Data Protection and Privacy

In International Electronic Disclosure
The Challenges of International Disclosure

Because discovery obligations cross territorial boundaries, a company in the U.S. engaged in litigation that needs to comply with the U.S. rules of court must disclose documents stored at its facilities or subsidiaries in other locations around the world. Europe has a long history of preserving the individual's right to privacy and a complex network of legal rules designed to protect it. Despite these statutes, many U.S. Courts will still expect global discovery from parties to US litigation that have international operations. Lawyers face the often difficult task of ensuring that U.S. discovery obligations are met while at the same time not violating the local laws of the place in which discovery is sought. Companies engaged in legal disputes involving European entities therefore have to think carefully about how data located in Europe is collected and processed.

Data Protection and Privacy Law

Many European countries have data protection laws or specific blocking statutes that prevent the transfer of certain information out of the jurisdiction and to the U.S. European Directive 95/46/EC which has been adopted into local law in the member states of the EU sets out eight basic data protection principles. They control how personal data is obtained, kept, processed and transferred. Personal data is defined broadly as any data which relates to a living individual who can be identified by the data or other information in the possession of the data controller. This broad definition includes names, birthdays, addresses, telephone numbers, fax numbers, email addresses as well as identifiable physiological, mental, economic, cultural and social traits. Processing includes collecting, hosting, transmitting and interrogating and covers basically any operation performed on personal data. This means certain rules must be observed in all cases when data is collected from EU member states and then processed and reviewed for production in US legal proceedings for discovery purposes. The basic principles require that personal data is handled fairly and lawfully, which in essence means that individuals must consent to the handling of their personal data or there must be a legal purpose for using the information. The EEC Directive also prohibits the transfer of personal information outside of the European Economic Area unless the country receiving the information provides an “adequate level of protection” for individuals in the processing of personal information (against loss, alteration, unlawful access etc). The U.S. is presently not considered to provide adequate privacy protections.

Other Privacy Laws

In addition to data protection law, employees in European countries may have privacy rights to information on their computers and other devices. These may be granted via local law, a specific employment contract or through local Works Councils. In many jurisdictions it is illegal to monitor employee email activity without prior notice to the employee unless the employer has a strong suspicion of criminal activity.

Issues to Consider When Collecting Evidence in Europe

US law firms and their clients typically consider the following issues when the need to collect European data arises.

» What legal mechanisms can be used to transfer data lawfully across borders?

» How can technology be used to target the data needed and reduce the risk of unlawful data transfers?

» Is it necessary to report the processing of data envisaged to and seek approval from the local data protection authority or Works Councils?

» Is it necessary to notify or obtain the express consent of data custodians before collecting their data?

» Do the data custodians have to be told how the data is going to be interrogated?

» Are individuals whose data is to be collected entitled to be present when data is collected from their computers?

» Can data be transferred to the U.S. or any other location in Europe for processing?

» Can data be reviewed in the U.S. via a web-based review tool where the data is hosted in Europe?

» Do you need a local agent or nominated representative in the jurisdiction where the collection takes place?

How Electronic Evidence Experts Can Help

Where data collected in Europe needs to be transferred to the U.S., companies can rely on:

» Computer forensic experts to harvest data onsite in a very targeted way.

» Filtering either onsite or in Europe to search across potentially relevant data and identify key data, using tools such as Kroll Ontrack’s ediscovery.com Onsite, a mobile ediscovery service that gives companies the benefits of an electronic discovery service provider's expertise and technology, in-house at their own offices.

» Advanced review tools like Ontrack® Inview™ and Ontrack® Advanceview™ which allow reviewers to identify and remove personal data from a data set or redact personal references.

This reduces the risk of sending personal data out of Europe and ensures that only that which is necessary for the legal proceedings is transferred.
Practical Examples: Overcoming the Prohibition Against International Data Transfers

Different approaches are taken by parties involved in discovery exercises to overcome the prohibition against transferring personal data out of the EEA, including the following:

» **Obtaining consent** of the individuals whose personal data is to be transferred, although this can be logistically difficult and time-consuming.

» **Reliance on other legal mechanisms** to legitimise the transfer of personal data across borders, such as the Hague Convention. Article 23 of the Hague Convention sets forth a uniform procedure for the issuance of letters of request which are letters of request or petitions from a court in one nation to a designated central authority in another country requesting assistance from that authority in obtaining information that is located within the central authority’s borders. An approved letter of request permits the transfer and processing of data. Among other states in the European Union, Germany has raised a reservation under Article 23 of the Hague Convention, not to deal with requests for legal assistance to be given in the context of pre-trial discovery taking place in Common Law countries.

» **Relying on legal exemptions** in data protection laws which allow data to be transferred for the purpose of bringing or defending legal claims and complying with discovery obligations. Some parties seek a legal opinion or court ruling first on the lawfulness of the transfer. In *Re Madoff Securities International Ltd v. [2009] All ER (D) 31 (Mar,) the Court allowed the transfer of data to the U.S. where this was required to unravel a fraud. In some countries, such as Germany, an obligation imposed by a foreign legal statute or regulation [such as a US discovery rule] would not qualify as a legal obligation by virtue of which data processing relating to e-discovery requests could be made legitimate.

» **Processing data first in Europe**, in an effort to identify and remove personal references from a data set before the data is transferred to or accessed in the U.S. In some cases this process is carried out by keyword searching during data processing and in others custodians manually select documents that are private in a first pass review database. Data has in some cases been reviewed for privacy by neutral European lawyers to ensure that personal references are removed or redacted before the data is transferred to the U.S. By processing and searching across the data in Europe first a party can show that steps have been taken to limit the data transferred to that which is strictly necessary to the case. This is in line with the Article 29 Working Party requirements that efforts should be made to restrict the transfer of personal data as much as possible and that only data which is relevant to the issues being litigated should be transferred.

» **Filtering data onsite** to ensure that privacy laws are adhered to. This may be required in the case of highly sensitive data or in jurisdictions which restrict transfers even between countries in Europe and which would prohibit a transfer to a central data processing centre outside of its national border.

» **Creating a contractual safe harbour** for data transferred to third countries by implementing model contract clauses recommended by the European Commission and designed to ensure adequate safeguards for the data are in place.

» **Relying on data transfers** to an ediscovery provider in the U.S. that has safe harbour status. The U.S and EU have developed a safe harbour agreement that allows U.S. organizations to certify to the U.S. Department of Commerce that they will provide privacy protections that meet the Directive’s adequacy standards when transferring personal data outside of the EU. Safe harbour certification requires that U.S organizations meet certain standards including notice and choice provisions which must be observed when data is transferred to third parties.

**Final Comments**

Many litigants are adopting a conservative approach to data transfers between jurisdictions due to concerns about the criminal and civil sanctions attached to contraventions of data protection laws in many Europeans counties. Relying on local legal experts to navigate the complexities of data protection and privacy law in Europe is essential. It also makes sense to draw on the experience of a global discovery provider with local ediscovery experts familiar with the data handling requirements in different countries. Technology can also be relied on to ensure that, where necessary, data is processed onsite or in-country and that only that which is strictly necessary for legal proceedings is transferred across national borders or outside of Europe. This is in line with the Article 29 Working Party requirements that efforts should be made to restrict the transfer of personal data as much as possible and that only data which is relevant to the issues being litigated should be transferred. Apart from, ensuring that data protection laws are not breached this approach also ensures that discovery costs are kept to a minimum which makes economic sense.

---

1 EEC Directive on “Protection of individuals with regard to the processing of personal data and on the free movement of such data”.  Implemented by European Commission in 1995, addressed to the member states and transposed into internal law by 27 member states. See European Commission website on data protection: [http://ec.europa.eu/justice_home/fsj/privacy/](http://ec.europa.eu/justice_home/fsj/privacy/).


3 Article 29 Working Party.

4 The EEA plus Iceland, Liechtenstein and Norway.

5 If the search criteria are automatic and are to be used as the sole means of evaluating the conduct of an individual (as certain investigations may), in the UK this information must be provided.