ARTICLE 29 DATA PROTECTION WORKING PARTY

00339/09/EN
WP 158

Working Document 1/2009 on pre-trial discovery for cross border civil litigation

Adopted on 11 February 2009

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.

Common Law – United States

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.[2] 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.

United Kingdom
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.

Civil Code countries
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 courts[5] 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.

[5] Société Nationale Industrielle Aérospatiale v United States District Court, 482 U.S. 522, 544 n.28 (1987), Volkswagen AG v Valdez [No.95-0514, November 16, 1995, Texas Supreme Court] and In re: Baycol Litigation MDL no. 1431 (Mfd/JGL), March 21, 2003. For a more thorough analysis of the US jurisprudence see the Sedona Conference Framework for Analysis of Cross-Border Discovery Conflicts (note 5 infra).

(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.[6] 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[7].

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.[8] 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"[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.

[11] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), p. 11.

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 or 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."[12]

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[13] 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[14].

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