 enacted for the Application of Act No. 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties, as amended by Decree No. 2007-451 of 25 March 2007, available at <http://www.cnil.fr/index.php?id=4>, the blocking statute, and the primacy of employee privacy as found by French courts. See, e.g., *Philippe K. v. Cathnet-Science*, Cour de Cassation, Chambre Sociale, Arrêt No. 1089 FS-P+B+R+1, Pourvoi No. J-03-40.017, 5/17/05. Reported in the *BNA Privacy Law Watch* (June 6, 2005), available at http://www.juritel.com/Ldj_html-1095.html; *Nikon France v. Onos*, Cass. Soc., Arrêt No. 41-64, October 2, 2001, discussed in <http://euro.ecom.cmu.edu/program/courses/tcr840/2003/workplace.pdf>.

120 *Sedona Framework* at 22.

121 The provisions are found in the Swiss Penal Code (the SPC).

Under Article 273, “secret information” is construed broadly and any information not evident or publicly available may be a business secret if there is a legitimate interest in keeping it confidential.¹²² For example, information regarding foreign law violations is generally deemed secret (e.g., foreign tax or antitrust regulations, or criminal offenses).

Article 273 aims to protect Switzerland’s commercial interests, and violation occurs only if the secret information is connected to Switzerland. Business relations among Swiss parties meet this requirement. However, if the data concerns business relations between a Swiss and a foreign party, the disclosure is only prohibited by Article 273 if the Swiss party wants to keep the information secret. With some exceptions, the Swiss party may waive its right to secrecy and inform a foreign authority about the business secret. Foreign (based on domicile, not nationality) party secrecy interests are not protected.

Because Article 273 protects Swiss commercial interests, Swiss criminal law applies regardless of where the criminal act was committed. SPC, Art. 4. Thus, if a party outside of Switzerland investigates and provides foreign authorities with information about Swiss business partners, such disclosure falls within the scope of Article 273.

By way of contrast, the UK’s blocking statute, United Kingdom’s Protection of Trading Interests Act, 1980, ch. 11, § 2 (Eng.), permits the discovery of documents absent a contrary authority precluding it. Thus, the applicable UK provision seems to follow an approach reflecting the discretionary and industrial models for blocking statutes noted above. The UK statute has been invoked in the past as was the case when a British court enjoined a British corporation from pursuing a U.S. antitrust action against two British defendants in *British Airways Board v. Laker Airways*, [1983] W.L.R. 544, 588-91 (C.A. July 26, 1983). The effect of the injunction was to bar persons within the UK from producing documents located there in the *Laker Airways* antitrust action against the state-owned airline, British Airways, which was proceeding in the United States.

Bank Secrecy Laws

In some sense, bank secrecy laws function as specialized blocking statutes that prohibit the production of certain types of business or commercial information in litigation matters. Perhaps the best example of such statutes can be found in Swiss law.¹²³ Thus, Article 47 of the Swiss Federal Law on Banks and Savings Banks prohibits the disclosure of confidential or secret information entrusted to a person on account of his or her position or capacity as a manager, employee, agent, liquidator, or commissioner of a bank.¹²⁴ The duty of secrecy described by the law arises from the relationship between the bank and its customer regardless of the existence of any formal acknowledgment of the relationship by either party and a breach of that duty by bank personnel can be punished by criminal fines and, in addition, damages can be sought by the customer for breach.¹²⁵

122 “The term ‘business secret’ has been defined to include ‘all facts of business life to the extent that there are interests worthy of protection in keeping them confidential.’” *Swiss Federal Attorney v. A.*, 98 BGE IV 209 (Sept. 7, 1972), cited in *U.S. v. Vetco Inc.*, 691 F.2d 1281, 1287 (9th Cir. 1981).

123 Switzerland is not a member of the EU or the EEA. Nevertheless, it has been found to afford adequate protection to personal data under the EU Directive and it provides a well-known example of the type of law that, although not directly addressing data protection, can impede the collection and transfer of data housed in that country. See Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *The Level of Protection of Personal Data in Switzerland* (Op. No. 5/99 WP 22).

124 See Banking Act of 1934, available at <http://switzerland.isyours.com/e/banking/secrecy/banking.act.html>.

125 See Obtaining Discovery Abroad at 226.

Although exceptions to the rules in favor of secrecy exist for certain types of conduct, those exceptions have generally been applied only if the reason for intrusion into the banking relationship is recognized as a crime in Switzerland.¹²⁶ Perhaps the most well-known application of this rule concerns requests for information from Swiss banks regarding allegations of tax evasion, which were routinely turned down by Swiss authorities because tax evasion is not a crime in Switzerland.

This all may be changing. On March 13, 2009, the Swiss government announced it would yield to pressure from the United States, Britain, Germany, and France by adopting a model tax convention drawn up by the Organization for Economic Cooperation and Development, a group of 30 leading democracies. The revised tax code will require Switzerland to share banking records with other countries when individuals are suspected of tax evasion at home.¹²⁷ It remains to be seen whether other cracks will develop in the facade of Swiss banking secrecy.

Works Councils and National Labor Laws

Works councils are prevalent throughout the EU and can play an important role in the acquisition and transfer of information because of so-called codetermination rights granted the councils. The existence of such councils can be traced to the passage of an EU-wide directive on September 22, 1994 that called for the establishment of a European Works Council (EWC Directive).¹²⁸ Moreover, the EWC Directive applies to companies with at least 1,000 employees within the EU and at least 150 employees in each of at least two Member States.

For example, the French Labor Code contains specific provisions directly inspired by the French DPA. Such provisions include a principle of fairness and proportionality of personal data regarding the processing of employee data by an employer. Notably, employees or works councils (for companies hiring more than 50 employees) must be consulted by the employer prior to the implementation of any data processing or of any technology enabling the employer to monitor the activities of employees.

Further to such consultation, which must describe the purpose of the data processing, the data recipients and the employees' rights resulting from the French DPA (access, modification, updates), each affected employee must be informed of such elements as presented to the works council. This notification process is mandatory and subject to administrative, civil, and criminal sanctions. Moreover, noncompliance with such procedural steps would make the evidence gathered through such processing inadmissible against an employee under French law. A failure to provide employees with the detailed information just summarized might be considered as a direct violation of the French DPA, which would prevent the transfer of the data processed outside the EEA.

When the prior notification process described above has taken place, the employer may have access to any file or email stored on an employee's professional computer and/or the company's servers. Nonetheless, the employer must specifically inform the employee that the inspection is to take place and permit the employee to be present so that the employee's personal files, i.e., those relating to his or her private life, can be avoided and not inspected. Consent in this context is not required under the applicable labor rules.

¹²⁶ See *The Limits to Bank Secrecy*, available at <http://switzerland.isyours.com/e/banking/secrecy/limits.html>.

¹²⁷ See Craig Whitlock, *Swiss Preparing to Protect Banking Secrecy*, *The Seattle Times*, Mar. 30, 2009, available at http://seattletimes.nwsourc.com/html/nationworld/2008946042_swiss30.html.

¹²⁸ See generally, *European Works Councils*, available at <http://www.etuc.org/r/57>.

Like France, Germany has an especially active works council movement and the nature of the relationship between a German company and that of the applicable works council must be considered when assessing options for gathering and analyzing materials in the context of an internal investigation or ongoing litigation matter.¹²⁹ For example, depending on the level of consultation that took place between a German company and a works council regarding the establishment of rules governing email usage by company employees, the works council could block the usage of employee email by the company or its counsel in a U.S. litigation matter.¹³⁰

Similarly, counsel would be well advised to consider the possibility that national labor laws could restrict access to data. For example, in the Czech Republic, an employer cannot review the content of an employee's email without his or her consent with respect to the specific email in question.¹³¹

Telecommunications Laws

National telecommunications laws are another potential area that counsel should consider when attempting to access email data located in Europe. For example, one possible issue that can arise under these types of laws is that an employer might be considered to be a telecommunications services provider under the local law, especially in the context where the employer provides email services to its employees and does not restrict the usage of the email system to only business correspondence. Because these laws vary widely in their terms and reach, the specific statute in the locale where the data is housed should be reviewed.¹³²

Pre-Transfer Reporting Obligations

As observed throughout this paper, EU member nations were free, when enacting legislation to give effect to the EU Directive, to craft additional provisions governing the processing or transfer of personal data consistent with the concepts stated in the EU Directive. As a result, there is significant variation among the member nations pertaining to the procedural details that govern processing and transfer.

One example of this can be seen in whether a data controller must notify and/or seek permission from the national data protection authority before transferring data to a location outside the EEA. For example, the Czech DPA provides that prior to the onward

129 In Germany, the Works Constitution Act (i.e., the Betriebsverfassungsgesetz or BetrVG) should be consulted by those interested in assessing the reach of codetermination rights. See § 87 para. 1 no. 6 BetrVG. English language version of the Works Constitution Act *available at* <http://hikwww1.fzk.de/br/content/worksConstitutionAct-BetrVG.pdf>.

130 See Federal Labor Court, judgment of May 3, 1994, 1 ABR 24/93, NZA 1995 at 40; judgment of June 16, 1998, 1 ABR 68/97, NZA 1999 at 49.

131 See No. 262/2006 Coll. of the Labour Code and Article 13 of the Charter of Fundamental Rights and Freedoms, as incorporated into the Constitution of the Czech Republic.

132 If the data at issue is housed by an Internet Service Provider (ISP), Directive 2006/24/EC on Data Retention by ISPs should be consulted. Moreover, that directive limits the amount of time that an ISP is permitted to retain email records to not more than two years from the date of the communication. See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *available at* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>.

transfer of data on the grounds of “consent” or “legal necessity,” the controller must “apply to the Office [of Personal Data Protection] for authorization to [sic] the transfer.”¹³³

Once notified, the office is empowered to examine all the circumstances related to the transfer of personal data, including the source of the personal data, its final destination, the categories of personal data that are to be transferred, the purpose and period of the processing, and any available information about legal or other regulations governing the personal data processing in a third country.¹³⁴ A violation of this reporting duty is punishable by fines ranging from CZK1,000,000 (approximately €36,000) to CZK10,000,000 (approximately €360,000).¹³⁵

“So Where Does This Leave Us?”—Some Concluding Thoughts

The lawful collection of data and information located in Europe poses substantial challenges for U.S. counsel, especially in the context of preserving, collecting, and forwarding information as part of a U.S.-based litigation. National laws enacted to implement the EU Directive, general or industry-specific blocking statutes, and mandated access through only the Hague Convention can singularly or, in some instances, collectively impede legitimate access to information.

The most important steps in managing this issue are to recognize that it exists and to plan for how the company will confront the challenges posed by it. For example, counsel might consider the options and strategies proposed earlier in this paper as part of its overall EU eDiscovery readiness planning.¹³⁶ Indeed, in many respects, this process is similar to that being undertaken by companies and their counsel as they act to meet the challenges posed by electronic discovery under the 2006 amendments to the Federal Rules of Civil Procedure. Counsel must become familiar with the rules of the particular jurisdiction that might impact access to data. For example, it is important to consider whether the collection of needed information will in fact involve the “processing” of data, a necessary prerequisite for data protection rules to apply. Similarly, the likelihood that the data sought is in fact “personal data” under the local jurisdiction’s laws must be considered.

Next, assuming that data protection rules are implicated, it is important to consider whether any technological options are possible, like segregating data to minimize the presence of sensitive personal data or installing anonymization software to reduce the likelihood that identifiable “personal data” will be processed or transferred. The identification of third parties who could assist with data should be considered.

The progress of and pronouncements by the Article 29 Data Protection Working Party should be monitored and studied for additional clues about how to navigate these troubled waters. Thus, the pathway suggested by the Working Party with respect to the processing of personal data—the use of EU Directive Article 7(f) to process data deemed necessary for the purposes of legitimate interests pursued by the data controller—and

¹³³ Czech DPA art. 27(4).

¹³⁴ *Id.*

¹³⁵ *Id.* arts. 44, 45.

¹³⁶ Members of the Morgan Lewis eData Practice Group can assist in this planning exercise.

that proposed for the onward transfer of that data—under the terms and conditions of Article 26(1)(d) should be studied and, to the extent possible, used by counsel to develop a preservation, collection, and transfer strategy in anticipation of the need for EU-based information.

Finally, the use of the Safe Harbor rules, Standard Contractual Clauses, and BCRs should also be considered, especially in situations where a U.S. company needs to access European-based personal data on a regular basis as part of the performance of its ordinary course of business activities. Although of limited value in situations in which the “imported” information must be transmitted to a third party in the United States not subject to the obligations of confidence imposed on or agreed to by the data importer, each of these methods could facilitate the lawful export of data to the United States, especially when that data is to be held within the confines of a defined group.

For further information on the topics discussed in this paper, please contact any of the following Morgan Lewis attorneys:

Philadelphia

Stephanie A. “Tess” Blair 215.963.5161 tblair@morganlewis.com

New York

Denise Backhouse 212.309.6364 dbackhouse@morganlewis.com

Washington, D.C.

Robert A. “Barry” Wiggins 202.739.5040 bwiggins@morganlewis.com

Paris

Claude-Etienne Armingaud + 33 (0)1 53 30 44 08 cearmingaud@morganlewis.com
Etienne Drouard + 33 (0)1 53 30 44 12 edrouard@morganlewis.com

About Morgan, Lewis & Bockius LLP

Morgan Lewis is an international law firm with more than 1,400 lawyers in 22 offices located in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Minneapolis, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, and Washington, D.C. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

This White Paper is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered Attorney Advertising in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes.

© 2009 Morgan, Lewis & Bockius LLP. All Rights Reserved.