Balancing Discovery with EU Data Protection in International Arbitration Proceedings

By Karin Retzer and Sherman Kahn

As many organizations facing cross-border litigation know too well, U.S. discovery demands for evidence in the European Union ("EU") can create major conflicts with EU data protection requirements. In arbitration, where the proceedings do not have the imprimatur of a Court, this issue can be more difficult in some respects. However, the relative flexibility of the arbitration practice and the tradition of streamlined discovery makes the issue less difficult in other respects.

As might be expected, European data protection issues often arise in the international arbitration context. However, such issues may arise even in arbitrations under purely domestic United States rules if one of the parties is a European company or an affiliate of a European company. Indeed, as much international arbitration provides only for restricted discovery, it is in the United States domestic arbitration context that the most problematic privacy issues may arise.

This article first explains some of the conflicting obligations presented by EU and U.S. laws and summarizes the different approaches toward data protection in the United States and Europe. It then describes recent guidance from the EU data protection authorities to assist organizations with their compliance with U.S. requests for testimony and documentary evidence in a manner consistent with EU obligations. At the end, we provide some practical suggestions as to how to navigate these issues in the arbitration context.

I. Conflicting Obligations and Conflicting Expectations

Discovery problems tend to arise in cross-border litigation where the United States expectation of broad-ranging discovery is applied to persons or entities in European countries with significantly narrower approaches to discoverability of information in litigation. These problems are compounded when documents sought in discovery include information considered by European countries to be "personal information" relating to an individual – raising privacy concerns. The European view of what constitutes personal data is substantially different from that in the United States. Thus privacy law issues can create significant problems with cross-border discovery.

A. Different Approaches to Gathering Evidence

As has been widely discussed in international arbitration circles (and will not be repeated at length in this article), the civil law jurisdictions in the EU and the U.S. have fundamentally different methods of gathering evidence in civil litigation. Briefly put, civil law jurisdictions (such as those in continental Europe) generally limit disclosure of evidence to what is proffered by each party as evidence in support of the party's case. In contrast, pre-trial discovery obligations in common law countries, particularly in the United States, but also in the UK, are much broader.[1] In international arbitration involving parties from both sides of the Atlantic, the parties and the arbitrators may often wish to reach a middle ground between these approaches, providing some circumscribed discovery but not the type of wide-ranging discovery allowed by United States courts. Unfortunately, without care, even the provision of limited discovery can lead to privacy concerns and potential breaches of European law.

"The U.S. and the EU have different notions of what is considered 'personal data.'"

It is also important to keep in mind that European privacy laws are not just a tool used by parties unwilling to provide discovery. Rather, even if a European business entity involved in an arbitration is willing (or even eager) to provide discovery in an arbitration, it must still comply with applicable privacy and data protection laws. It is therefore important that an arbitration tribunal carefully manage the discovery process and carefully address privacy and data protection issues.

B. Different Approaches Toward Data Protection

The U.S. and the EU[2] have different notions of what is considered "personal data." To effectively manage discovery in an arbitration having participants from the United States and the European Union, it is critical to understand these differences.

The EU countries generally embrace a broader view of what constitutes "personal data" than that held in the United States. Indeed, some items, such as work related email, considered personal information in Europe would be considered quite the opposite in the United States. Protection of personal data under European law is generally governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("The 1995 Data Protection Directive").[3] Article 2 of the 1995 Data Protection Directive defines "personal data" as "any information relating to an identified or identifi-

able natural person ("data individual"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[4] This is a very broad conception of personal data, and as understood in Europe, under the 1995 Data Protection Directive personal information includes any information relating to an identified or identifiable individual, such as emails or documents created at the workplace (including lab notebooks, quality assurance documents, work-related memos or reports) that include the individual's name and contact information.

Under the 1995 Data Protection Directive, personal data may be collected only for a specific, explicit purpose, and may not be further processed in a manner incompatible with the original purpose unless the use meets a specified exception. The concept of "processing" is broadly defined as "*any operation or set of operations," whether manual or automated, including, but not limited to, "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*."[5] Clearly, the 1995 Data Protection Directive's broad definition of personal data in conjunction with its tight restriction on processing of such data can create issues regarding document discovery in arbitration—as typical discovery activities such as document review and production would constitute "processing."

The 1995 Data Protection Directive also requires that individuals must receive detailed notice regarding processing of their personal data.[6] Also, the 1995 Data Protection Directive requires that records containing personal data must be adequate, relevant, and not excessive to the purposes for which the data are processed as well as accurate and kept up-to-date.[7]

In the United States, by contrast, the concepts of "personal data" and "processing" are quite different. The idea that a business email is personal data of the sender or recipient, simply because it has the individual's name on it, would seem counter-intuitive to most U.S. lawyers and business people. Protection of "personal data" in the U.S. is generally restricted to specific types of sensitive information, such as personal medical information, social security information, information relating to children and financial information. The United States does not generally recognize any specific limits on processing of data for business purposes.

C. Guidance from EU Authorities

The Article 29 Working Party ("Working Party"), a consortium of data protection authorities from the various EU Member States established by Article 29 of the 1995 Data Protection Directive, has published a Working Document[8] ("Working Document") which provides useful guidance on the challenges that arise from discovery obligations for cross-border civil litigation. The Working Document does not address arbitration. Nonetheless, its non-binding guidance is very helpful in understanding how to approach the discovery issue in the arbitration context.

1. Processing Data

As outlined above, under the 1995 Data Protection Directive, data may only be processed where authorized by law. The Working Document analyzes three possible legal bases authorizing the processing of personal data that pertain to extraterritorial discovery:

- **Consent**: At first blush, it might appear that employers may legitimize their data processing regimes *ex ante* by obtaining the consent of employees who might potentially be relevant to discovery. However, the Working Document suggests that consent alone will not be sufficient to support processing of documents for litigation. Specifically, requirements that consent be both "specific" and "informed" seemingly would not support a general opt-out-type consent to data processing. Under the 2005 Data Protection Directive, consent is deemed to be valid only in cases where there is a "real opportunity" to withhold or withdraw consent without suffering any penalty.

  In earlier guidance, the Working Party has taken the position that a current employee cannot freely provide consent on account of the prejudice to the employee that might arise should consent be refused.[9] The Working Paper suggests that, with respect to certain employees, consent may be relied upon for discovery purposes. "The Working Party does recognize that there may be situations where the individual is aware of, or even involved in the litigation process and his consent may be properly relied upon as a ground for processing."[10]

  In commercial arbitration, because the issues typically revolve around a particular contract, many of the individuals who would potentially be providing relevant documents, *i.e.* current employees who participated in the negotiation of the contract or who are participating in its performance, may be in a position to give consent. However, even such individuals may subsequently withdraw their consent at any time. This possibility substantially lowers the utility of consent as a legal basis for complying with U.S. discovery requirements. It would be difficult, to say the least, to undo discovery in a situation where an individual has decided to withdraw consent. Moreover, complying with such a request as to relevant documents could leave a United States arbitration tribunal subject to

vacatur on the ground that it refused to hear evidence pertinent and material to the controversy.[11] In addition, if an employee refuses to consent, the company would not be excused from obligations to preserve and produce relevant information.

- **Legal Necessity**: Alternatively, an organization may establish the legitimacy of data processing where "necessary for compliance with a legal obligation." This legal basis is interpreted quite narrowly to include only those situations where there is an EU statutory requirement. This basis would not appear to apply directly to arbitration, which is a creature of contract, not legal obligation.

- **Necessary for purposes of a legitimate interest**: Arbitration discovery may well fall within this ground, which authorizes use of information where necessary for purposes of a legitimate interest pursued by the organization or by a third party to whom the data to be disclosed and not outweighed by the privacy rights of the individual.[12] Production of information in the context of a private confidential arbitration under the control of an arbitration tribunal in keeping with the arbitration goals of efficiency and justice would appear to be a legitimate interest. In order to rely on this ground, the Working Document stresses that issues of proportionality of the data, the relevance of the data, and possible consequences for the individuals concerned should be taken into account and adequate safeguards must be adopted to protect the individual's rights. This suggests that the arbitration tribunal should actively manage the arbitration process to ensure that any discovery allowed is reasonably circumscribed.

  The Working Document also suggests that, where possible, the organization should also anonymize or at least pseudonymize data, and apply filtering techniques to exclude or cull irrelevant data if possible by a "trusted" third party within the EU. Arbitration tribunals may wish to work with the parties to use these techniques where appropriate to further protect any privacy interests that may be implicated by needed discovery in the arbitration.

2. Transferring Data

In addition to determining whether data can be processed for use in an arbitration, EU privacy law places restrictions on the conditions under which the data can be transferred outside of the European Economic Area ("EEA").[13] Transferring records outside of the EEA requires compliance with the same general data protection principles that govern data retention. In addition, there must also be a legal basis to support transferring the data outside of the EEA. As a basic principle, the transferee country must meet the 1995 Data Protection Directive's "adequacy" requirements for data transfers or adequate safeguards, a global assessment of suitability to protect personal data based on the various provisions of the Directive. Under this standard, the United States has been deemed to have an inadequate data protection scheme.

To transmit data to a jurisdiction, such as the United States, which has not been deemed adequate, the party receiving the data must meet certain requirements. These are outlined below:

- **Safe Harbor Provisions**: The "Safe Harbor" established by the European Commission and the U.S. government allows U.S.-based organizations to self-certify that they will abide by Safe Harbor's principles of notice, choice, onward transfer, security, data integrity, access and enforcement and thus legitimizes transfers between an organization established in the EEA or Switzerland and the U.S. organization. However, Safe Harbor is not designed for the transfer of data in connection with a particularized proceeding such as an arbitration or litigation. Thus, while under certain circumstances, Safe Harbor may be useful for allowing document review, it will be quite difficult to use in an effort to legitimize the disclosure of documents to the other parties, witnesses or the arbitrators.

- **Model Contracts**: Article 26(2) of the 1995 Data Protection Directive provides that EU Member States may authorize transfers of data to organizations located in countries not deemed to be adequate if the data are safeguarded using appropriate contractual requirements. The European Commission has promulgated model contracts which it has deemed sufficient for this purpose.[14] Adopting model contractual language provides organizations located in a country that does not meet the EU's adequacy requirements with the necessary safeguards to engage in data transfers with EU parties.

  The model contracts may be a useful tool for transferring information in connection with arbitration discovery. The parties could include the EU Standard Contractual Clauses in an Arbitration Provision and/or agree, in the underlying agreement, that in the case of dispute they will enter into a model contract based on the EU Standard Contractual Clauses. Alternatively, the arbitration tribunal could incorporate the model contract requirements as a binding obligation in a procedural order governing discovery. The parties and the arbitrators would be required to sign such a model contract. Witnesses provided access to exchanged documents may also have to sign. We note, however, that the language of the model contracts cannot be varied and must be used exactly as published in order to be valid. Some terms of the model contract may be

unacceptable (for example, the EU entity would have to do due diligence on any of the receiving parties to ensure that they could adequately protect the personal information and the U.S. entities would have to agree to subject themselves to EU jurisdiction in the event of a breach of the agreement). In addition, some countries require model contractual language to be approved by data protection authorities—which can take significant time and reduce arbitration confidentiality.

The 1995 Data Protection Directive provides for certain exceptions from these standards for transferring data when the individual about whom the data relates unambiguously consents to the transfer, or when the transfer is necessary for the exercise or defense of a legal claim.

- **Consent of the Individual**: Whether consent is a valid basis for transfers of personal data outside the EEA follows the same standard as consent as a basis for processing personal data. Because of the limitations discussed above, consent is often an unreliable basis for cross-border data transfers, but in many cases it may be the only viable alternative.
- **Necessity for Legal Claim**: Article 26(1)(d) of the 1995 Data Protection Directive creates an exception for international transfers that are "necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims." Departing from earlier Member State interpretation,[15] the Working Document appears to apply the legal claims exception to "single" international transfers of data in compliance with foreign discovery obligations unless a "significant" amount of data are involved. There is no further guidance on what a "single" transfer or a "significant" amount of data would mean. However, according to the Working Party, the exception is subject to "strict interpretation."[16] It is not clear whether the Working Party would consider an arbitration to fall within the exception—although the way the exception is worded suggests it should—so it may be risky to rely on it. Moreover, the Working Document is non-binding and each Member State's interpretation of the Working Document may vary.

3. Data Security

The Working Document states that "[i]n accordance with Article 17 of the Directive, the [organization controlling the data] should take all reasonable technical and organizational precautions to preserve the security of the data to protect it from accidental or unlawful destruction or accidental loss and unauthorized disclosure or access."[17] The Working Document goes on to state that these requirements are also applicable to the law firms, litigation support services and experts who are involved with the litigation. Arbitration tribunals should work with the parties to include data security requirements in procedural orders in order to ensure the security of any documents produced during the arbitration.

Appropriate security standards must ensure the data are kept confidential and secure. Where service providers are used, they should be bound by contract to ascertain compliance with purpose limitation obligations, retention policies, and security standards. The Working Document states that expert witnesses, for example, should be treated as service providers.[18]

4. Access and Rectification

Article 12 of the 1995 Data Protection Directive gives an individual the right to access data held about himself or herself in order to rectify inaccuracies. The Working Document affirms that there is no waiver of the rights of access and correction for the discovery process and suggests that the obligation be placed on the receiver of the data.[19] Again, this is an issue that the arbitration tribunal can cover in an initial procedural order as this would need to cover any party that receives the data, including parties, witnesses and the arbitrators.

II. Practical Approaches to Minimizing Privacy Issues in International Arbitration

A. The Use of Procedural Orders to Impose Meaningful Restrictions

Prior to conducting any information transfers, arbitration tribunals should work with parties to negotiate terms to restrict who may access information to be transferred in an arbitration, as well as the purposes for which it may be used, in accordance with the security, transparency and finality principles of the Directive. One way to accomplish this may be to incorporate language from the model contracts into a discovery procedural order governing the arbitration.

Arbitration tribunals should also discuss with the parties how the disclosure of personal information could be limited consistent with the parties' needs in the arbitration process. The tribunal may wish to explore whether any personal data that is sufficiently relevant that it should be disclosed may be anonymized, or redacted to preserve the individual's privacy interest without causing substantial prejudice to the receiving party.

B. Address Data Protection in Dispute Resolution Clauses

In agreements among parties where European data protection issues may arise, it would be helpful to address data protection concerns in the dispute resolution clause of the underlying agreement. If the parties address these issues in the underlying agreement, many potential privacy and data protection issues can be avoided in the event the parties later have a dispute.

C. Keep Employees Apprised

We recommend that companies inform employees about the possibility that data possessed by the company may need to be retained and shared for discovery purposes. This could be accomplished using a technology use policy. Then, where appropriate, employees should be informed about the details of discovery requests, including possible recipients, third party service providers and the right to access and modify information. Some countries require notice to or consultation with works council, employee representatives or public authorities. While this may reduce arbitration confidentiality, where the law requires it may be necessary.

III. Conclusion

European data protection and privacy laws can add considerable complexity to the discovery process when a European party is involved in an arbitration. Those problems can be even more significant if the arbitration is subject to broad United States discovery principles. Ultimately the U.S. and the EU will need to reach some type of political solution to resolve these conflicts. No solution is perfect and there is no magic bullet. Nonetheless, in the meantime, some problems can be mitigated through careful case management by the arbitration tribunal and cooperation among the parties.

Endnotes

1. In court litigation, the conflict between civil law and common law discovery approaches can cause major problems. For example, some countries in continental Europe, notably France, have responded to American Courts' attempts to enforce discovery orders against their citizens by enacting "blocking statutes" which can subject parties voluntarily providing discovery in U.S. Court proceedings outside of Hague Convention procedures to fines and even criminal liability. These statutes do not, by their terms, apply to arbitration, and they are thus beyond the scope of this article.
2. The 27 Member States of the European Union (EU) currently are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the Netherlands and the United Kingdom (collectively, the "Member States").
3. Official Journal L 281, 31. The 1995 Data Protection Directive is not itself a law directly applicable to private individuals and organizations. Rather, it is a directive to member states to adopt national laws consistent with the directive. It is these national laws that are directly applicable to private parties. There is variation among the implementing legislation in the various member states and it is important to understand the applicable legislation in preparing a discovery plan for arbitration.
4. *Id.*
5. See Article 2(b) of the 1995 Data Protection Directive.
6. See Articles 10, 11 of the 1995 Data Protection Directive.
7. See Article 6 of the 1995 Data Protection Directive.
8. Article 29 Working Party, "Working Document 1/2009 on pre-trial discovery for cross-border civil litigation," WP 158, Adopted on 11 February, 2009, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp158_en.pdf.
9. Article 29 Working Party, "Opinion 8/2001 on the processing of personal data in the employment context," WP 48, Adopted on 13 September, 2001, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf.
10. Working Document, p. 9.
11. See, Federal Arbitration Act, 9 U.S.C. § 10(a)(3).
12. Working Document, p. 11.
13. The EEA consists of the 27 EU Member States plus Iceland, Liechtenstein and Norway.
14. Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, 2001/497/EC; Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of data to third countries (2004/915/EC).
15. For example, the Düsseldorfer Kreis, the assembly of the German federal state data protection authority, has taken the (informal) position that transfers of data outside the EU cannot be based on the necessity for legal claim exception.
16. Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, adopted on 25 November 2005, page 13.
17. Article 29 Working Party, "Working Document 1/2009 on pre-trial discovery for cross-border civil litigation," WP 158, Adopted on 11 February, 2009, page 12.
18. Article 29 Working Party, "Working Document 1/2009 on pre-trial discovery for cross-border civil litigation," WP 158, Adopted on 11 February, 2009, page 13.
19. *Id.*

Karin Retzer, kretzer@mofo.com, is Of Counsel in Morrison & Foerster's Brussels office. Her practice focuses on the legal aspects of privacy and data protection, e-commerce, technology licensing, and intellectual property law. Karin has provided strategic advice on worldwide privacy and data security compliance projects.

Sherman W. Kahn, SKahn@mofo.com, is Of Counsel with Morrison and Foerster, resident in the New York office and is Co-Chair of the NYSBA Dispute Resolution Section Arbitration Committee. He represents clients in international arbitration proceedings presenting complex technical and commercial issues and has arbitrated under the AAA, JCAA , ICC and other arbitration and dispute resolution rules.

Reprinted with permission from the *New York Dispute Resolution Lawyer*, Spring 2010, published by the New York State Bar Association, One Elk Street, Albany, New York 12207. http://www.nysba.org