Foreign Corrupt Practices Act Investigations and Privacy Protection
Safeguarding Data and Avoiding Violations of U.S. and International Privacy Laws

A Live 90-Minute Audio Conference with Interactive Q&A

Today's panel features:
James T. Parkinson, Partner, Mayer Brown, Washington, D.C.
Daniel L. Regard, Managing Director, iDiscovery Solutions, Washington, D.C.

Tuesday, August 11, 2009
The conference begins at:
1 pm Eastern
12 pm Central
11 am Mountain
10 am Pacific

The audio portion of this conference will be accessible by telephone only. Please refer to the dial in instructions emailed to registrants to access the audio portion of the conference.

CLICK ON EACH FILE IN THE LEFT HAND COLUMN TO SEE INDIVIDUAL PRESENTATIONS.

If no column is present: click Bookmarks or Pages on the left side of the window.
If no icons are present: Click View, select Navigational Panels, and chose either Bookmarks or Pages.

If you need assistance or to register for the audio portion, please call Strafford customer service at 800-926-7926 ext. 10
FCPA Investigations and Privacy Protection

*Safeguarding Data and Avoiding Violations of International Privacy Laws*

James T. Parkinson
Joseph R. Baker
*Mayer Brown LLP*

Daniel L. Regard
*iDiscovery Solutions, Inc.*

August 11, 2009
Oil in Azerbaijan

Shipping in Nigeria

Drilling in Argentina

Politics in Louisiana

Movies in Bangkok

Nuclear valves in China

Anything in Bulgaria

Construction in Bolivia

Nutritional products in Brazil
Hypothetical FCPA Scenario

• Thursday afternoon phone call: General counsel wants to discuss an FCPA concern.

• Anonymous email alleges that a sales manager based in Germany was paying bribes to sell the client’s products to the Indian government.

• Overnight, the security department imaged the German sales manager’s laptop and the exchange email server.

• Sales manager will be in Delhi Monday morning.

• What do you set in place before boarding the flight to Delhi?

• What are the issues for managing electronic data in this FCPA investigation?
Overview of the FCPA

• Anti-Bribery Provisions
  – Offer, promise or payment of money or anything of value
  – To a foreign official
  – Corruptly and willfully
  – With knowledge
  – An improper purpose
  – In order to obtain or retain business

• Accounting Provisions
  – Applicable to “Issuers”
  – Make and keep accurate books and records
  – Devise and maintain a system of internal accounting controls
Overview of the FCPA (cont’d)

• Heightened enforcement activity over the past few years
• Corporate penalties reaching new heights
  – Siemens: Over $1 billion
  – KBR/Halliburton: $579 million
  – Past two weeks have seen flurry of activity
• Prosecutions a reality for individuals
  – Prison time: Recent plea agreement for 7-year term
  – From the CEO, to sales managers, to consultants
  – First part of 2009 has been most active year for individuals prosecutions yet.
• Greater cooperation among enforcement authorities
FCPA Applied to the Hypothetical

• Jurisdiction
  – U.S.-based multinational, either an issuer or domestic concern

• Anti-Bribery Elements
  – Payment of money to a foreign official
  – With knowledge and an improper purpose
  – To obtain business

• Accounting Elements
  – Unknown how booked
  – Internal controls environment unknown
Overview of Investigative Goals

• Ensure that there is no ongoing conduct of concern
• Preserve the evidence and develop the facts
• Provide legal advice and represent client as the circumstances mandate
Investigative Goals

• Ensure that there is no ongoing conduct of concern
  – If the allegation is true, what needs to be done to stop the conduct?
  – Why is the sales manager in India?
  – Who else does the sales manager work with?
  – What other countries?
  – What other customers?
  – Any prior allegations regarding this person, this division, this country, this company?
Investigative Goals (cont’d)

• Preserve the evidence and develop the facts
  – Conduct the investigation in a principled, defensible manner
    • Assume that will have to report to the Board, the Audit Committee, auditors, and US enforcement authorities
  – Identify universe of custodians and information
    • Hypothetical: Sales
    • Possible additional functions: Procurement, audit, accounting, controller, operations, HR, legal, compliance, tax, treasury, regulatory, government relations, public affairs/communications, supply chain management
  – Identify applicable jurisdictions
    • Hypo: US, Germany, India
Investigative Goals (cont’d)

• Provide legal advice and represent client as the circumstances mandate
  – Legal analysis of the facts: Was there an FCPA violation?
    • If yes, what needs to be done by way of remediation, compliance enhancement, disclosure?
  – Protect client’s legal privileges
  – Data protection and privacy
  – Local law
  – HR concerns
International Data Protection Issues - Overview

• Many foreign countries – and the EU in particular – restrict or prohibit the processing and transfer of personal data

• We Will Address:
  1. The source of U.S. conflict with foreign data protection laws
  2. A review of the European data protection framework, the obstacles presented and some of the available exceptions
  3. Practical advice to help identify and address data protection concerns, at the outset of investigation and as it proceeds
  4. Longer-term enterprise-wide approaches to data protection compliance
  5. The outlook for resolving this cross-border “Catch-22”
International Privacy / Data Protection

1. Sources of Cross-Border Conflict

Differing Conceptions of “Privacy” and “Discovery”

• Privacy as a fundamental right overseas
  – Can extend to employee’s use of employer systems

• Discovery rules overseas
  – Not as liberal and wide-ranging as in U.S.

• Two main types of relevant foreign laws:
  – Privacy / Data protection – protecting the privacy rights of foreign citizens
  – “Blocking” statutes – protecting foreign citizens from invasive U.S.-style discovery
International Privacy / Data Protection

2a. EU Data Protection Framework

European Union 1995 data protection directive

• “Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to processing of personal data.”

• Restricts the “processing” and transfer of “personal data”
  – These terms are broadly defined

• Provides for notice to affected employees, including target of investigation

• Implemented differently in each EU member state
International Privacy / Data Protection

2b. Potential Exceptions to EU Data Protection Laws

Many Exceptions, But Not All Are Available

• Consent of data subject (difficult to achieve)
• Legal obligation (narrowest interpretation)
• Pursuit of legitimate interest (most promising)
• Whistleblower exceptions to notice requirements
• Exceptions to transfer restrictions
International Privacy / Data Protection

3a. Steps to take at the outset of investigation

• Determine relevant jurisdictions. Possible factors:
  – Relevant employees’ duty station, nationality?
  – Type and location of relevant data?

• Determine relevant restrictions. Sources of guidance:
  – Counsel – Early consultation with local counsel is essential – even within Europe
  – DPAs – Consultation with data protection authorities can be helpful; sometimes it is required
3b. Steps to take at the outset of investigation

• Initial data preservation considerations

  – What other employees are likely targets?
  – Is the Hard Drive a red-herring? (What other systems of communication likely have data?)
  – What other systems will (sooner or later) be involved in a broader FCPA investigation? (e.g. Accounting? Invoicing? Inventory? Shipping?)
  – What cascading investigations or litigations are likely to arise from an FCPA investigation? (e.g. Is the company publicly traded?)

• Need to balance investigative needs with avoidance of unnecessary data processing – i.e., privacy concerns counsel for narrow tailoring of preservation and processing
International Privacy / Data Protection

3c. Immediate steps to take

• Before You Board The Plane:
  – Instruct the security department not to transport the hard drive or server images
  – Immediately begin considering the types of data you will need to access and preserve
    • This is important for determining what to preserve, as well as what jurisdictions’ laws may apply
  – Reach out to counsel regarding data protection rules in Germany and India, and any other potentially relevant jurisdictions
International Privacy / Data Protection

3d. Steps to implement as the investigation proceeds

• It may be impossible to fully reconcile desire to fully investigate and cooperate under the FCPA with perfect data protection compliance

• But there are ways to limit exposure as you process and review:
  – Limit Collection: Early, narrow filtering of data in EU, in-country, or onsite
  – Local Review: EU or in-country processing and review
  – Anonymization: Redaction of identifying information to permit transfer
International Privacy / Data Protection

3e. Steps to implement as the investigation proceeds

• Consider methods for eventually qualifying for an exception to the restrictions on transfer of data out of the EU:
  – Safe harbor
  – Binding Corporate Rules
  – Model Contracts
  – Hague Evidence Convention
  – Transfers within EU
  – Certificate of Compliance
International Privacy / Data Protection

4. Longer-term preventative measures

• Consider enterprise-level measures to reduce risk of violations in international investigations and e-discovery
  – Internal “responsible persons” to monitor regulations and maximize compliance
  – Privacy and Document Retention Policies / Training – Increase internal transparency as to discovery practices
  – Advance consent of “high risk” or key employees
  – Overseas employment agreements
5. The state of the cross-border policy debate

• Is there a resolution in sight?
  – Current US – EU dialogue
  – Public law always takes time
  – Possibilities for relief:
    • Streamlined EU compliance procedures, such as a *certification of compliance* by counsel
    • Increased U.S. Court recognition of legitimacy of foreign restrictions
    • Recent Mutual Legal Assistance Treaties
    • Update to the Hague Convention
QUESTIONS?

• James Parkinson
  – + 202 363 3385
  – jparkinson@mayerbrown.com

• Joe Baker
  – + 202 263 3294
  – jbaker@mayerbrown.com

• Dan Regard
  – + 202 550 4764
  – dregard@idiscoverysolutions.com
Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime

Adopted on 1 February 2006
TABLE OF CONTENTS

I. INTRODUCTION.........................................................................................................................4

II. JUSTIFICATION FOR THE LIMITED SCOPE OF THE OPINION ..................................5

III. PARTICULAR EMPHASIS PUT BY DATA PROTECTION RULES ON THE PROTECTION OF THE PERSON INCrimINATED THROUGH A WHISTLEBLOWING SCHEME .................................................................6

IV. ASSESSMENT OF THE COMPATIBILITY OF WHISTLEBLOWING SCHEMES WITH DATA PROTECTION RULES .................................................................................................................................7

1. Legitimacy of whistleblowing systems (Article 7 of Directive 95/46/EC) .................................................................7
   i) Establishment of a whistleblowing system necessary for compliance with a legal obligation to which the controller is subject (Article 7(c)) ...........................................................................7
   ii) Establishment of a whistleblowing system necessary for the purposes of a legitimate interest pursued by the controller (Article 7(f)) ......................................................................................8

2. Application of the principles of data quality and proportionality (Article 6 of the Data Protection Directive) ......................................................9
   i) Possible limit on the number of persons entitled to report alleged improprieties or misconduct through whistleblowing schemes.................................................................10
   ii) Possible limit on the number of persons who may be incriminated through a whistleblowing scheme ......................................................10
   iii) Promotion of identified and confidential reports as against anonymous reports.................................................................10
   iv) Proportionality and accuracy of data collected and processed........12
   v) Compliance with strict data retention periods.........................12

3. Provision of clear and complete information about the scheme (Article 10 of the Data Protection Directive) .................................13

4. Rights of the incriminated person.................................................13
   i) Information rights......................................................................13
   ii) Rights of access, rectification and erasure.................................14

5. Security of processing operations (Article 17 of Directive 95/46/EC) .........................................................................................14
   i) Material security measures..........................................................14
   ii) Confidentiality of reports made through whistleblowing schemes .................................................................................................14

6. Management of whistleblowing schemes........................................15
   i) Specific internal organisation for the management of whistleblowing schemes........................................................................15
ii) Possibility of using external service providers............................... 16

iii) Principle of investigation in the EU for EU companies and exceptions.......................................................................................... 16

7. Transfers to third countries................................................................................................................ 17

8. Compliance with notification requirements ...................................................................................... 17

V – CONCLUSIONS ................................................................................................................................ 18
THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA


Having regard to Articles 29 and 30(1)(c) and (3) of that Directive,

Having regard to its Rules of Procedure, and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

This opinion provides guidance on how internal whistleblowing schemes can be implemented in compliance with the EU data protection rules enshrined in Directive 95/46/EC.²

The number of issues raised by the implementation of whistleblowing schemes in Europe in 2005, including data protection issues, has shown that the development of this practice in all EU countries can face substantial difficulties. These difficulties are largely owed to cultural differences, which themselves stem from social and/or historical reasons that can neither be denied nor ignored.

The Working Party is aware that these difficulties are partly related to the breadth of the scope of issues which may be reported through internal whistleblowing schemes. It is also aware that whistleblowing schemes raise specific difficulties in some EU countries with regard to labour law aspects, and that work is ongoing on these issues which will require further attention. The Working Party also needs to take into account the fact that in some EU countries the functioning of whistleblowing schemes is provided for by law, while in the majority of EU countries no specific legislation or regulation exists on this issue.

As a result, the Working Party deems it premature to adopt a final opinion on whistleblowing in general at this stage. By adopting this opinion, it has decided to address those issues on which EU guidance is most urgently needed. Considering this, and for reasons mentioned in the document, this opinion is formally limited to the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.


² In accordance with the specific mandate of the Working Party, this working document does not address other legal difficulties raised by whistleblowing schemes, in particular in relation to labour law and criminal law.
The Working Party adopted this opinion on the clear understanding that it needs to further reflect on the possible compatibility of EU data protection rules with internal whistleblowing schemes in other fields than the ones just mentioned, such as human resources, workers’ health and safety, environmental damage or threats, and commission of offences. It will pursue its analysis over the coming months to determine whether EU guidance is also needed on these issues, in which case the principles developed in this document might be supplemented or adapted in a subsequent document.

II. JUSTIFICATION FOR THE LIMITED SCOPE OF THE OPINION

The Sarbanes-Oxley Act (SOX) was adopted by the US Congress in 2002 following various corporate financial scandals.

SOX requires publicly held US companies and their EU-based affiliates, as well as non-US companies, listed in one of the US stock markets to establish, within their audit committee, “procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters”. In addition, Section 806 of SOX lays down provision aimed at ensuring the protection for employees of publicly traded companies who provide evidence of fraud from retaliatory measures taken against them for making use of the reporting scheme. The Securities and Exchange Commission (SEC) is the US authority in charge of monitoring the application of SOX.

These provisions are mirrored in the Nasdaq and New York Stock Exchange (NYSE) rules. If listed on either Nasdaq or NYSE, companies must certify their accounts to those markets yearly. This certification process implies that companies are in a position to assert that they comply with a number of rules, including whistleblowing rules.

Companies which fail to comply with these whistleblowing requirements are subject to heavy sanctions and penalties by Nasdaq, NYSE or the SEC. As a result of the uncertainty as to the compatibility of whistleblowing schemes with EU data protection rules, the companies concerned are facing risks of sanctions from EU data protection authorities if they fail to comply with EU data protection rules, on the one hand, and from US authorities if they fail to comply with US rules, on the other.

The applicability of some SOX provisions to European subsidiaries of US companies and to European companies listed in US stock markets is at present under judicial review in

3 Sarbanes-Oxley Act, Section 301(4).
4 Sarbanes-Oxley Act, Section 406, and, more particularly, regulations enacted by major US stock exchange institutions (NASDAQ, NYSE) also lay down that companies listed in those markets adopt “codes of ethics” applicable to senior financial officers and directors, concerning accounting, reporting and auditing matters, that should provide for enforcement mechanisms.

5 Rule 4350 (d) (3): “Audit Committee Responsibilities and Authority”
6 New York Stock Exchange (NYSE), Section 303A.06: “Audit Committee”
the United States.\(^7\) Despite this relative uncertainty as to the applicability of all of the SOX provisions to companies established in Europe, companies which are subject to SOX on the basis of clear extraterritorial provisions in this Act also want to be in a position to comply with the specific whistleblowing provisions of SOX.

Due to the risk of sanctions facing EU companies, the WP29 has deemed it urgent to concentrate its analysis primarily on whistleblowing systems established for the reporting of potential breaches in accounting, internal accounting control and auditing matters, such as referred to in the Sarbanes-Oxley Act, and on related matters mentioned below. In so doing, the Working Party intends to contribute to the provision of legal certainty to companies which are subject both to EU data protection rules and to SOX.

### III. PARTICULAR EMPHASIS PUT BY DATA PROTECTION RULES ON THE PROTECTION OF THE PERSON INCriminated THROUGH A WHISTLEBLOWING SCHEME

Internal whistleblowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of companies. Whistleblowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel. It supplements the organisation’s regular information and reporting channels, such as employee representatives, line management, quality control personnel or internal auditors who are employed precisely to report such misconducts. Whistleblowing should be viewed as subsidiary to, and not a replacement for, internal management.

The Working Party stresses that whistleblowing schemes must be implemented in compliance with EU data protection rules. As a matter of fact, the implementation of whistleblowing schemes will in the vast majority of cases rely on the processing of personal data (i.e. on the collection, registration, storage, disclosure and destruction of data related to an identified or identifiable person), meaning that data protection rules are applicable.

Application of these rules will have different consequences on the set-up and management of whistleblowing schemes. The whole range of these consequences is detailed below in this document (see Section IV).

The Working Party notes that while existing regulations and guidelines on whistleblowing are designed to provide specific protection to the person making use of the whistleblowing scheme (“the whistleblower”), they never make any particular mention of the protection of the accused person, particularly with regard to the processing of his/her personal data. Yet, even if accused, an individual is entitled to the rights he/she is granted under Directive 95/46/EC and the corresponding provisions of national law.

---

\(^7\) The U.S. Court of Appeals (1st Circuit) held on 5 January 2006 that SOX provisions on the protection of whistleblowers do not apply to foreign citizens working outside the US for foreign subsidiaries of companies required to comply with the remaining provisions of SOX.
Applying EU data protection rules to whistleblowing schemes means giving specific consideration to the issue of the protection of the person who may have been incriminated in an alert. In this respect, the Working Party stresses that whistleblowing schemes entail a very serious risk of stigmatisation and victimisation of that person within the organisation to which he/she belongs. The person will be exposed to such risks even before the person is aware that he/she has been incriminated and the alleged facts have been investigated to determine whether or not they are substantiated.

The Working Party is of the view that proper application of data protection rules to whistleblowing schemes will contribute to alleviate the above-mentioned risks. It also takes the view that, far from preventing these schemes from functioning in accordance with their intended purpose, application of these rules will generally contribute to the proper functioning of whistleblowing schemes.

IV. ASSESSMENT OF THE COMPATIBILITY OF WHISTLEBLOWING SCHEMES WITH DATA PROTECTION RULES

The application of data protection rules to whistleblowing schemes implies dealing with the question of the legitimacy of whistleblowing systems (1); application of the principles of data quality and proportionality (2); the provision of clear and complete information about the scheme (3); the rights of the person incriminated (4); the security of processing operations (5); the management of internal whistleblowing schemes (6); issues related to international data transfers (7); notification and prior checking requirements (8).

1. Legitimacy of whistleblowing systems (Article 7 of Directive 95/46/EC)

For a whistleblowing scheme to be lawful, the processing of personal data needs to be legitimate and satisfy one of the grounds set out in Article 7 of the data protection Directive.

As things stand, two grounds appear to be relevant in this context: either the establishment of a whistleblowing system is necessary for compliance with a legal obligation (Article 7(c)) or for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed (Article 7(f)).

i) Establishment of a whistleblowing system necessary for compliance with a legal obligation to which the controller is subject (Article 7(c))

The establishment of a reporting system should have the purpose of meeting a legal obligation imposed by Community or Member State law, and more specifically a legal obligation designed to establish internal control procedures in well-defined areas.

At the present time, such an obligation exists in most EU Member States in the banking sector, for instance, where governments have decided to strengthen internal control, in particular with regard to the activities of credit and investment companies.

8 Companies should be aware that in some Member States the processing of data on suspected criminal offences is subject to further specific conditions relating to the legitimacy of their processing (see infra, section IV, 8).
Such a legal obligation to put in place reinforced control mechanisms also exists in the context of combating bribery, in particular as a result of the implementation in national law of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD Convention of 17 December 1997).

By contrast, an obligation imposed by a foreign legal statute or regulation which would require the establishment of reporting systems may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC. As a result, SOX whistleblowing provisions may not be considered as a legitimate basis for processing on the basis of Article 7(c).

However, in certain EU countries whistleblowing schemes may have to be put in place by way of legally binding obligations of national law in the same fields as those covered by SOX. In other EU countries where such legally binding obligations do not exist, the same result may, however, be achieved on the basis of Article 7(f).

\[ ii) \text{ Establishment of a whistleblowing system necessary for the purposes of a legitimate interest pursued by the controller (Article 7(f))} \]

The establishment of reporting systems may be found necessary for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed (Article 7(f)). Such a reason would only be acceptable on condition that such legitimate interests are not “overridden by the interests for fundamental rights and freedoms of the data subject”.

Major international organisations, including the EU and the OECD, have recognised the importance of relying on good corporate governance principles to ensure the adequate functioning of organisations. The principles or guidelines developed in these forums consist in enhancing transparency, developing sound financial and accounting practices, and thus improving the protection of stakeholders and the financial stability of markets. They specifically recognise an organisation’s interest in putting in place appropriate procedures enabling employees to report irregularities and questionable accounting or auditing practices to the board or the audit committee. These reporting procedures must ensure that arrangements are in place for the proportionate and independent investigation of facts reported, which includes an adequate procedure of selection of the persons involved in the management of the scheme, and for appropriate follow-up action.

---

9 Dutch Corporate Governance Code, 9.12.2003, Section II, 1.6
Spanish Draft of Unified Code on corporate governance of listed companies, Chapter IV, 67(1)d). This Code has still to be examined by the Spanish Data Protection Authority in order to consider data protection implications.


11 OECD: OECD Principles of Corporate Governance. 2004. Part One, Section IV.
Moreover, these guidelines and regulations stress that the protection of whistleblowers should be ensured and there should be appropriate guarantees protecting whistleblowers against retaliatory measures (discriminatory or disciplinary actions).\textsuperscript{12}

Indeed, the goal of ensuring financial security in international financial markets and in particular the prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing matters and reporting as well as the fight against bribery, banking and financial crime or, insider trading appears to be a legitimate interest of the employer that justifies the processing of personal data by means of whistleblowing systems in these areas. Ensuring that reports on suspected accounting manipulations or defective account auditing, which may have an impact on the financial statements of the company and concern the legitimate interests of stakeholders in the financial stability of the company, actually reach the Board of directors with a view to appropriate follow-up is a critical concern for a public company, especially those listed in financial markets.

In this context, the US Sarbanes-Oxley Act may be considered as one of these initiatives adopted to ensure the stability of financial markets and the protection of legitimate interests of stakeholders by laying down rules that guarantee appropriate corporate governance of companies.

For all these reasons, the Working Party considers that in those EU countries where there is no specific legal requirement imposing the implementation of whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, and combating against bribery, banking and financial crime, data controllers still hold a legitimate interest in implementing such internal schemes in those fields.

However, Article 7(f) requires a balance to be struck between the legitimate interest pursued by the processing of personal data and the fundamental rights of data subjects. This balance of interest test should take into account issues of proportionality, subsidiarity, the seriousness of the alleged offences that can be notified and the consequences for the data subjects. In the context of the balance of interest test, adequate safeguards will also have to be put in place. In particular, Article 14 of Directive 95/46/EC provides that, when data processing is based on Article 7(f), individuals have the right to object at any time on compelling legitimate grounds to the processing of the data relating to them. These points are developed below.

\textbf{2. Application of the principles of data quality and proportionality (Article 6 of the Data Protection Directive)}

In accordance with Directive 95/46/EC, personal data must be processed fairly and lawfully;\textsuperscript{13} they must be collected for specified, explicit and legitimate purposes\textsuperscript{14} and not be used for incompatible purposes.\textsuperscript{14} Moreover, the processed data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.\textsuperscript{15} Combined, these latter rules are sometimes referred to as the

\begin{itemize}
\item \textsuperscript{12} See, for instance, UK Public Interest Disclosure Act 1998.
\item \textsuperscript{13} Article 6(1)(a) Directive 95/46/CE
\item \textsuperscript{14} Article 6(1)(b) Directive 95/46/CE
\item \textsuperscript{15} Article 6(1)(c) Directive 95/46/CE
\end{itemize}
“proportionality principle”. Finally, appropriate measures have to be taken to ensure that data which are inaccurate or incomplete are erased or rectified.\textsuperscript{16} The application of these essential data protection rules has a number of consequences as to the way in which reports may be made by an organisation’s employees and processed by that organisation. These consequences are studied below.

i) Possible limit on the number of persons entitled to report alleged improprieties or misconduct through whistleblowing schemes

In application of the proportionality principle, the Working Party recommends that the company responsible for the whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistleblowing scheme, in particular in the light of the seriousness of the alleged offences to be reported. The Working Party acknowledges, however, that the categories of personnel listed may sometimes include all employees in some of the fields covered by this opinion.

The Working Party is aware that the circumstances of each case will be decisive. Thus, it does not want to be prescriptive on this point and leaves it to data controllers, with possible verification by the competent authorities, to determine whether such restrictions are appropriate in the specific circumstances in which they operate.

ii) Possible limit on the number of persons who may be incriminated through a whistleblowing scheme

In application of the proportionality principle, the Working Party recommends that the company putting in place a whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported. The Working Party acknowledges, however, that the categories of personnel listed may sometimes include all employees in some of the fields covered by this opinion.

The Working Party is aware that the circumstances of each case will be decisive. Thus, it does not want to be prescriptive on this point and leaves it to data controllers, with possible verification by the competent authorities, to determine whether such restrictions are appropriate in the specific circumstances in which they operate.

iii) Promotion of identified and confidential reports as against anonymous reports

The question of whether whistleblowing schemes should make it possible to make a report anonymously rather than openly (i.e. in an identified manner, and in any case under conditions of confidentiality) deserves specific attention.

Anonymity might not be a good solution, for the whistleblower or for the organisation, for a number of reasons:

- being anonymous does not stop others from successfully guessing who raised the concern;
- it is harder to investigate the concern if people cannot ask follow-up questions;

\textsuperscript{16} Article 6(1)(d) Directive 95/46/CE
- it is easier to organise the protection of the whistleblower against retaliation, especially if such protection is granted by law,\textsuperscript{17} if the concerns are raised openly;
- anonymous reports can lead people to focus on the whistleblower, maybe suspecting that he or she is raising the concern maliciously;
- an organisation runs the risk of developing a culture of receiving anonymous malevolent reports;
- the social climate within the organisation could deteriorate if employees are aware that anonymous reports concerning them may be filed through the scheme at any time.

As far as data protection rules are concerned, anonymous reports raise a specific problem with regard to the essential requirement that personal data should only be collected fairly. As a rule, the Working Party considers that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement.

However, the Working Party is aware that some whistleblowers may not always be in a position or have the psychological disposition to file identified reports. It is also aware of the fact that anonymous complaints are a reality within companies, even and especially in the absence of organised confidential whistleblowing systems, and that this reality cannot be ignored. The Working Party therefore considers that whistleblowing schemes may lead to anonymous reports being filed through the scheme and acted upon, but as an exception to the rule and under the following conditions.

The Working Party considers that whistleblowing schemes should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint. In particular, companies should not advertise the fact that anonymous reports may be made through the scheme. On the contrary, since whistleblowing schemes should ensure that the identity of the whistleblower is processed under conditions of confidentiality, an individual who intends to report to a whistleblowing system should be aware that he/she will not suffer due to his/her action. For that reason a scheme should inform the whistleblower, at the time of establishing the first contact with the scheme, that his/her identity will be kept confidential at all the stages of the process and in particular will not be disclosed to third parties, either to the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. It is also necessary to make whistleblowers aware that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of the enquiry conducted by the whistleblowing scheme.

The processing of anonymous reports must be subject to special caution. Such caution would, for instance, require examination by the first recipient of the report with regard to its admission and the appropriateness of its circulation within the framework of the scheme. It might also be worth considering whether anonymous reports should be investigated and processed with greater speed than confidential complaints because of the risk of misuse. Such special caution does not mean, however, that anonymous reports should not be investigated without due consideration for all the facts of the case, as if the report were made openly.

\textsuperscript{17} E.g. under the UK Public Interest Disclosure Act
iv) Proportionality and accuracy of data collected and processed

In accordance with Article 6(1)(b) & (c) of the Data Protection Directive, personal data has to be collected for specified, explicit and legitimate purposes and must be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.

Given that the purpose of the reporting system is to ensure proper corporate governance, the data collected and processed through a reporting scheme should be limited to facts related to this purpose. Companies setting up these systems should clearly define the type of information to be disclosed through the system, by limiting the type of information to accounting, internal accounting controls or auditing or banking and financial crime and anti-bribery. It is recognised that in some countries the law may expressly provide for whistleblowing schemes also to be applied to other categories of serious wrongdoing that may need to be disclosed in the public interest\(^\text{18}\) but these are outside the scope of this opinion; they may not apply in other countries. The personal data processed within the scheme should be limited to the data strictly and objectively necessary to verify the allegations made. In addition, complaint reports should be kept separate from other personal data.

When facts reported to a whistleblowing scheme do not relate to the areas of the scheme in question, they could be forwarded to proper officials of the company/organisation when the vital interests of the data subject or moral integrity of employees are at stake, or when, under national law there is a legal obligation to communicate the information to public bodies or authorities competent for the prosecution of crimes.

v) Compliance with strict data retention periods

Directive 95/46/EC lays down that personal data processed shall be kept for the period of time necessary for the purpose for which the data have been collected or for which they are further processed. This is essential to ensure compliance with the principle of proportionality of the processing of personal data.

Personal data processed by a whistleblowing scheme should be deleted, promptly, and usually within two months of completion of the investigation of the facts alleged in the report.

Such periods would be different when legal proceedings or disciplinary measures are initiated against the incriminated person or the whistleblower in cases of false or slanderous declaration. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Such retention periods will be determined by the law of each Member State.

Personal data relating to alerts found to be unsubstantiated by the entity in charge of processing the alert should be deleted without delay.

\(^{18}\) For instance, UK Public Interest Disclosure Act 1998.
Furthermore, any national rules relating to archiving of data in the company remain applicable. These rules may in particular access to the data kept in such archives, and specify the purposes for which such access is possible, the categories of persons who may have access to those files, and all other relevant security regulations.

3. **Provision of clear and complete information about the scheme (Article 10 of the Data Protection Directive)**

The requirement of clear and complete information on the system obliges the controller to inform data subjects about the existence, purpose and functioning of the scheme, the recipients of the reports and the right of access, rectification and erasure for reported persons.

Data controllers should also provide information on the fact that the identity of the whistleblower shall be kept confidential throughout the whole process and that abuse of the system may result in action against the perpetrator of the abuse. On the other hand, users of the system may also be informed that they will not face any sanctions if they use the system in good faith.

4. **Rights of the incriminated person**

The legal framework set by Directive 95/46/EC specifically emphasises the protection of the data subject’s personal data. Accordingly, from a data protection point of view, whistleblowing schemes should focus on the data subject’s rights, without damage to the whistleblower’s ones. A balance of interests should be established between the rights of the parties concerned, including the company’s legitimate investigation needs.

i) **Information rights**

Article 11 of Directive 95/46/EC requires individuals to be informed when personal data are collected from a third party and not from them directly.

The person accused in a whistleblower’s report shall be informed by the person in charge of the scheme as soon as practicably possible after the data concerning them are recorded. Under Article 14, they also have the right to object to the processing of their data if the legitimacy of the processing is based on Article 7(f). This right of objection, however, may be exercised only on compelling legitimate grounds relating to the person’s particular situation.

In particular, the reported employee must be informed about: [1] the entity responsible for the whistleblowing scheme, [2] the facts he is accused of, [3] the departments or services which might receive the report within his own company or in other entities or companies of the group of which the company is part, and [4] how to exercise his rights of access and rectification.

However, where there is substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather the necessary evidence, notification to the incriminated individual may be delayed as long as such risk exists. This exception to the rule provided by Article 11 is intended to preserve evidence by preventing its destruction or alteration by the incriminated person. It must be applied restrictively, on a case-by-case basis, and it should take account of the wider interests at stake.
The whistleblowing scheme should take the necessary steps to ensure that the information disclosed will not be destroyed.

**ii) Rights of access, rectification and erasure**

Article 12 of Directive 95/46/EC gives the data subject the possibility to have access to data registered on him/her in order to check its accuracy and rectify it if it is inaccurate, incomplete or outdated (right of access and rectification). As a consequence, the setting-up of a reporting system needs to ensure compliance with individuals’ right to access and rectify incorrect, incomplete or outdated data.

However, the exercise of these rights may be restricted in order to ensure the protection of the rights and freedoms of others involved in the scheme. This restriction should be applied on a case-by-case basis.

Under no circumstances can the person accused in a whistleblower’s report obtain information about the identity of the whistleblower from the scheme on the basis of the accused person’s right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower’s confidentiality should always be guaranteed.

In addition, data subjects have the right to rectify or erase their data where the processing of such data does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data (Article 12(b)).

5. **Security of processing operations (Article 17 of Directive 95/46/EC)**

**i) Material security measures**

In accordance with Article 17 of Directive 95/46/EC, the company or organisation responsible for a whistleblowing scheme shall take all reasonable technical and organisational precautions to preserve the security of the data when it is gathered, circulated or conserved. Its aim is to protect data from accidental or unlawful destruction or accidental loss and unauthorised disclosure or access.

The reports may be collected by any data processing means, whether electronic or not. Such means should be dedicated to the whistleblowing system in order to prevent any diversion from its original purpose and for added data confidentiality.

These security measures must be proportionate to the purposes of investigating the issues raised, in accordance with the security regulations established in the different Member States.

Where the whistleblowing scheme is run by an external service provider, the data controller needs to have in place a contract for adequacy and, in particular, take all the appropriate measures to guarantee the security of the information processed throughout the whole process.

**ii) Confidentiality of reports made through whistleblowing schemes**

Confidentiality of reports is an essential requirement to meet the obligation provided for by Directive 95/46/EC to comply with the security of processing operations.
In order to meet the objective for which a whistleblowing scheme has been established and encourage persons to make use of the scheme and report facts which may show misconduct or illegal activities by the company, it is essential that the person who reports be adequately protected, by guaranteeing the confidentiality of the report and preventing third parties from knowing his/her identity.

Companies establishing whistleblowing schemes should adopt the appropriate measures to guarantee that the whistleblowers’ identity remains confidential and is not disclosed to the incriminated person during any investigation. However, if a report is found to be unsubstantiated and the whistleblower to have maliciously made a false declaration, the accused person may want to pursue a case for libel or defamation, in which case the whistleblower's identity may have to be disclosed to the incriminated person if national law allows. National laws and principles on whistleblowing in the field of corporate governance also provide for the whistleblower to be protected from retaliatory measures for making use of the scheme, such as disciplinary or discriminatory action being taken by the company or the organisation.

The confidentiality of personal data must be guaranteed when it is collected, disclosed or stored.

6. Management of whistleblowing schemes

Whistleblowing schemes require careful consideration of how the reports are to be collected and handled. While favouring internal handling of the system, the Working Party acknowledges that companies may decide to use external service providers to which they outsource part of the scheme, mainly for the collection of the reports. These external providers must be bound by a strict obligation of confidentiality and commit themselves to complying with data protection principles. Whatever the system established by a company, the company must comply in particular with Articles 16 and 17 of the Directive.

i) Specific internal organisation for the management of whistleblowing schemes

A specific organisational must be set up within the company or the group dedicated to handling whistleblowers’ reports and leading the investigation.

This organisation must be composed of specially trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations.

This whistleblowing system should be strictly separated from other departments of the company, such as the human resources department.

It shall ensure that, insofar as is necessary, the information collected and processed shall be exclusively transmitted to those persons who are specifically responsible, within the company or the group to which the company belongs, for the investigation or for taking the required measures to follow up the facts reported. Persons receiving this information shall ensure that the information received is handled confidentially and subject to security measures.
ii) Possibility of using external service providers

Where companies or groups of companies turn to external service providers to outsource part of the management of the whistleblowing scheme, they still remain responsible for the resulting processing operations, as those providers merely act as processors within the meaning of Directive 95/46/EC.

External providers may be companies running call centres or specialised companies or law firms specialising in collecting reports and sometimes even conducting part of the necessary investigations.

These external providers will also have to comply with the principles of Directive 95/46/EC. They shall ensure, by means of a contract with the company on behalf of which the scheme is run, that they collect and process the information in accordance with the principles of Directive 95/46/EC; and that they process the information only for the specific purposes for which it was collected. In particular, they shall abide by strict confidentiality obligations and communicate the information processed only to specified persons in the company or the organisation responsible for the investigation or for taking the required measures to follow up the facts reported. They will also comply with the retention periods by which the data controller is bound. The company which uses these mechanisms, in its capacity as data controller, shall be required to periodically verify compliance by external providers with the principles of the Directive.

iii) Principle of investigation in the EU for EU companies and exceptions

The nature and structure of multinational groups means the facts and outcome of any reports may need to be shared throughout the wider group, including outside the EU.

Taking the proportionality principle into account, the nature and seriousness of the alleged offence should in principle determine at what level, and thus in what country, assessment of the report should take place. As a rule, the Working Party believes that groups should deal with reports locally, i.e. in one EU country, rather than automatically share all the information with other companies in the group.

The Working Party acknowledges some exceptions to this rule, however.

The data received through the whistleblowing system may be communicated within the group if such communication is necessary for the investigation, depending on the nature or the seriousness of the reported misconduct, or results from how the group is set up. Such communication will be considered as necessary to the requirements of the investigation, for example if the report incriminates a partner of another legal entity within the group, a high level member or a management official of the company concerned. In this case, data must only be communicated under confidential and secure conditions to the competent organisation of the recipient legal entity, which provides equivalent guarantees as regards the management of whistleblowing reports as the organisation in charge of handling such reports in the EU company.
7. **Transfers to third countries**

Articles 25 and 26 of Directive 95/46/EC apply where personal data are transferred to a third country. Application of the provisions of Articles 25 and 26 will be relevant, namely, when the company has outsourced part of the management of the whistleblowing scheme to a third party provider established outside of the EU or when the data collected in reports are circulated inside the group, thus reaching some companies outside of the EU.

These transfers are particularly likely to occur for EU affiliates of third country companies.

Where the third country to which the data will be sent does not ensure an adequate level of protection, as required pursuant to Article 25 of Directive 95/46/EC, data may be transferred on the following grounds:

1. where the recipient of personal data is an entity established in the US that has subscribed to the Safe Harbor Scheme;
2. where the recipient has entered into a transfer contract with the EU company transferring the data by which the latter adduces adequate safeguards, for example based on the standard contract clauses issued by the European Commission in its Decisions of 15 June 2001 or 27 December 2004;
3. where the recipient has a set of binding corporate rules in place which have been duly approved by the competent data protection authorities.

8. **Compliance with notification requirements**

In application of Articles 18 to 20 of the Data Protection Directive, companies which set up whistleblowing schemes have to comply with the requirements of notification to, or prior checking by, the national data protection authorities.

In Member States providing for such a procedure, the processing operations might be subject to prior checking by the national data protection authority in as much as those operations are likely to present a specific risk to the rights and freedoms of the data subjects. This could be the case where national law allows the processing of data relating to suspected criminal offences by private legal entities under specific conditions, including prior checking by the competent national supervisory authority. This could also be the case where the national authority considers that the processing operations may exclude reported individuals from a right, benefit or contract. The evaluation of whether such processing operations fall under prior checking requirements depends on the national legislation and the practice of the national data protection authority.
V – CONCLUSIONS

The Working Party acknowledges that whistleblowing schemes may be a useful mechanism to help a company or an organisation to monitor its compliance with rules and provisions relating to its corporate governance, in particular accounting, internal accounting controls, auditing matters, and provisions relating to the fight against bribery, banking and financial crime and criminal law. They may help a company to duly implement corporate governance principles and to detect facts that would impact on the position of the company.

The Working Party emphasises that the establishment of whistleblowing schemes in the areas of accounting, internal accounting controls, auditing matters, and fight against bribery, banking and financial crime, to which the present opinion relates, must be made in compliance with the principles of protection of personal data, as enshrined in Directive 95/46/EC. It considers that compliance with these principles helps companies and whistleblowing schemes to ensure the proper functioning of such schemes. Indeed, it is essential that in the implementation of a whistleblowing scheme the fundamental right to the protection of personal data, in respect of both the whistleblower and the accused person, be ensured throughout the whole process of whistleblowing.

The WP stresses the principles of data protection, as laid down in Directive 95/46/EC, must be applied in full to whistleblowing schemes, in particular with regard to the rights of the accused person to information, access, rectification and erasure of data. However, given the different interests at stake, the WP recognises that application of these rights may be the object of restriction in very specific cases, in order to strike a balance between the right to privacy and the interests pursued by the scheme. However, any such restrictions should be applied in a restrictive manner to the extent that they are necessary to meet the objectives of the scheme.

Done at Brussels, 1 February 2006

For the Working Party

The Chairman
Peter Schaar
Working Document 1/2009 on pre-trial discovery for cross border civil litigation

Adopted on 11 February 2009

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/06.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
Executive Summary

This working document provides guidance to data controllers subject to EU Law in dealing with requests to transfer personal data to another jurisdiction for use in civil litigation. The Working Party has issued this document to address its concern that there are different applications of Directive 95/46 in part as a result of the variety of approaches to civil litigation across the Member States.

In the first section of this document the Working Party briefly sets out the differences in attitudes to litigation and in particular the pre-trial discovery process between common law jurisdictions such as the United States and the United Kingdom and civil code jurisdictions.

The document goes on to set out guidelines for EU data controllers when trying to reconcile the demands of the litigation process in a foreign jurisdiction with the data protection obligations of Directive 95/46.

Introduction

The issue of transborder discovery, particularly in relation to data held in Europe but required in relation to legal proceedings, for example, in the United States is one which has come to the fore recently. Often companies with a US settlement or subsidiary are under significant pressure to produce documents and materials (including items stored electronically) in relation to litigation and law enforcement investigations brought in the US. The material that is required will frequently contain personal data relating to employees or third parties, including clients or customers.

There is a tension between the disclosure obligations under US litigation or regulatory rules and the application of the data protection requirements of the EU. There is also the issue of the contrast between the geographical and territorial basis of the EU data protection regime and the multinational nature of business where a corporate body can have subsidiaries or affiliates across the globe. This is of particular relevance to the European affiliates of multinational companies which can be caught between the conflicting demands of US legal proceedings and EU data protection and privacy laws which govern the transfer of personal information.

The Working Party recognises that the parties involved in litigation have a legitimate interest in accessing information that is necessary to make or defend a claim, but this must be balanced with the rights of the individual whose personal data is being sought.

Although this paper sets out guidelines it is to be noted that resolving the issues of pre-trial discovery is beyond the scope of an Opinion by the Working Party and that these matters can only be resolved on a governmental basis, perhaps with the introduction of further global agreements along the lines of the Hague Convention.

1. Concept of Pre-Trial Discovery

There are various aspects of US litigation law and procedure where data held by European firms may be affected. Some of the most common include:

- Pre-emptive document preservation in anticipation of proceedings before US courts or in response to requests for litigation hold, known as “freezing”.
Pre-trial discovery requests in US civil litigation;
Document production in US criminal and regulatory investigations;
Criminal offences in the US relating to data destruction.

This paper will only deal with the first two issues and recognises that these have implications for the litigation process and the question of transfers of personal data to a third country. Pre-trial discovery can include not just discovery within the context of legal proceedings but also the preservation of data in relation to prospective legal proceedings.

The aim of the discovery process is to ensure that the parties to litigation have access to such information as is necessary and relevant to their case given the rules and procedures of the jurisdiction in which the litigation is taking place. Within common law countries for example, the disclosure requirements are not limited to personal data or only electronic documents. Information sought may include special sensitive personal data e.g. health data as well as personal emails (the provision of which may conflict with duties under telecoms or secrecy regulations) and the data of third parties, for example, employees or customers.

Although the civil litigation rules in the UK refer to the term “document”, this does include electronic documents including email and other electronic communications, word processed documents and databases, in addition to documents that are readily accessible from computer systems and other electronic devices. It also includes documents stored on servers and back-up systems and electronic documents that have been “deleted”. It extends to metadata i.e. any additional information stored and associated with electronic documents.

The increasing use of electronic records when previously reliance would have been only on hard copy documents has meant that more information than ever before is available. The ease with which electronic records can be downloaded, transferred or otherwise manipulated has meant that the discovery process in litigation often gives rise to a vast amount of information which the parties need to manage to determine which parts are relevant to the particular case in hand. In contrast with stored paper records, the volume of electronically stored information is vastly greater and the storage capacity of the various memory products now means that more information is obtainable and discloseable with greater ease.¹

Differences between Common Law and Civil Code jurisdictions

The first issue that arises is the difference in civil code and common law jurisdictions, not just in relation to litigation generally, but, in particular, in relation to pre-trial discovery. The scope of discovery differs greatly between common law and civil code jurisdictions and is seen as a fundamental part of the litigation process in the former. The ability to obtain and, indeed, the obligation to provide information in the course of litigation is part of the process in common law jurisdictions. This is based on the belief that the most efficient method for identifying the issues in dispute is the extensive exchange of information prior to the matter being heard by the court. This is particularly the case in the United States where the scope of pre-trial discovery is the widest of any common law country.

¹ According to figures from the Advisory Committee on Civil Rules in the US, 92% of all information generated today is in digital form and approximately 70% of those records are never reduced to hard copy. As a result almost all litigation discovery now is e-discovery and the US has taken steps to introduce rules to deal with this area.
In the US, once litigation has been commenced, companies must comply with the obligations imposed by US litigation procedure, not just under Federal but also under the State rules of civil procedure which encourage parties to exchange materials prior to trial. This includes not just the discovery of relevant information but also of information that itself may not be of direct relevance but could lead to the discovery of relevant information (the so-called “smoking gun”). This is in contrast to the situation that exists in many European civil code jurisdictions where “fishing expeditions” are forbidden.

Rule 26f of the US Federal Rules of Civil Procedure requires that the parties “meet and confer” to allow both parties the opportunity early in the process to discuss and reach agreement on the issues surrounding discovery. One aim of this meeting is to plan for the preservation of the evidence including data and documents necessary for the litigation.

However, US courts too can restrict via stipulative protective order voluntarily or if one party requests it, the scope of excessively broad pre-trial discovery requests as they have the power under the Rules to limit the frequency or extent of use of discovery methods for various reasons including obtaining the information from a more convenient source, or where the burden or expense of the proposed discovery outweighs its likely benefit. The courts may also make via this Protective Order to protect a person or party from annoyance, embarrassment, oppression or undue burden or expense by, for example, ordering that disclosure or discovery may be had only on specified terms and conditions, including the method or the matters to be considered.

It is likely therefore that a judge in a US court will grant a request for discovery as long as that request is reasonably aimed at the discovery of admissible evidence and does not contain impracticable demands.

A similar but more limited approach is taken in the United Kingdom where, under Rule 31 of the Civil Procedure Rules, a party must disclose documents upon 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 relevant court practice direction. Unlike the US, the UK (like another common law jurisdiction, Canada) have data protection obligations.

By way of contrast with the transparency required discovery process in the US and other common law countries, most civil code jurisdictions have a more restrictive approach and often have no formal discovery process. Many such jurisdictions limit disclosure of evidence to what is needed for the scope of the trial and prohibit disclosure beyond this. It is for the party to the litigation to offer evidence in support of its case. Should the other side require that

---

2 For example, Rule 34(b) of the Federal Rules of Civil Procedure provides that “Any party may serve on any other party a request to produce and permit the party making the request or someone acting on the requestor’s behalf to inspect, copy, test, or sample any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations stored in any medium from which the information can be obtained…and which are in the possession, custody or control of the party upon which the request is served.”
information, the burden is upon them to be able to know and identify it. The French and Spanish systems, for example, restrict disclosure to only those documents that are admissible at trial. Document disclosure is supervised by the judge who decides on the relevance and admissibility of the evidence proposed by the parties.

In Germany e.g., litigants are not required to disclose documents to the other party; instead a party needs only to produce those documents that will support its case. Those documents must be authentic, original and certified but the party seeking the document must appeal to the court to order the production of the document. This appeal must be specific in the description of the document and must include the facts that the document would prove and the justification for having the document produced. If the document is in the possession of a third party, the document seeker must obtain permission from the third party. If permission is refused, the seeker must commence proceedings against the holder of the documents.

Aside from any data protection issues, it is the contrast between the “opinion of the truth” compared to the “truth and nothing but the truth” that emphasises the difference between the approach of the civil code and common law jurisdictions to questions of discovery of information including personal data.

**Preventative legislation**

Some countries, mainly those in civil law jurisdictions, but also a few common law countries have introduced laws (*blocking statutes*) in an attempt to restrict cross border discovery of information intended for disclosure in foreign jurisdictions. There is little uniformity in how these have been introduced, their scope and effect. Some, for example France, prohibit the disclosure from the country, of certain type of documents or information in order to constitute evidence for foreign judicial or administrative procedures. A party who discloses information may be guilty of violating the laws of the country in which the information is held and this may result in civil or even criminal sanctions.3.

The US courts have so far not accepted such provisions as providing a defence against discovery in relation to US litigation. Under the Restatement (Third) of Foreign Relations Law of the United States no. 442, a court may order a person subject to its jurisdiction to produce evidence even if the information is not located in the United States 4. As supported by the decisions of various courts5 a balancing exercise should be carried out with the aim that the trial court should rule on a party’s request for production of information located abroad only after balancing:

---

3 One example of this is the French Penal Law No. 80-538 which provides that:

“Subject to international treaties or agreements and laws and regulations in force, 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, commercial, industrial, financial nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures.” In 2008 the French Supreme Court upheld the criminal conviction of a French lawyer for violating this statute who had complied with a request from US courts in the case of Strauss v. Credit Lyonnais, S.A., 2000 U.S. Dist. Lexis 38378 (E.D.N.Y. May 25, 2007). The lawyer was fined 10,000 Euro (about 15,000 US $).

4 It is important to note that the US judge considers that if the company is subject to US law and possesses, controls, or has custody or even has authorized access to the information from the US territory (via a computer) wherever the data is “physically” located, US law applies without the need to respect any international convention such as the Hague Convention.

(1) the importance to the litigation of the information requested;
(2) the degree of specificity of request;
(3) whether the information originated in the United States;
(4) the availability of alternative means of securing the information;
(5) the extent to which non-compliance would undermine the interests of the United States or compliance with the request would undermine the interests of a foreign sovereign nation.

The recent publication from the Sedona Conference on cross-border discovery conflicts sets out more a detailed analysis of the US jurisprudence and considers the relevant factors when determining the scope of cross border discovery obligations. It stresses that this requires a balancing of the needs, costs and burdens of the discovery with the interests of each foreign jurisdiction in protecting the privacy rights and welfare of its citizens. The Sedona Conference Framework also notes that the French decision in the case of Credit Lyonnais has altered the perception of US courts as to the reality of enforcement of foreign preventative statutes.

The Hague Evidence Convention
Requests for information may also be made through the Hague Convention on the taking of evidence abroad in civil and commercial matters. This provides a standard procedure for issuing “letters of request” or “letters rogatory” which are petitions from the court of one country to the designated central authority of another requesting assistance from that authority in obtaining relevant information located within its borders. However, not all EU Member States are parties to the Hague Convention.

A further complication is provided by Article 23 of the Convention whereby “a contracting state may at the time of signature, ratification or accession declare that it will not execute letters of request issued for the purposes of obtaining pre-trial discovery of documents. Many signatory States, including France, Germany, Spain and the Netherlands have filed such reservations under Article 23 with the effect of declaring that discovery of any information, regardless of relevance, would not be allowed if it is sought in relation to foreign legal proceedings. In France, it is allowed for the competent judge to execute letters rogatory in case of pre-trial discovery if requested documents/information are specifically listed in the letters rogatory and have a direct and precise link with the litigation in case.

According to the Hague Convention, pre-trial discovery is a procedure which covers requests for evidence submitted after the filing of a claim but before the final hearing on the merits. It is of interest to note that there is a wider interpretation under UK law as an application may be made where the evidence is to be obtained for the purposes of civil proceedings which either have been instituted before the requesting court or whose institution before that court is contemplated. This would therefore appear to allow for a greater scope for information to be provided in the UK than in other Member States.

---

6 The Sedona Conference Framework for analysis of cross border discovery conflicts – A practical guide to navigating the competing currents of international data privacy and discovery – 23 April 2008 (Public Comment Version), A Project of the Sedona Conference Working Group 6 on International Electronic Information Management, Discovery and Disclosure.
7 Sedona Framework, p. 31.
8 Evidence (Proceedings in Other Jurisdictions) Act 1975
The United States Supreme Court has ruled that the procedure foreseen by the Hague Evidence Convention is an optional but not a mandatory way of collecting evidence abroad for litigants before US courts\(^9\). Since then US courts have largely followed this line but occasionally they have required litigants to resort to the Hague Convention procedure\(^{10}\).

**Other difficulties**

One of the main difficulties with cross border litigation is the control of the use, for litigation purposes, of personal data which has already been properly transferred for example to the US for other reasons under BCR or Safe Harbour. This is not a question that will be dealt with in this paper but the Working Party recognises that this may lead more readily to the disclosure of data.

2 **Opinion**

The working party sees the need for reconciling the requirements of the US litigation rules and the EU data protection provisions. It acknowledges that the Directive does not prevent transfers for litigation purposes and that there are often conflicting demands on companies carrying on international business in the different jurisdictions with the company feeling obliged to transfer the information required in the foreign litigation process. However where data controllers seek to transfer personal data for litigation purposes there must be compliance with certain data protection requirements. In order to reconcile the data protection obligations with the requirements of the foreign litigation, the Working Party proposes the following guidelines for EU data controllers.

**Guidelines**

It should be recognised that there are different stages during the litigation process. The use of personal data at each of these stages will amount to processing, each of which will require an appropriate condition in order to legitimise the processing. These different stages include:

- retention;
- disclosure;
- onward transfer;
- secondary use.

Various issues are raised in relation to retention as the Directive provides that personal data shall be kept for the period of time necessary for the purposes for which the data have been collected or for which they are further processed. It is unlikely that the data subjects would have been informed that their personal data could be the subject of litigation whether in their own country or in another jurisdiction. Similarly given the different time limits for bringing claims in different countries, it is not possible to provide for a particular period for retention of data.

Controllers in the European Union have no legal ground to store personal data at random for an unlimited period of time because of the possibility of litigation in the United States however remote this may be. The US rules on civil procedure only require the disclosure of *existing* information. If the controller has a clear policy on records management which provides for

---

\(^9\) Société Nationale Industrielle Aérospatiale v United States District Court, 482 U.S. 522, 544 n.28 (1987)

\(^{10}\) See the Compendium of reported post-Aérospatiale cases citing the Hague Evidence Convention compiled for the American Bar Association by McNamara/Hendrix/Charepoo (June 1987-July 2003)
short retention periods based on local legal requirements it will not be found at fault with US
law. It should be noted that even in the United States there has recently been a tendency to
adopt restrictive retention policies to reduce the likelihood of discovery requests.

If on the other hand the personal data is relevant and to be used in a specific or imminent
litigation process, it should be retained until the conclusion of the proceedings and any period
allowed for an appeal in the particular case. Spoliation of evidence may lead to severe
procedural and other sanctions.

There may be a requirement for “litigation hold” or pre-emptive retention of information,
including personal data. In effect this is the suspension of the company’s retention and
destruction policies for documents which may be relevant to the legal claim that has been filed
at court or where it is “reasonably anticipated”.

There may however be a further difficulty where the information is required for additional
pending litigation or where future litigation is reasonably foreseeable. The mere or
unsubstantiated possibility that an action may be brought before the US courts is not sufficient.

Although in the US the storage of personal data for litigation hold is not considered to be
processing, under Directive 95/46 any retention, preservation, or archiving of data for such
purposes would amount to processing. Any such retention of data for purposes of future
litigation may only justified under Article 7(c) or 7(f) of Directive 95/46.

Legitimacy of processing for litigation purposes
In order for the pre-trial discovery procedure to take place lawfully, the processing of personal
data needs to be legitimate and to satisfy one of the grounds set out in Article 7 of the Data
Protection Directive. In addition, for transfers to another jurisdiction the requirements of
Article 26 would have to be met in order to provide a basis for such transfer.

There appear to be three relevant grounds, namely consent of the data subject, that the
compliance with the pre-trial discovery requirements is necessary for compliance with a legal
obligation under Article 7(c) or further purposes of a legitimate interest pursued by the
controller or by the third party to whom the data are disclosed under Article 7(f). For the
reasons set out below the Working Party considers that in most cases consent is unlikely to
provide a proper ground for such processing.

Consent
Whilst consent is a ground for processing under Article 7, the Working Party considers that it
is unlikely that in most cases consent would provide a good basis for processing. Article 2(h)
defines data subject’s consent as “any freely given specific and informed indication of his [the
data subject’s] wishes by which the data subject signifies his agreement to personal data
relating to him being processed”. The main argument underlying the US jurisprudence since
the Aérospatiale case is that if a company has chosen to do business in the United States or
involving US counterparts it has to follow the US Rules on Civil Procedure. However, very
often the data subjects such as customers and employees of this company do not have this
choice or have not been involved in the decision to do business in or relating to the United
States.
Consequently exporting controllers in the European Union should be able to produce clear evidence of the data subject’s consent in any particular case and may be required to demonstrate that the data subject was informed as required. If the personal data sought is that of a third party, for example, a customer, it is at present unlikely that the controller would be able to demonstrate that the subject was properly informed and received notification of the processing.

Similarly, valid consent means that the data subject must have a real opportunity to withhold his consent without suffering any penalty, or to withdraw it subsequently if he changes his mind. This can particularly be relevant if it is employee consent that is being sought. As the Article 29 Working Party states in its paper on the interpretation of Article 26(1): “relying on consent may…prove to be a ‘false good solution’, simple at first glance but in reality complex and cumbersome”\(^\text{11}\).

The Working Party does recognise that there may be situations where the individual is aware of, or even involved in the litigation process and his consent may properly be relied upon as a ground for processing.

**Necessary for compliance with a legal obligation**
An obligation imposed by a foreign legal statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. However, in individual Member States there may exist a legal obligation to comply with an Order of a Court in another jurisdiction seeking such discovery.

In those Member States where there is no such obligation (e.g. because a reservation under Art. 23 of the Hague Evidence Convention has been made), there may still be a basis for processing under Article 7(f) for the data controller who is required to make a pre-trial disclosure.

**Necessary for the purposes of a legitimate interest**
Compliance with 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). This basis would only be acceptable where such legitimate interests are not “overridden by the interests for fundamental rights and freedoms of the data subject”.

Clearly the interests of justice would be served by not unnecessarily limiting the ability of an organisation to act to promote or defend a legal right. The aim of the discovery process is the preservation and production of information that is potentially relevant to the litigation. The aim is to provide each party with access to such relevant information as is necessary to support its claim or defence, with the goal of providing for fairness in the proceedings and reaching a just outcome.

Against these aims have to be weighed the rights and freedoms of the data subject who has no direct involvement in the litigation process and whose involvement is by virtue of the fact that his personal data is held by one of the litigating parties and is deemed relevant to the issues in hand, e.g. employees and customers.

---

This balance of interest test should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject. Adequate safeguards would also have to be put in place and in particular, there must be recognition for the rights of the data subject to object under Article 14 of the Directive where the processing is based on Article 7(f) and, in the absence of national legislation providing otherwise, there are compelling legitimate grounds relating to the data subject’s particular situation.

As a first step controllers should restrict disclosure if possible to anonymised or at least pseudonymised data. After filtering (“culling”) the irrelevant data – possibly by a trusted third party in the European Union – a much more limited set of personal data may be disclosed as a second step.

**Sensitive Personal Data and other special categories**
Where the information in question is sensitive personal data, a ground for processing under Article 8 of the Directive must be found. Instead, the appropriate ground would be to rely on the explicit consent of the data subject under Article 8(a) or where the processing is necessary for the establishment, exercise or defence of legal claims under Article 8(e). There may be specific requirements in the different Member States relating to the processing and transfer of personal data overseas with which there would need to be compliance by the data controller.

Data protection is not the only issue surrounding the use of an individual’s personal data. Where, for example, the personal data sought is health data, there may be other duties of confidentiality between doctor and patient. There may also be other requirements of secrecy or subsisting duties of confidentiality in relation to the information, for example legal professional privilege between lawyer and client or the secrecy of confession to a priest. In addition there may be legal protection for certain types of information, e.g. the e-Privacy Directive. In those circumstances it may not be fair or lawful to process that personal data in a way that is incompatible with the other obligations. Furthermore violations of telecommunications secrecy may carry criminal sanctions in a number of Member States.

**Proportionality**
Article 6 of the Directive provides that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not used for incompatible purposes. The personal data must be adequate relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

In relation to litigation there is a tension in the discovery process in seeking a balance between the perceived need of the parties to obtain all information prior to then determining its relevance to the issues within the litigation and the rights of the individuals where their personal data is included within the information sought as part of the litigation process.

It is clear from the US civil procedure rules and the principles expounded by the Sedona Conference that the approach of both the US and the EU legal systems place importance on the proportionality and the balance of the rights of the different interests.

There is a duty upon the data controllers involved in litigation to take such steps as are appropriate (in view of the sensitivity of the data in question and of alternative sources of the information) to limit the discovery of personal data to that which is objectively relevant to the issues being litigated. There are various stages to this filtering activity including determining the information that is relevant to the case, then moving on to assessing the extent to which this
includes personal data. Once personal data has been identified, the data controller would need to consider whether it is necessary for all of the personal data to be processed, or for example, could it be produced in a more anonymised or redacted form. Where the identity of the individual data subject’s is not relevant to the cause of action in the litigation, there is no need to provide such information in the first instance. However, at a later stage it may be required by the court which may give rise to another “filtering” process. In most cases it will be sufficient to provide the personal data in a pseudonymised form with individual identifiers other than the data subject’s name.

When personal data are needed the “filtering” activity should be carried out 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 jurisdiction outside the EU.

The Working Party recognises that this 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.

Throughout the discovery process including freezing, the Working Party would urge the parties to the litigation to involve the data protection officers from the earliest stage. It would also encourage the EU data controllers to approach the US courts in part to be able to explain the data protection obligations upon them and ask US courts for relevant protective orders to comply with EU and national data protection rules. As the Supreme Court stressed in the Aérospatiale case “American courts, in supervising pre-trial proceedings, should exercise special vigilance to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a disadvantageous position.”

**Transparency**

Articles 10 and 11 of the Directive address the issue of information that should be provided to the data subject.

In the context of pre-trial discovery this would require advance, general notice of the possibility of personal data being processed for litigation. Where the personal data is actually processed for litigation purposes, notice should be given of the identity of any recipients, the purposes of the processing, the categories of data concerned and the existence of their rights.

Article 11 requires that individuals are informed when personal data are collected from a third party and not from them directly. This is likely to be a common scenario where the personal data is held by one of the parties to the litigation or by a subsidiary or affiliate of such a party.

---

12 482 U.S. 522, 546 (No.15, 16a).
In such cases the data subjects should be informed by the data controller as soon as reasonably practicable after the data is processed. Under Article 14 the data subject also has a right to object to the processing of their data if the legitimacy of the processing is based on Article 7(f) where the objection is on compelling legitimate grounds relating to the person’s particular situation.

As was discussed in the Opinion of the Working Party on internal whistleblowing schemes there is however an exception to this rule where there is a substantial risk that such notification would jeopardise the ability of the litigating party to investigate the case properly or gather the necessary evidence. In such a case the notification to the individual may be delayed as long as such a risk exists in order to preserve evidence by preventing its destruction or alteration by that person. This exception however must be applied restrictively on a case by case basis.

Rights of access, rectification and erasure

Article 12 of the Directive gives the data subject the right to have access to the data held about him in order to check its accuracy and rectify it if it is inaccurate, incomplete or outdated. It is for the data controller in the EU to ensure that there is compliance with the individual’s rights to access and rectify incorrect, incomplete or outdated personal data prior to the transfer.

The Working Party would suggest that such obligations are imposed on a party receiving the information. This could be achieved by way of a Protective Order. This has the merit of allowing a data subject to check the personal data and to satisfy himself that the data transferred is not excessive.

These rights may only be restricted under Article 13 on a case by case basis for example where it is necessary to protect the rights and freedoms of others. The Working Party is clear that the rights of the data subject continue to exist during the litigation process and there is no general waiver of the rights to access or amend.

It should be noted however 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 any changes (whilst only for correction purposes) would have the effect of altering the evidence in the litigation.

Data security

In accordance with Article 17 of the Directive, the data controller shall 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. These measures must be proportionate to the purposes of investigating the issues raised in accordance with the security regulations established in the different Member States. These requirements are to be imposed not just on the data controller but such measures as are appropriate should also be provided by the law firms who are dealing with the litigation together with any litigation support services and all other experts who are involved with the collection or review of the information. This would also include a requirement for sufficient security measures to be placed upon the court service in the relevant jurisdiction as much of the personal data relevant to the case would be held by the courts for the purposes of determining the outcome of the case.

13 Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime (WP 117 00195/06/EN)
**External service providers**

Where external service providers are used for example as expert witnesses within the litigation process, the data controller would still remain responsible for the resulting processing operations as those providers would be acting as processors within the meaning of the Directive.

The external service providers will also have to comply with the principles of the Directive. They shall ensure that the information is collected and processed in accordance with the principles of the Directive and that the information is only processed for the specific purposes for which it was collected. In particular they must abide by strict confidentiality obligations and communicate the information processed only to specific persons. They must also comply with the retention periods by which the data controller is bound. The data controller must also periodically verify compliance by external providers with the provisions of the Directive.

**Transfers to third countries**

Articles 25 and 26 of the Directive apply where personal data are transferred to a third country.

Where the third country to which the data will be sent does not ensure an adequate level of protection as required under Article 25 the data may be transferred on the following grounds:

1. where the recipient of personal data is an entity established in the US that has subscribed to the Safe Harbor Scheme;
2. where the recipient has entered into a transfer contract with the EU company transferring the data by which the latter adduces adequate safeguards, for example, based on the standard contract clauses issued by the European Commission in its Decisions of 15 June 2001 or 27 December 2004;
3. where the recipient has a set of binding corporate rules in place which have been approved by the relevant data protection authorities.

Where 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. Where a significant amount of data is to be transferred the use of Binding Corporate Rules or Safe Harbor should be considered. However, the Working Party reiterates its earlier opinion that Art. 26 (1)(d) cannot be used to justify the transfer of all employee files to a group’s parent company on the grounds of the possibility that legal proceedings may be brought one day in US courts.

The Working Party recognises that compliance with a request made under the Hague Convention would provide a formal basis for a transfer of personal data. It does recognise that not all Member States however have signed the Hague Convention and even if a State has signed it may be with reservations.

---

14 WP 114, p. 15.
Whilst there may be some concerns about the length of time such a procedure could take, the courts, for example in the US, are experienced in the use of the Hague Convention and such timescales can be built into the litigation process. 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.

**Conclusion**

This working document is an initial consideration of the issue of the transfer of personal data for use in cross border civil litigation. It is an invitation to public consultation with interested parties, courts in other jurisdictions and others to enter a dialogue with the Working Party.

Done at Brussels, on 11/02/2009

_For the Working Party_

_The Chairman_

_Alex TÜRK_