European Data Protection Law v E-Discovery Requirements under US Law – How to Tackle the Dilemma

By John J. Rosenthal and Stefan Hanloser

Data protection is antagonistically opposed to discovery: discovery promotes the disclosure of data whereas data protection is intended to prevent such disclosure. The underlying legal principles of both are often in conflict in the context of civil litigation both in the United States and in Member States of the European Union. In this regard, neither the disclosure nor discovery rules of the US and European courts have been harmonised. This often places European companies that are doing business in the United States (or that have their parent company, a subsidiary, or an affiliate in the United States) in a dilemma—comply with compulsory discovery/disclosure obligations v. protecting your employees' and customers' data. However, the consequences of this dilemma can be avoided, or at least mitigated.

Discovery Requirements under US Law and Discovery Restrictions under European Data Protection Law

Recent amendments to US pre-trial discovery require the responding party to search for and produce electronically stored information (ESI) regardless of where that information is stored within the corporate information technology infrastructure. Often, ESI stored within with a facility located in an EU Member State may indeed be subject to discovery in the United States.

Under European Data Protection Directive 95/46/EC, "personal data" is any information relating to an identified or identifiable natural person; "processing" of personal data includes the disclosure of personal data by transfer to a third party. Responsive electronic files and e-mails (including electronic files attached to e-mails) may contain personal data. An example would be responsive e-mails that contain personal data relating to the responding party's customers. The Directive further restricts the transfer to any non-EU state that does not afford the same privacy protections as an EU Member State. In this regard, the United States is expressly recognised as a country that does not afford such protections.

Circumstances under Which Personal Data Can Be Transferred

Unfortunately, the laws and regulations surrounding when and how data can be transferred to the United States remain a web of confusion with no necessarily clear answers. There are, however, certain best practices that should be followed when transferring "personal data" to the United States for the purposes of discovery.

First, personal data may generally be transferred if the data subject, for instance the customer, has given its unambiguous prior consent. It is, however, uncommon to ask for the consent to a disclosure for discovery purposes in advance.

Second, data transfer may also be permitted if the legitimate interests of the responding party prevail. This "balancing of interests" necessarily leaves the responding party with the uncertainty whether the national data protection authorities, if becoming aware of the data transfer, will actually find that the responding party's legitimate interest in defending its rights in a court trial outweigh the conflicting interests of the data subjects.

Third, even if the personal data can be transferred in principle, a transfer is justified under Article 26(2)(d) Data Protection Directive only if "the transfer is necessary or legally required … for the establishment, exercise or defence of legal claims". Interestingly, however, the "Article 29 Working Party", an advisory board composed of the national data protection authorities of each EU Member State, claims in its "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC" of 25 November 2005 that the exception of Article 26(2)(d) "can only be applied if the rules governing … this type of international situation have been complied with, notably as they derive from the provisions of the Hague Conventions of 18 March 1970 ('Taking of Evidence' Convention) …" As a consequence, the transfer of electronic files and e-mails to the United States in compliance with the Hague Convention would become particularly burdensome in most Member States. Moreover, Member States like Germany have declared that they will not execute Letters of Request under the Hague Convention that were "issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries".

Fourth, transfer could also take place under the guise of a "safe harbor" or "binding corporate contract". Corporations that have implemented privacy policies consistent with the Data Protection Directive are permitted, in exchange, to transfer the data to the United States.

Finally, it is within a US court's discretion to order discovery even if the responding party is forced to infringe European data protection law. When ordered, this places the company in a difficult position of having to violate the EU Director or face potential sanctions before the US courts.

Practical Advice

In order to address the conflicting obligations regarding discovery v. data protection, we suggest several practical steps. Generally speaking, whereas US companies are likely to have implemented strict data retention policies that require the erasure of backup data once they are no longer required, their European affiliates might still take a rather lax approach. For companies with a transatlantic business focus, it is therefore worth developing uniform, worldwide data retention policies that limit the amount of unnecessarily stored data.

Strategically speaking, the data protection laws of the EU Member States also offer various opportunities to avoid, limit or delay the discovery of unfavourable data stored in Europe. Some US courts are in fact responsive to objections against discovery requests if the requested party would be in violation of EU data protection laws. In *Volkswagen v Valdez*, 909 S.W.2d 900 (Tex. 1995), the Supreme Court of Texas reversed a decision that required Volkswagen to produce its corporate phone book as, in order to do so, Volkswagen would be in violation of German data protection law.

The responding party should also make sure that a protective order contains language that allows the redaction of non-responsive personal data in electronic documents of European origin that are otherwise responsive. The dissemination of responsive personal data by the requesting party should be explicitly limited, if not prohibited, under the protective order.

Finally, we strongly suggest that, if you are a company with operations in the United States, you secure a "safe harbour" or "binding corporate contract" status that would allow you to transfer data to the United States consistent with the EU data protection laws.

Some US courts are in fact responsive to objections against discovery requests if the requested party would be in violation of EU data protection laws.

John J. Rosenthal is a partner in the Washington, D.C., office of Howrey LLP. He can be contacted at rosenthalj@howrey.com.

Dr. Stefan Hanloser is a senior associate in the Munich and Washington, D.C., offices of Howrey LLP. He can be reached at hanlosers@howrey.com.