CLIENT ALERT

European Working Party Offers Guidance On Discovery For Cross-Border Civil Litigation

Mar.05.2009

Multinational companies with operations both in the U.S. and Europe are keenly aware of the conflict between European data protection laws and U.S. discovery requirements. Compliance with discovery rules are clear legal obligations for entities facing litigation in the U.S. However, the handling of European personal data to comply with these legal obligations may breach the national laws in Europe implementing the requirements of Data Protection Directive (95/46/EC) (the "Directive").

Last week, the EU Article 29 Data Protection Working Party (the "Working Party") published its latest working paper (WP 158), purporting to provide guidance to data controllers on how to reconcile the demands of the litigation process in a foreign jurisdiction with the requirements of the Directive.

Conflicting Demands Between U.S. and European Laws

Before reflecting on the Working Party's comments it is useful to look briefly at the key conflicts between U.S. discovery requirements and European data protection laws:

- **Triggering the Directive in U.S. Pre-trial Discovery:** Under the U.S. legal requirements, U.S. litigants have a duty to preserve information when litigation is reasonably anticipated. This might include data stored in Europe or otherwise subject to the protections of the Directive. Wherever personal data that identifies a living individual is "processed" (this includes storage, access, review, and disclosure) in Europe, the legal requirements of the Directive will apply in relation to the handling of that data. Therefore, the retention of data for purposes of anticipated or pending litigation is subject to these requirements.
- **Limits on Circumstances in which Personal Data can be Handled:** The Directive only permits the "processing" of personal data in certain circumstances. Compliance with a foreign legal statutes or regulations (such as the U.S. Federal Rules of Civil Procedure) is not included in the list of permissible processing grounds under the Directive. So personal data may only be preserved in connection with U.S. litigation where other grounds are satisfied.
- **Proportionate Data Filtering:** To comply with the requirements of the Directive, all processing of European personal data must be conducted in a proportionate fashion. To meet these requirements, any data filtering required as part of the U.S. discovery process should ideally be carried out in the country where the data is found, or at the very least within the EU. Relevancy decisions should also be made by someone with knowledge of the litigation. This could be the services of a "trusted third party" within the EU 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. Only those categories of data that are required for litigation should then be transferred to the U.S. for disclosure in litigation proceedings.
- **Transparency:** The Directive requires the processing of personal data to be transparent. Individuals (including company employees) must ordinarily be informed of the ways in which their personal data is being processed. In some

circumstances (where, for example, there is a risk of the intentional destruction of evidence) it is not always possible to provide advance notice of internal investigations.

- **Data Retention:** The Directive requires personal data to be kept for as long as it is collected or for which it will be further processed.European personal data may not be retained for unlimited periods simply because of the possibility of U.S. litigation.

Prohibition on Data Transfer to the U.S.: The Directive contains a basic prohibition on the "transfer" (this includes the review of personal data stored in Europe by personnel located in the U.S.) of personal data to the U.S. There is an exception to this prohibition which permits the transfer of personal data to the U.S. where it is necessary or legally required for the establishment, exercise or defense of legal claims. However, data disclosed must generally be limited to categories that are relevant to anticipated or pending U.S. proceedings. The wholesale transfer of all potentially relevant personal data to the U.S. for preservation purposes is not permissible under EU law.

The Working Party Guidance

In its paper on this topic, the Working Party acknowledges the need to reconcile U.S. litigation rules and EU data protection provisions and states that it intends to offer up guidelines for EU data controllers on the four stages of the litigation process - retention, disclosure, onward transfer, and secondary use. In reality, the guidance provided does little more than to summarize the conflicts identified above, as well as to impose additional obligations under the Directive for the handling of EU personal data.

Because of this, U.S. litigants may feel that the document provides very little guidance or relief. For example, the Working Party urges the use of the Hague Convention as a first method of transferring data to the U.S. even though the Working Party recognizes that all member states have not signed the Hague Convention and that the procedures set forth in the convention are less than efficient. The Working Party paper is, however, useful in that it seeks to identify many of the key issues that arise as a result of the conflict in the legal regimes.

What Next?

In its paper, the Working Party acknowledges that resolving the issues involved in cross-border discovery is beyond the scope of a Working Party opinion and calls instead for a government solution. For the time being, at least from a European perspective, it seems that the issue is being left to data protection authorities and national courts to resolve.

Our Advice - Risk Reduction Strategies

In the meantime, the following measures may help to reduce risk:

- Allocating roles and responsibilities for this issue internally;
- Mapping corporate information management infrastructure so that there is an understanding of where personal data is located;
- Adopting a clear privacy policy, providing notice contemplating disclosures of EU personal data in U.S. litigation, including in pre-trial discovery;
- Adopting or revising records storage, retention and destruction policies to contain fixed retention schedules;

- Adopting detailed network monitoring and use policies that contemplate the review of employee email and other data;
- Ensuring European workers union/counsel agreements adequately address this issue;
- Establishing a plan for the retention and transfer of corporate data for U.S. litigation, including considering a corporate transfer solution such as binding corporate rules;
- Considering obtaining advance consent from key personnel to the disclosure of their personal data;
- Providing training to key personnel, especially personnel who may be involved in the processing or transfer of data for litigation outside the EU;
- Learning the enforcement attitudes of the data protection authorities in relevant European jurisdictions; and
- Monitoring enforcement actions in relevant European jurisdictions.

If you would like advice and guidance on how to reconcile the demands of the U.S. litigation process with the requirements of the Directive, please contact us.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeane A. Thomas, CIPP/E
Partner – Washington, D.C., Brussels
Phone: +1 202.624.2877, +32.2.282.4082
Email: jthomas@crowell.com

Kris D. Meade
Partner – Washington, D.C.
Phone: +1 202.624.2854
Email: kmeade@crowell.com