Article

US e-discovery obligations v EU data protection laws: a conundrum for businesses

Feb 12 2008 Bridget C. Treacy

Bridget Treacy

The conflict between US e-discovery obligations and European Union data protection legislation is reaching a climax. How do US companies comply with their e-discovery obligations — which may involve exporting European personal data to the US — yet stay within the boundaries of European data protection laws? These laws regulate both the purposes for which such data may be processed and a company's ability to export the data abroad.

US e-discovery rules

US companies who are engaged in litigation have wide-ranging obligations under Rule 34 of the US Federal Rules of Civil Procedure which requires them to retain all documents which may be relevant to actual or reasonably foreseeable litigation. The duty to preserve documents applies to both paper files and to electronically stored files, wherever they are located. Where documents are stored outside the US, the obligation to preserve documents may conflict with European data protection laws. Further, the process of identifying, isolating, reviewing and selecting documents that are relevant to litigation requires considerable care under European data protection laws.

European data protection laws

Each EU member state has implemented the EU Data Protection Directive (95/46/EC) in relation to the processing of personal data. "Personal data" is defined in broad terms as any information that relates to an identified or identifiable natural person. The directive applies to entities based in Europe who process personal data within their European businesses. In relation to discovery obligations, there are two relevant principles in the directive which must be considered:

1. Purpose limitation

   European companies should only collect personal data for specific, legitimate purposes, and use, disclose and retain the data only as needed for those purposes. Using business records which contain personal data (such as e-mails) in the course of litigation is a secondary use of the data which, generally, is not permitted.

   The French data protection authority, Commission nationale de l'informatique et des libertés, has recently highlighted its concerns in regard to the number of requests to transfer personal data from EU businesses to the US as part of the preparation for US-based litigation. CNIL has called for the

Article 29 Working Party, the independent advisory body made up of data protection regulators from each of the 27 EU member states, to examine this issue and publish guidance.

2. Export limitation

   Article 25 of the directive provides that the transfer of personal data to a third country may only take place if the third country ensures an "adequate" level of protection. The European Commission has compiled a list of those countries it considers to have adequate protection. Currently there are five countries on the list. The US is not one of them.

   Article 26 of the directive provides exceptions to the restriction on international transfers including in circumstances where the transfer is necessary or legally required for the establishment, exercise or defence of legal claims. At first sight, it would appear that US e-discovery should fall within this exception; however, this derogation has been interpreted very narrowly by the European regulators. In many EU member states it cannot be used to support the export of data for the purposes of complying with discovery obligations. According to the Article 29 Working Party, the Article 26 exception is inapplicable to US document production requests except where individual EU member states have enacted local law derogations.

Practical implications

One of the most complex discovery issues is where potentially relevant documents include employee e-mails. EU data protection authorities consider virtually all data about employees to be personal data and subject to data protection laws. Further, in many EU member states, local employment laws will significantly restrict, or even prohibit, a company's actions to review an employee's e-mail folders. Companies commonly seek to deal with this issue by obtaining employees' consent to a review of their e-mail folders, but some EU member states consider that an employee's consent in this context is invalid and cannot legally be relied upon.

In addition, in some EU jurisdictions, the process of discovery is contrary to the fundamental principles of local civil procedure. In Germany, complying with e-discovery requests may breach telecommunications secrecy laws. Works councils may object to the e-discovery process on behalf of a company's employees.

Practical steps

What can companies do to ensure that they do not breach EU data protection laws when they seek to comply with their US discovery obligations? They must think ahead of possible litigation and devise a policy in advance. It is easier to devise a coherent policy without a discovery deadline looming. The policy should:

- provide a clear explanation of the issues, and focus on both the purpose limitation and data export issues;
- explain strategies for identifying and narrowing the search for relevant data sets using automated tools within local jurisdictions;
- where possible, obtain consent to any subsequent processing and to the transfer itself, but treat the consent with caution;
- undertake the main processing of the data within the EU and only transfer to the US the reduced data set;
- apply for a confidentiality order in the US; and
- document the steps taken to process the data for review and transfer.

There is a growing body of jurisprudence in the US where courts have accepted in evidence the fact that

companies have not been able to comply fully with discovery obligations because of EU data protection laws. Not all courts have taken this view. For practical purposes, the majority of organisations seek to comply with their US discovery obligations but judgments required on this issue are often finely balanced. This article does not provide a complete statement of the law. It is intended merely to highlight issues which may be of general interest and does not constitute legal advice.

• ***Bridget Treacy*** *is a partner in the Hunton & Williams Global Sourcing and Privacy practices. Tel: +44 (0)20 7220 5731*

This article first appeared on Complinet on www.complinet.com *on February 12 2008. For a free trial of Complinet's services, please contact client support on* client.support@complinet.com *or* +44 (0) 870 042 6400.