HOWREY LLP

Client Alert

E-DISCOVERY UPDATE | FEBRUARY 25, 2009

NEW GUIDELINES FOR THE RECONCILIATION OF E-DISCOVERY RULES AND EUROPEAN PRIVACY AND DATA PROTECTION LAW

GILBERT S. KETELTAS

STEFAN HANLOSER

The underlying legal principles of US discovery and European data protection are often in conflict. This conflict is heightened in litigation involving multinational corporations with relevant data located in Europe given the dramatic increase in electronic information and a US discovery model that expressly recognizes the importance of the preservation, collection and production of electronically-stored information (ESI). A party that receives a request for the production of personal data that is, for instance, stored on a server of a European subsidiary or affiliate is often placed in a dilemma—satisfy compulsory US discovery obligations or comply with European data protection laws.

On February 11, 2009, the European Data Protection Working Party—an independent European advisory board on data protection and privacy—adopted Working Paper 158 concerning "pre-trial discovery for cross-border civil litigation."[1] The Working Paper aims to reconcile the "demands of the litigation process in foreign [non-European] jurisdictions" with European data protection obligations.

Summary Practice Pointers

- The Working Paper covers the retention, preservation or archiving of data for litigation purposes (referred to in Europe as "processing"), and discovery of such data in US civil litigation. It expressly does not address "[d]ocument production in US criminal and regulatory investigations" or "[c]riminal offences in the US relating to data destruction."
- The Working Paper recognizes that the transfer of personal data for litigation purposes to the United States is not illegal per se under the European Data Protection Directive (95/46/EC). But such data transfers must follow specific requirements of the Data Protection Directive to comply with European privacy and data protection law.
- If personal data is relevant to a pending, imminent, or reasonably foreseeable litigation, it may be retained until the termination of the proceedings.
- The Directive permits the transfer of personal data to a country with an inadequate data protection level, for instance the US under European standards, if the transfer is necessary or legally required for the establishment, exercise or defense of legal claims in court, however, in the Working Group's view, only if there is one single transfer of all relevant data.
- Non-responsive documents that contain personal data should be culled in the EU Member State and irrelevant personal data on responsive documents should be redacted in the Member State so that only relevant personal data is actually transferred to the US and disclosed to the requesting party.
- The data subject's freely given, specific and informed prior consent to a later data processing for litigation purposes can only be expected in rare cases, for instance if the individual is involved in

[1] WP 158 of February 11, 2009; <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf>

the litigation, and will not typically be a basis for finding that the "processing" of personal information in Europe is legitimate.

- An obligation imposed by a non-EU legal statute or regulation will not usually justify data processing within the EU (unless, for example, an individual Member State recognizes an obligation to comply with an order of a foreign court).
- If the identity of the data subject is irrelevant, data should be anonymised or pseudonymised.
- The Working Party finally recognizes that a request under the Hague Convention on the taking of evidence[2] is a valid ground for a data transfer to the US in compliance with the Directive.

The Standing of the Working Party

The Working Party is an independent advisory body on European privacy and data protection law. It is composed of data protection officials from EU Member States, the European Data Protection Supervisor and the European Commission. The Working Party's opinions and guidelines expressed in its Working Papers are not binding on the national data protection authorities but are persuasive authority. To give a most recent example: In its decision[3] on the structuring and management of whistle-blower hotlines under the Sarbanes-Oxley Act by European affiliates of US companies in compliance with European privacy and data protection law, the Austrian Data Protection Commission explicitly adopted the key principles developed by the Article 29 Working Party in its Working Paper 117 on "the application of EU data protection rules to internal whistle-blowing schemes". Therefore, the European data protection authorities, when required to decide on data processing related to US-style e-discovery, are likely to follow the guidelines set out in WP 158. And parties to US litigation are likely to invoke the guidelines when arguing over the extent to which European privacy and data protection law permits or restricts the transfer of personal data to the US for litigation purposes.

The New Guidelines in Detail

The Working Paper assesses the handling of data in litigation in two different areas: (1) the general legal requirements for the retention of personal data by the responding party during the preservation phase and the later transfer of such data to the requesting party during the production phase; and (2) the specific legal requirements for a data export to third countries that lack—from the point of view of the European Commission or the national data protection authorities—an adequate level of protection (like the United States with its sector-specific privacy laws).

General Requirements for the Retention and Transfer of Personal Data

Whenever litigation or regulatory investigations and proceedings are reasonably anticipated by a legal entity, no matter whether the entity is the initiator or the target of litigation, it has a duty to preserve the potentially relevant data, i.e. protect it from destruction or alteration. Under the European Data Protection Directive, the *retention* of data constitutes "processing" and requires justification under Article 7 of the Directive. This is the same with the later *transfer* of personal data to the requesting party, which is also deemed to be data processing under European data protection law.

The data subject's consent to data processing for litigation purposes under Article 7(a) of the Directive can only be expected in rare cases. In practice, the boiler-plate declarations of consent signed by employees or customers are often insufficient to cover data processing in legal proceedings with a third-party. In addition, the Working Group casts doubt on whether employees can give their consent voluntarily if asked to do so by their employer once a litigation is anticipated or even pending.

Since, in the Working Group's view, an obligation imposed by a foreign statute or regulation does not typically qualify as a "legal obligation" within the meaning of Article 7(c) of the Directive, discovery obligations under the Federal Rules for Civil Procedure cannot justify data processing within the EU either.

[2] Hague Convention on the taking of evidence abroad in civil and commercial matters of March, 18, 1970.
[3] Decision of December 5, 2008; <http://www.ris2.bka.gv.at/Dsk/> (in German only).

But under Article 7(f) of the Directive, personal data my be processed if legitimate interests necessitate the processing, unless such legitimate interests are overridden by the interests […]or[4] fundamental rights and freedoms of the data subject. The Working Party gives some guidance how to balance the conflicting interests under Article 7(f) of the Directive: If the personal data is irrelevant, the responding party cannot claim any legitimate interests in processing such data for litigation purposes. Therefore, if the identity of the data subject is irrelevant, data should be anonymised or at least pseudonymised, the Working Party argues. Non-responsive documents that contain personal data should be filtered out in the EU Member State and irrelevant personal data on responsive documents should be redacted in the Member State so that only relevant personal data is transferred to the US and disclosed to the requesting party. In practice, the disclosing party is required to seek the requesting party's agreement (i) for the production of anonymised or pseudonymised documents or data and (ii) for the redaction of irrelevant personal data on responsive documents.

Specific Requirements for the Export of Personal Data to the US

Rightly, the Working Group singles out Article 26(1)(d) of the Directive which explicitly permits the transfer of personal data to a country with what the EU characterizes as an "inadequate data protection level," for instance the US, if the transfer is necessary or legally required for the establishment, exercise or defense of legal claims [in court[5]]. This provision is in fact key to the reconciliation of e-discovery rules and European privacy and data protection law. However, the Working Group restricts this beneficial provision to cases "[w]here the transfer of personal data for litigation purposes is likely to be a single transfer of all relevant information" without even giving an explanation for this potentially burdensome limitation. As an alternative, only a subscription to the Safe Harbor Programme, the implementation of Binding Corporate Rules or the signing of Standard Contractual Clauses could be an option to legalize a data export to the US

The Working Group's reference to the Hague Convention is of little practical relevance since a Letter of Request procedure is seen as "unduly time consuming and burdensome"[6] and some European countries like Germany, Italy, and Spain, do not "execute Letters of Request [for] pre-trial discovery".

FOR FURTHER INFORMATION:

For further information regarding the topic(s) discussed in this briefing paper, please contact any Howrey attorney with whom you have an existing relationship or any of the individuals listed below:

Gilbert S. Keteltas, Partner
1299 Pennsylvania Ave., NW
Washington, DC 20004
t. +1 202.383.7060
f. +1 202.383.6610
KeteltasG@howrey.com

Stefan Hanloser, Senior Associate
Gmunder Straße 53
81379 Munich, Germany
t. +49 89 20308 1234
f. +49 89 20308 1201
HanloserS@howrey.com

[4] In the English translation of the Directive there is a typo at this point; in all other languages it reads "or", not "for".
[5] In the English translation of the Directive the restriction "in court" was left out by mistake.
[6] *Société Nationale Industrielle Aérospatiale* v. *US Dist. Ct.*, 482 US 522, 542 (1987).