e-Discovery and legal frameworks governing Privacy and Data Protection in European countries

Confidential Appendix

ORLA LYNSKEY, NEIL ROBINSON, MICHAEL GREENBERG

WR-812-FTI

November 2010

Prepared for FTI Consulting Inc.

EUROPE

Preface

RAND Europe was commissioned by FTI Consulting to conduct a short study to explore the conflict between the European legal framework for privacy and data protection and the sometimes competing requirements of e-disclosure imposed on US firms with European subsidiaries by legislation such as the US Foreign Corrupt Practices Act (FCPA).

To undertake this research, RAND Europe conducted desk research and commissioned fieldwork from in country legal experts in each of the identified countries (France, Germany, Spain, Switzerland and the United Kingdom).[1]

This report was prepared by Neil Robinson & Orla Lynskey of RAND Europe and Michael Greenberg of RAND's Centre for Ethics and Corporate Governance in the Institute for Civil Justice. National correspondents consulted included:

- France: Fanny Coudert, time.lex Law Offices, Paris
- Germany: Petra Hansmersmann, Unverzagt von Have, Hamburg
- Switzerland: Martin Eckert, Meyer Müller Eckert Partners, Zurich
- Spain: Cristina de Lorenzo, Sánchez Pintado & Núñez, Abogados, Madrid
- United Kingdom (England and Wales) Ruth Boardman, Dania Rifaat and Sarah Weindling, Bird and Bird, London

RAND Europe is an independent not-for-profit policy research organisation that aims to improve policy and decision making in the public interest, through research and analysis. RAND Europe's clients include European governments, institutions, NGOs and firms with a need for rigorous, independent, multidisciplinary analysis.

This document represents the Confidential Appendix containing the national country profiles. The authors would like to thank Hans Graux and Matt Bassford for their helpful comments during the preparation of this report.

[1] Noting that Switzerland is not a member of the European Union and therefore not subject to the European legal framework regarding privacy and data protection

For more information about RAND Europe or this document, please contact:

RAND Europe
Westbrook Centre
Milton Road
Cambridge CB4 1YG
United Kingdom
Neil_Robinson@rand.org

Joe Looby
Senior Managing Director
FTI Consulting
New York
joe.looby@fticonsulting.com

Veeral Gosalia
Managing Director
FTI Consulting
Washington, D.C.
veeral.gosalia@fticonsulting.com

Craig Earnshaw
Managing Director
FTI Consulting
London
craig.earnshaw@fticonsulting.com

Contents

Summary

Rationale

RAND Europe was commissioned by FTI Consulting to prepare a short paper exploring the conflict between the European legal framework for privacy and data protection and the sometimes competing requirements of electronic discovery ('e-discovery') imposed on US firms with European subsidiaries by legislation such as the US Foreign Corrupt Practices Act (FCPA).

Background

The competing and sometimes conflicting requirements of pre-trial discovery and legal obligations regarding the protection of personal data represent a unique and pressing public policy challenge. As the trends of globalisation and electronic storage of data continue and more and more firms are asked to produce materials (often stored electronically) there is an ever greater impact on compliance with different regulatory architectures governing personal data. Given volumes of commerce between the United States and Europe, this problem is particularly pertinent: especially so when the specific requirements of the legal framework governing the protection of personal data of European citizens are taken into account. This study comes at a critical junction in EU policy-making, when there is increased political appetite for improving the legal protection of personal data for European citizens.

The European legal framework governing privacy and data protection

In Europe different legal frameworks currently apply to privacy and data protection in different contexts, whether in the context of private international law within and between commercial entities, or concerning the use of personal data in the pursuit of police and criminal justice activities.[2] Although the applicability of these legal frameworks is currently under review (given the relatively recent entry into force of the TFEU), the divergence in

[2] For a detailed review of the strengths and weaknesses of EU Data Protection Directive 95/46/EC see Robinson, N., Valeri L. et al *Review of the Strengths and Weaknesses of the European Data Protection Directive* RAND; Santa Monica 2009 http://www.rand.org/pubs/technical_reports/TR710/

how these different uses of personal data has evolved historically into being covered by three legal frameworks:

- Directive 95/46/EC and e-Privacy Directive 2002/58 regarding the processing of personal data in the context of the Internal Market (i.e. 'First Pillar')
- Regulation 45/2001/EC in respect of the uses of personal data relating to the Common Foreign and Security Policy (formerly second pillar)
- Framework Decision 2008/977/JHA governing personal data processed in the domain of police and criminal justice co-operation (Formerly the 'Third Pillar' of police and criminal justice co-operation).

The Treaty of Lisbon represents a fundamental shift in how data protection is addressed throughout the Union. Specifically, the removal of the pillar structure of policy-making, combined with the general applicability of Art 16 TFEU means that all areas of EU law could be now covered, including processing in the former First Pillar (Internal Market), Second Pillar (Common Foreign and Security Policy) and Third Pillar (Police and Judicial Co-operation).[3]

The requirements of e-discovery

An important challenge posed to the EU legal framework for privacy and data protection is "e-discovery," or the demand for production of electronic records in connection with civil litigation and a range of other legal and corporate proceedings. In the simplest case, e-discovery involves a plaintiff demand for documents in connection with ongoing litigation, pursuant to formal judicial rules of procedure, which a defendant is obligated to comply with under those rules. In common law jurisdictions, the burdens of e-discovery in a civil case involving corporations can be enormous –literally millions of pages of corporate electronic documents and records can sometimes be demanded by a plaintiff for disclosure, in the context of a specific case. Simply identifying, organising, and producing the relevant documents can represent a Herculean task. Particularly in the U.S., e-discovery has become a big business, as technology vendors have entered the market to help corporations manage demands for large-scale document production in litigation.

e-Discovery in situations involving both EU and U.S. actors becomes even more complicated and burdensome. Litigation-based requests for document production under the procedural laws of one country (e.g., the U.S.) can easily run into conflict with the data protection requirements of another (e.g., national transpositions of the EU Data Protection Directive 95/46/EC). Consider hypothetical U.S. litigation that involves a multinational corporate actor based partly in Europe, with a large pool of corporate records tied to individual employees (e.g., internal e-mails), the latter arguably protected under EU privacy law. The corporation in this scenario is targeted as a defendant in a U.S. law suit, and demands are made for the production of corporate records and internal e-mails. In addition to all of the logistical burdens pertaining to e-discovery, the corporation in this instance will also need to worry about the application of EU privacy law to its records. In

[3] Hijmans, H, and Scirocco, A; *Shortcomings in EU Data Protection in the Third and Second Pillars: Can Lisbon be expected to help?* 2009 Common Market Law Review (46) 1485-1525 London

the worst case, the corporation might find itself facing a legal obligation to disclose records in a U.S. court, while simultaneously facing a legal obligation in one or more EU states not to disclose those records, per EU privacy law.

Analysis

Evidence from analysis of national approaches illustrate the difficulties of international transfers of data for e-discovery purposes. Despite the fact that all EU states are party to the 1970 Hague Evidence Convention (Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters or hereafter Hague Convention) and have transposed the EU Data Protection Directive into national law, stark differences in the legal regime applicable to international transfers for the purposes of e-discovery exist between EU Member States. These differences stem only in part from the fact that EU states have divergent common and civil law legal traditions. Of relevance when considering transfers of evidence for civil proceedings is whether the State concerned has invoked the Article 23 exception to the Hague Convention (which even the United Kingdom, a common law country, has invoked). Transfers of evidence for criminal proceedings are governed by bilateral agreements which differ from state to state. Moreover, some states, for instance France, have enacted 'blocking statutes' entailing harsh criminal sanctions for those who transfer certain types of information abroad. The data protection legislation in place also needs to be complied with. Here, although there are some minor differences between transposition in various countries, the overall legal framework remains similar; transfer to the United States is possible without consent once an 'adequate' level of protection is guaranteed whether that be by resorting to Standard Contractual Clauses, falling with the scope of a Safe Harbor agreement or by respecting Binding Corporate Rules.

Way forward

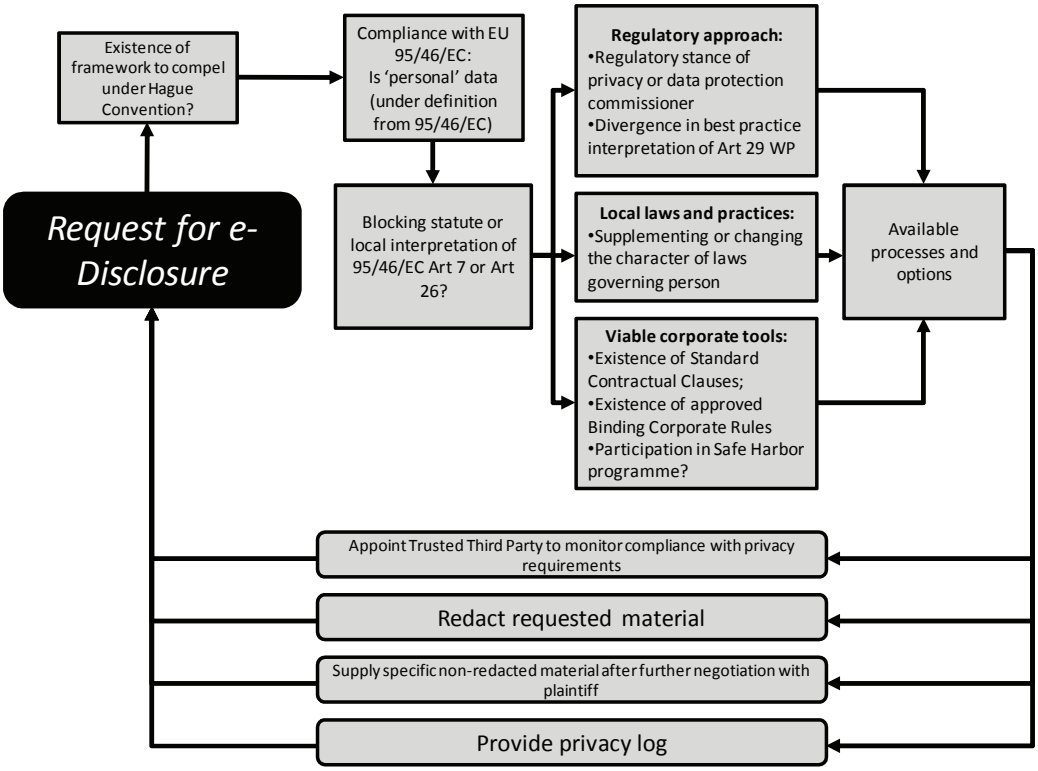
Based on our analysis and noting guidance from the Article 29 Working Party issued in 2009 on the use of personal data in pre-trial discovery and from our review of the situation in different countries, we propose our own suggested approach below:

- First – is there any potential framework to compel co-operation with US discovery rules for example under the Hague Convention or other bilateral agreements (depending on the civil or criminal nature of the request)
- Consider whether any protected data is likely to be involved – an estimation of the types and character of the data (whether it falls within the scope of EU data protection rules as it relates to an 'identifiable person'; whether the data concerned is 'sensitive data'). If the data concerned fall within the scope of the European Data Protection Directive (Directive 95/96/EC), as transposed into national law, verify whether the data transfer is permitted by the data protection regime. For instance, Article 7 of the Data Protection Directive enumerates the criterion according to which data processing is deemed legitimate. Article 26 sets out derogations to the general rules for transfer of data to third countries.

- Next, consider whether a blocking statute or other local legal restriction or interpretation on data disclosure exists – stemming from relevant Applicable National Law transposing Articles of 95/46/EC e.g. under Art 7(f) and Art 26(1)(d)
    - Whether the company has approved Standard Contractual Clauses (SCC), Binding Corporate Rules (BCRs), or participates in the Safe Harbor scheme which would cover the onward transfer of personal data;
    - Whether there are any unique local regulations or laws supplementing or changing the character of legislation governing the processing and transfer of personal data;
    - Similarly, whether the application of the law in practice differs in any respect given the regulatory stance and strategic approach of the Data Protection or Privacy Commissioner in the interpretation of this guidance (as has been shown elsewhere, EU Member States may differ in how they interpret the official guidance as presented by the Article 29 Working Party).
- Finally, upon answering the above, investigate processes and options that respect the fundamental rights of European citizens under Article 16 of the TFEU and Article 8 of the Charter of Fundamental Rights of the European Union whilst serving the purposes of pre-trial discovery. Such options might include the following:
    - Redacting or anonymising all documents in country, prior to the disclosure and onward transfer to the United States
    - Provision of a Privacy Log which details the information protected from disclosure in order for plaintiffs to determine more clearly the necessity of the disclosure of such data and possibilities for amendment of the Protective Order in order to safeguard defendants from liability for the production of this data
    - For those deemed of specific interest by the litigants in the pre-trial discovery process in the United States the European based subsidiary supply them in non-redacted form
    - Assigning a suitably qualified and appropriate Trusted Third Party to support the adherence of the processing to appropriate level of adequacy of protection in line with the European legal framework for privacy and data protection.

This is illustrated below in Figure 1.

Figure 1. Suggested e-Disclosure workflow



Source: RAND Europe

Methodology

To undertake this research, RAND Europe conducted desk research and interviews with 'in-country' legal experts in each of the selected countries (France, Germany, Spain, Switzerland and the United Kingdom). The countries were selected on a pragmatic basis after consultation with FTI Consulting as a representative selection of jurisdictions likely to be of interest in respect of the research question.

Structure of report

Chapter 1 National Contexts - Summary presents our framework for each country profile. Chapters 2-7 present country profiles for each of the countries selected for review. In each country report we provide an overview of the relevant legislation and regulatory stance, where known of privacy and data protection regulators in five countries: France, Germany, Switzerland, Spain and the United Kingdom (England and Wales). We cover the law on the books as well as issues relating to its implementation including relevant case law and public reports of cases where known. We also detail any relevant other legislation such as blocking statutes or legislation governing the processing of personal data in the workplace. Finally, each country profile considers the policy context and the resources and interest of the regulator dedicated to this conflict of laws challenge.

CHAPTER 1 National contexts - summary

Interviews were conducted with national experts in five European countries (France, Germany, Spain, Switzerland and the United Kingdom) in order to identify the legal framework applicable to e-discovery requests at national level as well as the policy factors that are taken into consideration in each of these jurisdictions. With the exception of Switzerland, all of the countries in which interviews were conducted are EU Member States; they were selected on the basis of their differing legal traditions and approaches to privacy issues. A complete overview of these interviews can be found in the appendices of this report however the findings made in these interviews can be summarised as follows.

The rules on pre-trial discovery differ significantly between these states. The UK, as a common law jurisdiction, has a well-established set of pre-trial discovery rules in place; a party to litigation is required to disclose any documents which adversely affect its own case as well as documents which support the opposing litigant's case. The other jurisdictions, which are all civil law jurisdictions, have no system of pre-trial discovery. Rather, parties must only offer evidence to the Court to prove that the facts they are asserting are true. In strictly circumscribed circumstances in each of these jurisdictions however an order for disclosure can be sought from a judge.

The legal basis for processing an e-discovery request depends on the nature of the proceedings for which the information concerned is sought. If the request is made to obtain evidence for civil proceedings, the Hague Convention is applicable. However, Article 23 of the Hague Convention allows Contracting States to declare that they will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents. All of the jurisdictions considered in this report have invoked this exception. Nevertheless, it is only Germany and Spain that refuse to consider Letters of Request under any circumstances. In France, in accordance with a declaration made by the French government, a Letter of Request will be authorised if it identifies a limited number of documents to be disclosed and the documents have a direct connection with the subject matter of the dispute. In Switzerland Letters of Request are accepted if they comply with strict limitations designed to prevent 'fishing expeditions' for evidence. In the UK evidence can be sought in accordance with the Evidence (Proceedings in Other Jurisdictions) Act 1975; applications must be made to the High Court supported by written evidence accompanied by the request as a result of which the application is made. All of the jurisdictions considered have concluded a bilateral agreement with the United States allowing for mutual assistance in criminal matters; evidence for criminal proceedings can

be sought by relying on these agreements. In France when documents and information of an economic, commercial, industrial, financial or technical nature are transferred to foreign individuals or entities and the Hague Convention or a Mutual Assistance Agreement is not applied, penal sanctions can be imposed on the transferor. Such a 'blocking statute' also exists in Switzerland and has been applied on numerous occasions.

Pre-trial discovery requests must also comply with the data protection provisions in place in each jurisdiction. As the European Data Protection Directive (Directive 95/46/EC) has been transposed into national law in France, Germany, Spain and the UK the rules in place in these jurisdictions are almost identical. Moreover, the Swiss have followed the scheme set out in the Directive to a large extent. The Data Protection Directive regime does not prohibit data processing (which includes the act of transferring personal data). Rather, according to Article 7, data processing is legitimate provided one of the criteria set out therein is complied with and the quality-assurance principles relating to data processing in Article 6 are respected. The most likely legal basis for legitimate data processing is Article 7(f) according to which processing is legitimate if it 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 for fundamental rights and freedoms of the data subject'. Indeed, the French data protection agency (the CNIL) specifically referred to this provision as a basis for data transfers in its recommendation concerning e-discovery in civil and commercial proceedings. The application of this provision requires that the data transfer is proportionate. For instance, when this provision has been applied by the British judiciary in the context of freedom of information requests specific attention has been paid to the meaning of the word necessary. This test will be difficult for lay-parties to apply and legal guidance will be needed. Indeed, the Information Commissioner in the UK has urged caution when applying it. As a result some data protection agencies, for instance the Swiss, are happy to provide transferors with ex ante advice concerning the legitimacy and proportionality of the transfer.

According to the Directive an adequate level of protection must be provided by the data recipient when a transfer is made to a third country. In general, the adequacy of the level of protection applied can be proven if the safe harbour principles are complied with, the data recipient has signed up to standard contractual clauses with the data controller or binding corporate rules are in place within a commercial group. Certain national distinctions nevertheless still exist. For instance, in France, non-massive transfers (transfers of small amounts of data on a non-recurring basis) do not require the prior-approval of the CNIL.

At a policy level, data protection authorities operate at a national level in France and the UK and at a regional level in Switzerland and Germany. In Spain, both regional and national data processing authorities exist; the national authority is responsible for processing by private parties. In general in these countries there is little awareness of the provisions of the FCPA. Although the data protection authorities in each of the jurisdictions considered have the power to impose significant sanctions for breaches of the data protection rules, no jurisdiction has exercised this power to sanction the transfer of data to a third country for discovery purposes. Indeed, it appears that it is only in France that this issue has been given serious consideration. The CNIL has been quite vocal on the issue and has issued a recommendation concerning e-discovery in civil and commercial

proceedings. The other data protection authorities have been concentrating their enforcement efforts elsewhere; for instance, in Germany priority has been given to publicly visible privacy issues (although private enterprises continue to be sanctioned) while in the UK the main focus is on security breaches and audit.

CHAPTER 2 Country Report: France

2.1 Introduction

The laws governing cross-border e-discovery in France are complicated. Any given e-discovery request, made for instance under the US Foreign Corrupt Practices Act (FCPA) by the Department of Justice or the Securities Exchange Commission, may be analysed under the lens of a national 'blocking statute' or international agreements and, potentially, under national data protection rules.

By way of background, Directive 95/46 EC (the 'Data Protection Directive') has been transposed into national law by Law No. 78-17 of 6 January 1978 concerning data processing, computer files and liberties, as amended by Law No. 2004-801 of 6 August 2004 concerning the protection of individuals with regard to processing of personal data. Moreover, the French Labour Code also encompasses some data protection elements as it places an obligation on employers to inform employees when employee monitoring systems are implemented in the workplace. The basic obligations set out in the French labour code have been elaborated upon by the Courts. In 2001, in the *Nikon* case strong statements emerged from the Court regarding the confidentiality rights of employees. These statements were subsequently nuanced and now a right to privacy extends only to e-mails and files contained on corporate owned equipment which the employee identifies as personal. Therefore, all of an employee's e-mails may be accessed with the exception of those which the employee earmarks as private.

The French system of pre-trial disclosure differs fundamentally from the US system. In France, parties must only offer evidence in support of their case; there is no obligation on parties to furnish other litigants with evidence. Nevertheless, if any party to the litigation requests specific documents, an order for disclosure can be sought from a judge. The judge plays a crucial role in the disclosure process by considering whether the requested document is necessary for the litigation. Moreover, a 'freezing order' can be sought from a judge in a 'référé civil' if there is a risk that proof will be destroyed. In practice, judges are generally willing to grant these orders if they are sufficiently motivated. When considering whether to grant such an order, the judge will take into account whether the document is necessary for the proceedings and the nature of the document in question.

2.2 Transfer of data

2.2.1 General rules governing transfer of information

International Conventions

Data transfer from France to third countries, such as the US, for the purpose of civil proceedings is governed by the Hague Convention. Article 23 of this Convention allows contracting States to declare that they will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents. In accordance with a declaration made by the French in the context of Article 23, a Letter of Request will only be authorised if it identifies a limited number of documents to be disclosed and the documents have a direct connection with the subject matter of the dispute. Letters of Request must be addressed by the competent third country authority to the competent authority in France, namely the Ministry for Justice. The Ministry for Justice then sends this Letter of Request on to a judicial authority to determine whether or not an order for disclosure should be made.

In the context of criminal proceedings, a Mutual Assistance Agreement was concluded between France and the US in 2001. Similarly to under the Hague Convention, a letter must be addressed to the competent French Ministry which is then translated and sent to the competent judicial authority for consideration.

French companies must inform the French Ministry of Justice when they receive an e-discovery request. In the one case involving the FCPA to date in France, the French company concerned worked in collaboration with both the French and US governments to produce the correct documents.

Blocking Statute

France has enacted a so-called 'Blocking Statute' (Law No. 68-678 of 26 July 1968 concerning the transmission of documents and information of an economic, commercial, industrial, financial or technical nature to foreign individuals or legal entities). Under this Statute, French residents and nationals and the employees, agents and officers of French companies wherever located are prohibited from disclosing to 'foreign public authorities documents or information of an economic, commercial, industrial, financial or technical nature' when such disclosure is liable to effect French sovereignty, security or 'fundamental economic interests'. Breach of the Blocking Statute, whether oral or written, may be punished by up to 6 months of imprisonment or an €18,000 fine. The Blocking Statue is applicable when either the Hague Convention or the Mutual Assistance Agreement has not been applied. Although the law creating the Blocking Statute dates from 1968, it was not applied until 2007 when the Supreme Court fined a French lawyer €10,000 for transferring information to an American law firm. The French lawyer had phoned a French company, which was a defendant in American proceedings, in order to obtain some information from the company informally (concerning how decisions were made within the French insurance company). The information at stake was not sensitive.

Since this judgment, the Commission nationale de l'informatique et des libertés (CNIL) has been contacted more frequently by lawyers with concerns regarding the Blocking Statute however the Blocking Statute has not subsequently been applied. Moreover, the CNIL does not have the legal authority nor mandate to deal with requests concerning the Blocking Statute. It has asked the government to clarify the law in the area by stating how domestic lawyers are to deal with e-discovery requests from abroad. In 2008 the CNIL issued a press release stating that an inter-ministerial committee had been convened to

consider the issue however no additional information concerning the work of this committee has been released since then and the status quo is unclear.

2.3 Privacy rules governing transfer of information

The Data Protection Act is only relevant to requests for data transfers if the transfer involves the transfer of 'personal data', i.e. data relating to an identified or identifiable person.

Article 7(f) of the Data Protection Directive, transposed into French law by Article 7.5 of the Law on Data Processing and Liberties, provides that personal data may be processed if '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 for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).' This provision is mentioned specifically by the CNIL in its recommendation concerning e-discovery in civil and commercial proceedings and some guidance as to its application is provided. According to the CNIL, the observance of international agreements and applicable national provisions, such as the Hague Convention, is necessary in order to protect the fundamental rights of the person concerned.

The CNIL has emphasised that 'a serious verification of the proportionality and the quality of the data collected and transmitted is fundamental and must be carried out objectively in order to guarantee that only the information legally authorised is transmitted'. In this regard, it recommends the implementation of a filtering operation, to take place in the country where the personal data are located, using 'key words defined in partnership with the legal department and specialised advisors'. It also recommends relying on 'trusted third parties' to verify the proportionality of the data processing. Finally, it highlights that the transmission of information does not necessitate the transmission of personal data in all cases and that anonymisation and pseudonymisation techniques should be used to minimise the transfer of personal data where possible. The CNIL gives an example of previous dealings with the Securities and Exchange Commission where French companies who were initially asked for large volumes of data were able to ultimately transfer redacted data as it was not in fact necessary to transfer the personal data contained therein.

When the transfer of personal data cannot be avoided, it must be limited to 'the identity, responsibilities and contact information of the person concerned; and, information that is strictly related to the litigation in progress'.

Rights of the data subject

The data subject must be informed that personal data concerning him or her is to be/has been transferred to a third country for the purposes of litigation as soon as the data are processed or at the latest when the data is first sent to a third party. The data subject must be informed of the entity responsible for processing, the facts of the proceedings and the existing connection that requires the transmission of his or her personal data, whether or not processing is optional, the consequences for the person in question in the case of a refusal to disclose, the department that may be assigned to the search, the possible transfer

of data to a third country State and the methods for exercising his rights to access, oppose and correct his personal data.

These obligations are limited in circumstances where they may jeopardise the proceedings in question. According to the CNIL, there is an exception to the principle of transparency when 'there is a risk that informing the person concerned will endanger the ability of the party to the proceedings to conduct an investigation or to assemble proof. In such circumstances, the provision of the information to the person concerned may be conducted after the risk is averted.

2.3.1 Initial transfer of information to a third country

'Non-massive' transfers

In France a distinction is made between 'massive' and 'non-massive' transfers of data although no quantifiable criteria are set as to when a certain quantity of data would cross this threshold. When an international transfer of data is made from France to the US, and the transfer is a 'non-massive' one and is non-recurring, Article 69.3 of the 1968 law may be used to justify the transfer for purposes of findings, safeguards or defense of a legal right for the data controller. Although such a transfer must be notified to the CNIL, it does not need CNIL authorisation.

'Massive' transfers

With regard to 'massive' transfers of data which are recurring, the transfer of personal data may take place when the recipient of the data adheres to the Safe Harbour principles, the recipient of the data has signed standard contractual clauses with the data controller in France or when the recipient has implemented binding corporate rules within its group.

2.3.2 Onward transfer of information in a third country

Alternatively, when the personal data concerned has already been the subject of a transfer to the US for a previously authorised purpose, its onward transfer is subject to different provisions. If it is transferred to a judicial authority, the data controller must provide adequate protection for the data, for instance by entering into a stipulative court order. If the data is passed on to a party to the proceedings or a third party, they must make adequate contractual undertakings (or undertake to respect the Safe Harbor clauses in the event of further onward transfer) to ensure the data is correctly safeguarded.

FCPA and France

The national expert was unaware of instances of the application of the FCPA to French nationals. However, France has transposed both the OECD's International Convention on the Fight against Corruption in 2000 and the UN Convention in 2007 and has introduced new crimes relating to corruption into national law as a result. One specificity of the French system is that when the act of corruption takes place outside of the EU, the Minister for Public Prosecutions ('ministère public' or 'parquet') still has the exclusive power to commence an investigation against a French national. Moreover, in order to do so, the Minister for Public Prosecutions must receive a complaint from the victim or a complaint from the country where the act of bribery took place. It is therefore unclear to what extent the French government would cooperate with US authorities in the investigation of an FCPA complaint. However, it should be noted that the US government

could rely on the Mutual Assistance Convention when requesting French cooperation to obtain access to documents that are located in France.

2.4 Policy issues

Strict sanctions are in place for the violation of French data protection laws and the CNIL has been particularly vocal about discussions on cross border transfers in respect of e-Discovery. The CNIL has at its disposal the ability to impose administrative fines up to 5% of the company's gross revenue which in 2009 was capped at €300,000. However, proposals before the French Senate in November 2009 would increase this to €600,000. Since 2005 the CNIL has imposed over €500,000 worth of fines. Finally, there are criminal sanctions available for the breach of French data protection laws of up to five years imprisonment and a fine of €300,000 which may be multiplied five times for companies.

CHAPTER 3 Country Report: Germany

3.1 Introduction

The German Federal Data Protection Act (Bundesdatenschutzgesetz-BDSG) transposes the European Data Protection Directive (Directive 95/46 EC) into German law. As the German system is a federalised one, there is a Federal Data Protection Officer as well as a Data Protection Authority in each of the sixteen *Länder* or States. It is the State Data Protection Authorities that are responsible for the enforcement of the data protection legislation. Sector specific legislation, for instance the Telecommunication Act (Telekommunikationsgesetz-TKG), also exists. In addition, German employment legislation contains some provisions addressing data protection concerns; s. 87 of the Works Constitution Act provides for a right of co-determination for the 'works council' (an employee elected body) regarding 'the introduction and use of technical devices designed to monitor the behaviour or performance of the employees'.

Germany does not have a pre-trial disclosure system such as that in place in the US and other common law jurisdictions. Parties to litigation are obliged only to provide the Court with the documentation necessary to prove that the facts they are asserting before it are true. The German Civil Code of Procedure permits the disclosure of specific documents in the course of proceedings only once a reasoned application for disclosure has been made before it. In practice, such applications for disclosure are rarely made before the Courts. This may be because the parties already possess the relevant documentation to argue their case.

3.2 Transfer of data

3.2.1 General rules governing transfer of information

Germany is party to the *Convention on the Taking of Evidence Abroad in Civil or Commercial Matters* (The Hague Convention) and has invoked the Article 23 exception contained therein. As a result, Germany will not process Letters of Request issued for the purpose of obtaining pre-trial discovery of documents. There has been some academic debate in Germany over this provision however it is usually strictly applied.

With regard to evidence sought in the context of criminal proceedings, cooperation in criminal matters between Germany and the United States is based on the Treaty on Mutual Legal Assistance in Criminal Matters as well as a Supplement Treaty to that Treaty. Article 1(4) of the Treaty provides that assistance shall be provided regardless of whether the conduct in question in the Requesting State would constitute a criminal or

regulatory offense under the laws of the Requested State (unless otherwise provided by the Treaty).

No blocking statute per se exists in German law. However, it is interesting to note that a District Court in Utah has likened the application of the German Federal Data Protection Act to a blocking statute (see further *Accessdata Corporation v. Alste Technologies GmbH*, Case No. 2:08cv569).

3.3 Privacy rules governing transfer of information

The German Data Protection Act distinguishes between processing by public bodies and processing by private bodies. Processing may take place under the Act only if permitted or ordered by the German Data Protection Act or other law, or if the data subject has provided consent (Section 4 of the German Data Protection Act).

As the Act is applied by the State Data Protection Authorities, the decisions of which are not published, it is difficult to advise clients with certainty as to the Act's application. However, each State Data Protection Authority publishes an annual report in which it discusses the issues which have been brought to its attention in the previous year and outlines the solutions reached. The various State Authorities agree on a two-step approach should a company receive an e-discovery request. First, only data that is anonymised should be transferred and second, non-anonymised personal data should only be transferred where strictly necessary. In addition, a Data Protection Authority should be consulted on the transfer.

The German legislation states that the data subject must be informed that his or her personal data has been transferred 'as soon as possible'. Certain exceptions to this rule are expressly set out in the Act: for example, such notification is not required if the data must be kept secret by law or due to the nature of the data, namely due to the overriding legal interests of a third party.

In addition to requiring a justification for the initial and subsequent processing of personal data, German data protection law prohibits the transfer of personal data to countries where an adequate level of data protection cannot be guaranteed (see Section 4b of the German Data Protection Act). In order to ensure that such a level is in place, companies may use pre-approved standard contractual clauses to govern the transfer. Any subsequent amendment of or variation to these standard clauses must be subject to the approval of a competent data protection agency. They may also apply the Safe Harbour principles which allow EU companies to transfer data to US companies that agree to adhere to minimum privacy protection standards. Alternatively, Binding Corporate Rules may be in place which set out the data protection principles applicable within certain corporate groups (this would only be an option when transferring data within a single corporate group).

However, Section 4(c) of the German Data Protection Act provides for certain exceptions, even if an adequate level of data protection cannot be guaranteed: for example, the transfer of personal data abroad is lawful if the data subject has given his consent or if the transfer is necessary or legally required for the establishment, exercise or defence of legal claims within court proceedings. The competent Authorities are of the opinion that e-discovery is not part of the court proceedings, and thus, that this exception cannot apply if a company

seeks documents through e-discovery. Therefore they recommend using the two-step approach instead (e.g., evaluating whether an adequate level of protection can be afforded and secondly determination of consent).

3.4 Policy considerations

The issue of e-discovery has become more prominent in Germany following the amendment of the US Federal Rules of Procedure as German companies are encountering more difficulties complying with their legal obligations. German Authorities have participated in the Sedona Conference and have been in contact with US authorities to discuss possible approaches. There is however, at present, no indication that the law in place will change. Indeed, much of the focus nationally has been on more publicly and politically visible data protection enforcement initiatives, for instance the debate on Google Streetview.

In 2006 the Berlin Data Protection Agency engaged in discussions with a German company involved in a US lawsuit which was asked to provide emails relating to 160 of its employees. Ultimately the company reached an agreement with the regulator using consent as the platform for the onward transfer of personal data in compliance with the requirements of the law.

In terms of enforcement, since 2009 according to Article 43 of the BDSG the Data Protection Authorities can impose fines of up to €300,000 per violation of the BDSG. In addition, the BDSG also allows the confiscation of profits arising out of the particular offence. There is no cap for the sums that may be recovered using this remedy. Fines have become more common in recent years. The highest fine ever imposed by a German data protection authority was for over €1.1 million and was imposed on Deutsche Bahn AG by the Berlin data protection authority for various violations of German Data Protection Law between 2002 and 2007. Fines have also been imposed, for instance, for illegal disclosure of customers' bank account transaction data (North Rhine-Westphalia DPA fined Deutsche Postbank AG €120,000), for illegal retention of sensitive health-related data (Baden-Wurtemberg DPA fined the Müller Group €137,500) and for the illegal recording of employee health data (North Rhine-Westphalia fined a Lidl subsidiary €36,000). From the research conducted, it appears that no prosecutions relating to compliance with e-discovery requests have taken place and the Authorities have demonstrated an understanding of the difficulties faced by companies. Moreover, as Germany does not have a system of pre-trial disclosure, no sanctions have been imposed for failure to produce documents in a discovery context.

3.4.1 Foreign Corrupt Practices Act

In recent years both Siemens and Daimler (both German enterprises) have been fined under the FCPA. The extent to which the German Authorities cooperated in the FCPA proceedings, and in particular the pre-trial discovery process, is unclear.

CHAPTER 4 Country Report: Spain

4.1 Introduction

The Data Protection Directive is transposed in Spain by Organic Law 15/1999 of 13 December on the protection of personal data. Royal Decree 1720/2007 of 21 December approves the regulation implementing the Organic Law and explains the Organic Law in detail. Moreover, the Spanish Data Protection Agency (DPA) issues instructions and orders on particular aspects of data protection law. One such instruction was issued in 2000 concerning international data transfers (Instruction 1/2000). Instruction 1/2000 was then modified by a judgment issued by a National Court on 14 March 2002. Employment legislation does not deal in particular with data protection issues. However, each employment sector is regulated by a Collective Agreement and it is possible that such Collective Agreements contain specific data protection provisions.

Spain is a civil law jurisdiction. In general, there is no obligation on parties to disclose documents pre-trial; there is simply an obligation on the party making a claim before the Court to prove the facts upon which the claim is based. In doing this however, the party making the claim maintains control of the evidence it wishes to use and the documents it wishes to submit to the Court for consideration. Pre-trial discovery, in the US sense, does not exist although Article 328 of the Civil Proceedings Act (Act 1/2000 enacted on 5 January 2001) requires the parties to litigation to disclose documents and/or evidence requested by others and admitted by the Court. Documents requested should be related to the subject matter of the litigation. A petition must be made in the case management hearing seeking such disclosure and copy of the document sought, or a detailed outline of its contents should be provided. This duty of identification severely limits the possibility of securing disclosure of unknown documents. Moreover, the Courts are generally reluctant to look favourably upon wide disclosure requests. However, if a disclosure order is made and a party refuses to comply, they may be subject to criminal sanctions for contempt of court.

4.2 Transfer of data

4.2.1 General rules governing transfer

Spain is party to the *Convention on the Taking of Evidence Abroad in Civil or Commercial Matters* of 18 March 1970 (The Hague Convention) and has invoked the Article 23 exception contained therein. As a result, Spain will not process Letters of Request issued

for the purpose of obtaining pre-trial discovery of documents. If the evidence to be transferred abroad is not for pre-trial discovery, then the rules of The Hague Convention will apply in full to the transfer provided the State to which the evidence is to be transferred is a Contracting State. If the State to which the evidence is to be transferred is not a Contracting State, then it should be examined whether there is a relevant Bilateral Agreement in place.

The transfer of evidence abroad for the purposes of criminal proceedings is governed by bilateral agreements.

4.3 Data Protection rules governing transfer

It follows from Article 287 CPA that evidence that is obtained in violation of constitutional rights is not valid. Disclosure of documents referring to third parties may therefore be refused if they are subject to a confidential business agreement or the rights of the third party (e.g. the right to privacy) would be breached as a result of the disclosure. The Court can order, for instance, partial disclosure to take account of these third party rights.

The Organic Law is applicable in both civil and criminal jurisdictions. Article 11 of the Organic Law states that personal data subjected to processing may be communicated to third persons only for purposes directly related to the legitimate functions of those involved in the transfer and with the prior consent of the data subject. However, the consent of the data subject is not needed when the communication to be effected is destined for, inter alia, judges or courts. Moreover, consent is not needed however if, for instance, the personal data is related to the parties of a contract or preliminary contract for a business, employment or administrative relationship, and they are necessary for its maintenance or fulfilment. In the context of criminal proceedings the Court may waive the applicability of these rules in certain circumstances.

The Organic Law contains specific provisions regulating the transfer of data to third countries. However, it should be highlighted that the controller who transfers the data abroad is not excluded from the application of the rules of the Organic Law. Article 33 sets out a general prohibition on temporary or permanent transfers of personal data to countries which do not provide a comparable level of protection to that provided for by the Organic Law. This prohibition does not apply if a transfer complies with the provisions of the Organic Law and prior authorisation is obtained from the Director of the Data Protection Agency. Moreover, derogations to the general prohibition on international data transfers are set out in Article 34. It states that the general rule does not apply where a) the international transfer of personal data is the result of applying treaties or agreements to which Spain is a party or b) the transfer serves the purposes of offering or requesting international judicial aid.

Title IV of Royal Decree 1720/2007 of 21 December provides further guidance on these provisions of the Organic Law. Article 66 reflects Article 34 of the Organic Law and states that authorisation is not required if the transfer is covered by one of the situations covered by section 34 a) to j) of the Organic Law. However, Article 66(3) of the Royal Decree provides that an international transfer of data shall be notified in order to proceed with its

registration in the General Data Protection Register. In any event, it follows from Articles 67 and 68 of the Royal Decree that the authorisation of the Data Protection Officer is not necessary if either the Spanish Data Protection Agency or the European Commission has issued an adequacy decision (indicating that the third country provides an adequate level of protection) with regard to the Country where the intended data recipient is located.

The Organic Law foresees the possibility for a foreign judicial authority to directly address a contact point in Spain to obtain information for civil or criminal procedures. This contact point is ordinarily the Ministry of Justice. The competent Court in Spain then goes directly to the company or person concerned and the requested information is then returned to the competent Court, which oversees its transfer.

4.4 Policy considerations

Potential conflicts between data protection and e-discovery obligations have not been publicly discussed in Spain. Moreover, there is little awareness of the provisions of the American FCPA Statute in Spain.

CHAPTER 5 Country report: Switzerland

5.1 Introduction

The Swiss Data Protection legislation (Swiss Federal Act of Data Protection of 19 June 1992) pre-dates the European Community' Data Protection Directive (Directive 95/46 EC). Its provisions are however closely aligned to those of the Directive. Several other pieces of Swiss legislation also contain data protection components, for instance banking law provisions and the provisions on professional secrecy set out in the Swiss Penal Code.

Pre-trial discovery, similar to that in place in the US, does not exist in Switzerland. Evidence can be gathered by a judge in limited circumstances, for instance if it is likely to be destroyed. At present, each of the 26 Swiss cantons applies its own procedural rules. Federal procedural rules will be enacted in 2011. In general, Swiss Courts can order litigants or third parties to reveal specific evidence during the course of a trial provided a number of criteria are met.[4]

5.2 Transfer of data

2.1 General rules governing transfer of evidence

Switzerland is a signatory of the *Convention on the Taking of Evidence Abroad in Civil or Commercial Matters* (The Hague Convention) and has invoked its Article 23 exception. This limits Swiss cooperation with pre-trial discovery requests significantly; Switzerland accepts Letters of Request however subject to strict limitations. Letters of Request are not executed if the documentation sought has no direct and necessary link with the proceedings in question, if the Letter of Request requires a person to indicate what documents are in his possession, or if a person is required to produce documents other than those specifically mentioned in the Request. The purpose of these limitations is to

[4] First, the document(s) in question must be described in enough detail to identify them. Second, the document(s) requested must be materially relevant to the outcome of the dispute in question. Third, the burden of proof is on the party seeking disclosure to demonstrate that it has no reasonable alternative way to obtain the evidence. Fourth, the party from whom the evidence is sought may invoke legitimate reasons to resist production. In such a case, the judge must exercise judicial discretion in considering whether the interests of upholding the secrecy of the evidence outweigh the interests of disclosure.

exclude "fishing expeditions". As a result, Letters of Request that are not drafted with these Swiss criteria in mind have little chance of success. On the other hand, once correctly drafted Swiss judges are generally inclined to execute Letters of Request. If execution of a Letter of Request is granted, the person from whom the disclosure is sought may object if he has a privilege or duty to refuse to give the evidence (either under US or Swiss law according to Article 11 of the Convention).Thus, the production of evidence located in Switzerland may be successfully opposed. These defences to the production must be evaluated carefully.

With regard to transfers of evidence for criminal proceedings, a Mutual Legal Assistance Treaty is in force between the USA and Switzerland (U.S. Swiss Legal Assistance Treaty): *The Treaty with the Swiss Confederation on Mutual Assistance in Criminal Matters* (signed at Bern, May 25, 1973; entered into force January 23, 1977). When evidence is sought in the US, a request is filed with the competent US Authorities who then contact the relevant Swiss Authorities to execute the request. A 'blocking statute' is also in place in Switzerland. Article 271 of the Swiss Penal Code prohibits the gathering or taking of evidence in Switzerland for proceedings abroad unless the provisions on mutual assistance are complied with. Breach of this provision is subject to severe penal sanctions including imprisonment. Moreover, Article 273 of the Swiss Penal Code prohibits the disclosure of business secrets of third parties residing in Switzerland to foreign states and foreign entities (including affiliates and parent companies) without the permission of the third parties at issue; the official mutual assistance route must again be followed. Both of these provisions have led to prosecutions however they are not very common.

5.3 Privacy rules governing transfer of information

Article 6 of the Swiss Federal Act of Data Protection governs cross-border disclosure. It prohibits the transfer of personal data abroad if the personal privacy of the persons affected could be seriously endangered, in particular in cases where there is a failure to provide protection equivalent to that provided under Swiss law. It also provides that the Federal Data Protection and Information Commissioner (FDPIC) should be notified in cases where there is no legal obligation to disclose the data and the data subjects have no knowledge that the data will be transmitted. Notification can be exempted by the FDPIC if the processing does not endanger the privacy of the data subject. A list of countries that have sufficient data protection safeguards in place has been created however the US is not on this list. Nevertheless, a "US-Swiss-Safe Harbor Framework" is in place. US companies are able to register and self-certify with the US Department of Commerce that they comply with the data protection principles contained in the US-Swiss Safe Harbor Framework" – rules that are similar to the Safe Harbor system operated with the European Union. If the receiving US company is not registered, standardized 'Transborder Data Flow Agreements' can be conducted and submitted to the FDPIC for approval, according to which the receiver of the data agrees to protect it, not to use the data for purposes other than those for which it was initially transferred and not to make the data publicly available. Under US civil procedure, a judge can issue a 'protective order' to ensure that the transfer of data is possible and to facilitate this process.

In Switzerland a Court Order can be sought to protect evidence. Such an Order can be based on cantonal or federal procedural rules (in particular in IP disputes) or can be made by relying on a general principle of 'fairness' in legal proceedings. As a matter of course data is transferred in redacted or anonymised form although there are no specific guidelines on this matter. The Swiss data protection legislation differs from the European Union legislation in so far as its protection extends to companies as well as natural persons and it does not contain 'transparency' provisions such as those set out in the Directive. Therefore data subjects are not automatically informed that their data has been processed or subject to a data transfer; they must have actively exercise their right to be informed concerning their data by making a request about it.

5.4 Policy issues

E-discovery is not an issue at political level in Switzerland and therefore the legislation in place is unlikely to change in the future. The Data Protection Authorities in the cantons have enforcement powers. Although they can, in principle, sanction cross-border transfers that breach data protection norms such instances are rare. The Data Protection Authorities are happy to be contacted concerning potential data transfers and any issues are resolved on an informal basis hence there is little need for enforcement action.

CHAPTER 6 Country Report: United Kingdom (England and Wales)

6.1 Introduction

The Data Protection Act 1998, which was brought into force on 1st March 2000 by the Data Protection Act 1998 (Commencement) Order 2000 (SI 2000/183), transposed the Data Protection Directive into national law in England and Wales. The Regulation of Investigatory Powers Act 2000 (RIPA) may also be of relevance in the context of international e-disclosure. This particular Act applies, *inter alia*, to interception of communications – which can be relevant in accessing stored e-mails in some circumstances. Moreover, like in other EU countries, the European Data Retention Directive has been transposed by the United Kingdom. This legislation imposes an obligation on communications companies to retain traffic or communications data for a period of 12 months. Different periods of retention of personal data are foreseen by other legislative instruments in the UK, depending on the context.

As a common law jurisdiction, the rules on discovery in England and Wales are more closely aligned to the US rules on discovery than those in most European jurisdictions. Once litigation is pending before the Courts, a party to litigation must disclose the documents on which it intends to rely and any other document which adversely affects its own case, or which affects or supports any other parties' case or which is required to be disclosed by a court practice direction.

6.2 Transfer of data

6.2.1 General rules governing transfer of information

International Conventions

Data transfer from the United Kingdom to non-EU States for the purpose of civil proceedings is governed by the Hague Convention. Under the Convention a judicial authority can be requested to take evidence from a person, or arrange for it to be taken (it is not a request for disclosure of documents). As the UK has used Article 23 to "opt out" of the document disclosure obligations imposed by the Convention, disclosure obligations do not apply to the UK and thus have not been incorporated into the CPR.

The UK has invoked Article 23 in relation to pre-trial discovery:

"*In accordance with Article 23 Her Majesty's Government declare that the United Kingdom will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents. Her Majesty's Government further declare that Her Majesty's Government understand "Letters of Request issued for the purpose of obtaining pre-trial discovery of documents" for the purposes of the foregoing Declaration as including any Letter of Request which requires a person:*

- *to state what documents relevant to the proceedings to which the Letter of Request relates are, or have been, in his possession, custody or power; or*
- *to produce any documents other than particular documents specified in the Letter of Request as being documents appearing to the requested court to be, or to be likely to be, in his possession, custody or power."*

Civil Procedure Rule 34.16 deals with evidence for foreign courts (foreign courts meaning those not in another EU member state, except for Denmark). Applications under the Evidence (Proceedings in Other Jurisdictions) Act 1975 must be made to the High Court supported by written evidence accompanied by the request as a result of which the application is made, and where appropriate, a translation of the request into English. Such an application can be made with or without notice and the request can be to produce documents.

There is no specific rule in the UK prohibiting the destruction of documents after proceedings have been commenced but before an order for disclosure has been made and no direct authority. However, where solicitors are instructed they should, from the outset of the instruction, have advised on the preservation of documents and it may be difficult for the court to resist drawing adverse inferences from the fact that documents have been destroyed. The case of *Douglas v Hello* [2003] gives guidance on the position before proceedings have been commenced. It states that documents must not be destroyed before proceedings are commenced if their destruction is in an attempt to pervert the cause of justice.

With regard to criminal proceedings, the Crime (International Cooperation) Act 2003 provides for judicial authorities in the UK to request and provide evidence requested in relation to criminal proceedings or criminal offences, from other jurisdictions, including the US.

There is no blocking statute in place in the United Kingdom which might impede the transfer of data to third countries for the purposes of pre-trial litigation.

6.2.2 Privacy rules governing transfer of information

According to Schedule 2, paragraph 6 of the Data Protection Act processing may take place where it is 'necessary for the purposes of legitimate interests pursued by the data controller or by the third party to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject'. The processing of data for the purposes in England and Wales for the purposes of future use in pre-trial discovery could therefore potentially be justified on the basis of this provision. Schedule 2, paragraph 6 has been invoked before the Courts on a number of occasions, albeit primarily in the context

of freedom of information cases. The MPs expenses case has summarised the interpretation of this provision as follows:

"It was common ground that "necessary" within schedule 2 para 6 of the DPA should reflect the meaning attributed to it by the European Court of Human Rights when justifying an interference with a recognised right, namely that there should be a pressing social need and that the interference was both proportionate as to means and fairly balanced as to ends.

… The Court has noted that, while the adjective "necessary" within the meaning of article 10(2) is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" and that it implies the existence of a "pressing social need".

There are no published decisions applying this provision to international e-discovery requests. However, it is likely that in the context of an FCPA-related request for data, the fact that England has bribery legislation (the U.K.'s Bribery Act of 2010) that is similar in scope to the FCPA (or even arguably broader) would be a helpful relevant factor in determining that disclosure was in the legitimate interests of the recipients of the data.

There is no specific obligation set out in the Data Protection Act for the data subject to be advised that data relating to him/her has been transferred to a third country. However, in general the Act places a transparency obligation on the data processor/data controller (Schedule 2, para 2(1)) as it provides that data will not be processed fairly unless controllers notify individuals of, inter alia, the purpose(s) of processing. However, there are a number of exemptions to this requirement the most relevant is provided for by section 35 of the Act which permits disclosure where it is required by any enactment, rule of law or order of a court (section 35(1)), or where disclosure is necessary for the purpose of or in connection with any legal proceedings (including prospective legal proceedings) (section 35(2)).

Although it is not explicitly stated in the Data Protection Act, the Information Commissioner's Office (ICO) has indicated in informal guidance that section 35(1) only covers domestic requirements for the disclosure of personal data. However, Section 35(2) is drafted very broadly and equivalent wording relating to international transfers has applied this exemption to proceedings overseas (see *Madoff* below).

There is no guidance on how likely proceedings must be, nor is there any requirement that the individual disclosing the data should be a party to the proceedings. Perhaps as a result, old Legal Guidance issued by the Information Commissioner tries to encourage controllers to be cautious about relying on this condition (page 69): "In many cases, the data controller will not be in a position to make a decision as to whether the necessity test can be met, or will not wish to make the disclosure because of his relationship with the data subject, with the result that the requesting party will have to rely upon a Court Order to obtain the information".

The ICO has moreover issued a 'best practice note' on when information can be disclosed to a private investigator (dated 23 April 2009). This note highlights that the Act generally restricts disclosure of personal information to third parties unless an exemption applies and that even where an exemption from the Act applies an organisation can decide to withhold information from a private investigator unless or until a court orders them to disclose it.

The information may be disclosed when an exemption does not apply if the disclosure is in compliance with the good information handling principles contained in the Act. In addition, the following elements must be present: there must be no overriding duty of confidence in the particular circumstances, the purpose that the information will be used for must be in the legitimate interests of the individual and must not prejudice them in any way and the organisation must subsequently inform them of the unexpected disclosure.

Moreover, the subsequent transfer of data to a third country, such as the US, is governed by Schedule 1 which sets out the data protection principles. Paragraph 8 states that 'personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data'. Schedule 4 of the Data Protection Act sets out cases where this eighth principle does not apply. Paragraph 5 is of relevance in this context. It states that paragraph 8 does not apply where the transfer (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), (b)is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights (see in this regard, *Bernard L Madoff Investment Securities LLC sub nom In the Matter of Madoff Securities International Ltd* [2009] EWHC 442 (Ch)) which held that transfers of personal data to the US could be permitted, *inter alia*, under this condition, where the data was necessary for investigations linked to US proceedings). The Information Commissioner's Office has provided guidance on the international transfer of data in a document entitled 'The eighth data protection principle and international data transfers' published on 28 April 2010. In this document the ICO quotes the example of how the derogation could be invoked cited by the Article 29 Working Party; a parent company based in a third country is sued by an employee of a European subsidiary and the transfer of employee data is necessary for the defence.

However, the proportionality of the disclosure would be analysed under the Data Protection Act. Therefore, for instance, if e-mails were transferred from the UK to the US for the purposes of e-discovery in FCPA proceedings the e-mails would be reviewed both for relevance both to the proceedings and in order to comply with the third data protection principle set out in the Data Protection Act (that personal data not to be excessive in relation to the purpose for which they are processed, in situ discovery) and in order to assess necessity for the legitimate interests tests, the exemption from notice and the exemption to the transfer prohibition principle. It is noteworthy in this context that unopened e-mails (even if corporate) are likely to be regarded as still 'in the course of transmission' and hence covered by the Regulation of Investigatory Powers Act 2000. The Lawful Business Practice Regulations 2000 would entitle the employer, as the system-owner, to access the e-mails on its system inter alia in order to 'establish the existence of facts', however, it must make all reasonable efforts to inform users of the system (in practice, employees) that this is taking place. This would usually be done by an IT-usage/employee monitoring policy. However, if a suitable policy is not in place, then notice should be given. Interception in these circumstances without having given notice would leave a risk of tortious liability to the sender/recipient/intended recipient under section 1(3) of RIPA.

6.3 Policy considerations

At present, the main focus of data protection enforcement is on security breaches and audit; the Commissioner has placed no emphasis on the issue of e-discovery. Moreover, despite the potential negative impact of the Article 29 Working Party's Opinion (WP158) on international transfers of data for e-discovery purposes on the UK, it would appear the Information Commissioner's Office has no intention to dedicate increased resources to e-discovery issues in the future.

While UK practitioners are aware of the existence of FCPA investigations, we are not aware of any cases where it has been applied in relation to UK nationals. The UK's ICO was recently granted powers to impose fines of £500,000 across the private sector but this has not been used to date. It is thought that no enforcement has taken place by the ICO in relation to e-disclosure. Anecdotal evidence from stakeholders in the UK suggests that the ICO has no plans ICO has no plans to issue guidance.