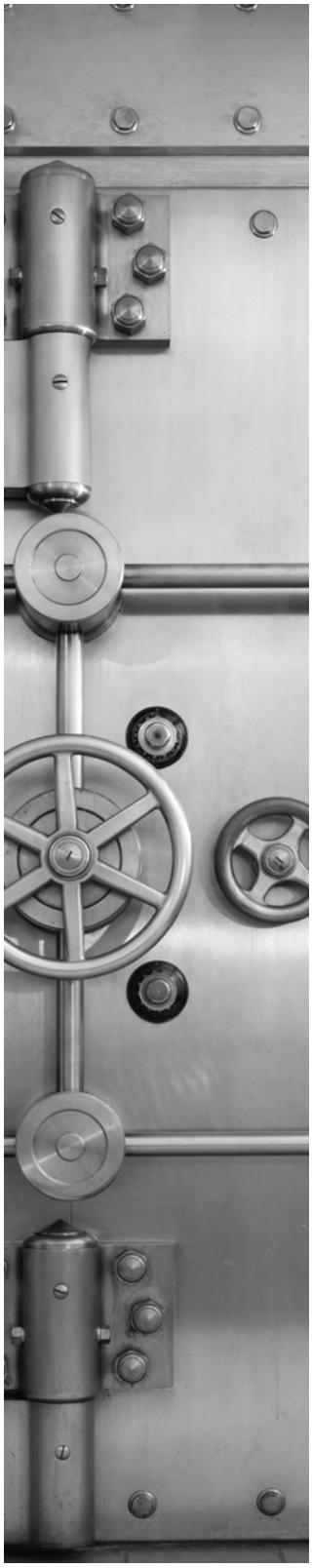
PRIVACY UPDATE

HOGAN & HARTSON



How to Conduct Trans-Border Discovery

New EU Guidelines Shed Light on Compliance Issues Relating to U.S. Civil Discovery

Introduction

Complying with U.S. Federal Rules of Civil Procedure while simultaneously respecting EU data privacy rules can be problematic for multinational companies that are required to disclose internal documents for U.S. litigation purposes – particularly when those documents include personal data as defined by the EU Data Protection Directive. Until recently, there was little guidance on this issue from European data protection authorities, exacerbating the legal uncertainty and compliance difficulties.

On February 17, 2009, the Article 29 Working Party published its long-awaited guidelines for litigating parties, which are intended to help them reconcile the demands of the litigation process in the U.S. with the data privacy obligations imposed by the EU Data Protection Directive. The Working Party is an independent EU advisory body consisting of representatives of the European Commission and the EU Member States' data protection authorities. It provides guidance on how to interpret and apply the provisions of EU Data Protection Directive uniformly throughout the EU. Although its opinions, recommendations, and working documents are not legally binding, they often become the "EU standard" for privacy compliance.

Scope

The guidelines cover two aspects of U.S. civil litigation, namely pre-emptive document preservation in anticipation of proceedings before U.S. courts or in response to requests for litigation hold, and pre-trial discovery requests in U.S. civil litigation. The guidelines are not intended to cover document production in U.S. criminal and regulatory investigations, nor do they address criminal offenses in the U.S. relating to data destruction.

The guidelines offer standards by which companies anticipating or engaged in litigation can evaluate their requirements pursuant to U.S. litigation demands in contrast with the EU Data Protection Directive.

Guidance Summary

Data Retention

Litigating parties may implement litigation holds or pre-emptive retention of information, including personal data, in anticipation of litigation. However, any retention of personal data in the EU for

purposes of future litigation must have a legal basis and legitimate purpose under the EU Data Protection Directive.

- Personal data should not be stored for an unlimited period of time because of the mere possibility of litigation in the U.S.: in the ordinary course of business, it should be possible to implement short retention periods (based on EU Member State legal requirements) without violating U.S. Federal Rules of Civil Procedure, as these rules only require the disclosure of *existing* information.
- Personal data relevant to specific or imminent litigation may be retained until the conclusion of the proceedings (including appeal periods).

Legitimate Purpose

Personal data can only be processed for pre-trial discovery purposes on one (or more) of the legitimate grounds identified by the EU Data Protection Directive. In this particular context, there appear to be three relevant grounds, namely 1) consent of the individual; 2) necessity to comply with a legal obligation; and 3) pursuance of a legitimate interest. The third ground is the most likely to provide a valid basis for processing data pursuant to litigation demands.

1. Consent is unlikely to constitute a suitable legal basis in most cases because of the difficulty in producing clear evidence of the fact that freely given, specific, and informed consent was obtained. Moreover, valid consent implies that individuals should be able to withdraw their consent without suffering any consequences, which is not possible in the context of discovery. Therefore, relying on consent may prove to be complex and cumbersome in practice. Consent should be relied on in exceptional situations only, *e.g.,* if the individual is aware of, or even involved in the litigation process, or if sensitive personal data (*i.e.*, heath-related data) are being processed;
2. Processing of personal data in the EU would be legitimate if it is necessary for compliance with a legal obligation in a Member State. Obligations imposed by foreign (*i.e.*, non-EU) laws or regulations may not qualify for this particular purpose; and
3. Processing personal data in pre-trial discovery situations may be necessary for the data controller (or a third-party recipient) to pursue a legitimate interest (compliance with U.S. litigation demands). Promoting or defending a legal right in court constitutes such legitimate interest. However, this legitimate interest must be weighed against the freedoms and rights of individuals who may not be directly involved in the litigation, but whose personal data are being processed as part of the litigation. The balance of interests test should take into account issues of proportionality, the relevance of the data to the litigation, as well as possible ramifications for impacted individuals. To safeguard individuals' privacy rights, disclosure should be restricted – if possible – to anonymized or encoded data. Furthermore, irrelevant data should be filtered so that eventually a more limited set of personal data may be disclosed.

HOGAN & HARTSON

Proportionality

The guidelines provide suggestions on how to weigh the proportionality of risk associated with the data proposed to be processed. Some of these standards may be difficult to apply to real-life discovery scenarios.

- Personal data must be relevant and not excessive in relation to the purposes for which they were collected and/or further processed.
- Parties involved in litigation have a duty to take such steps as are appropriate to limit the discovery of personal data to that which is objectively relevant to the issues being litigated. Unless an individual's identity is relevant to the cause of action, it may be sufficient to provide data in anonymous or encoded form.
- To the extent that personally identifiable information (as opposed to anonymized or encoded data) is necessary for trial purposes, "filtering" the irrelevant personal data should be carried out, preferably in the country where the data were found (and before they are sent to another jurisdiction outside the EU). In some cases, it may be advisable to use the services of a trusted third party – such as a law firm – located in an EU Member State to determine the relevance of personal data to the litigation.
- Litigating parties that qualify as data controllers in the EU should approach the U.S. courts to explain the data protection obligations upon them and possibly request protective orders to comply with EU and national data privacy rules.

Transparency

Consistent with the EU Data Protection Directive, the guidelines suggest notice to affected individuals that their personal data has been or may be processed.

- At the pre-trial discovery stage, individuals should be given advance, general notice of the possibility that their personal data may need to be processed for litigation purposes.
- When personal data are actually processed for trial purposes, affected individuals should be given notice of the identity of any recipients, the purposes of the processing, the categories of data concerned, and details on the individuals' rights.
- In most cases, individuals should be informed as soon as reasonably practicable after the data are processed. However, such notification may be delayed if there is a substantial risk that notifying a particular individual would jeopardize the litigating party's ability to investigate the case properly and gather the necessary evidence.

Rights of Access, Rectification and Erasure

- The EU Data Protection Directive provides individuals with the right to access and modify their personal data that has been collected, regardless of the form in which they are collected (*e.g.*, electronic or paper). The guidelines echo this requirement with regard to litigation demands. The tension between this recommendation and U.S. litigation requirements is that, contrary to EU data protection rules, U.S. discovery rules do not allow for incomplete production, require the production of complete original documents,

as well as any modified documents, and impose penalties for document destruction/erasure.

Data Security

- All reasonable technical and organizational measures must be taken to protect personal data from accidental or unlawful destruction or accidental loss and unauthorized disclosure or access. These measures must be proportionate to the purposes of investigating the issues raised in accordance with the security regulations established in the different Member States.
- Protective measures should be provided by the litigating parties, their lawyers as well as other experts involved in the litigation.

External Service Providers

- Parties using external service providers to assist in the litigation process (*e.g.*, as expert witnesses) remain responsible (as "data controllers") for the data processing of such service providers. These external service providers must comply with all the principles of the EU Data Protection Directive, and the litigating parties must periodically verify compliance by their external service providers.

Data Transfers

- Where litigation purposes require that significant amounts of personal data are sent outside the EU and the recipient's jurisdiction does not ensure an adequate level of protection (such as the U.S.) as required under the EU Data Protection Directive, the data may be transferred provided that:
    1. The recipient is established in the U.S. and has subscribed to the EU/U.S. Safe Harbor scheme;
    2. The recipient has entered into a data transfer contract with the data exporter (*e.g.*, based on the European Commission's Standard Contractual Clauses); and
    3. The recipient has put in place Binding Corporate Rules for its cross-border data flows.
- Where the transfer of personal data for litigation purposes is likely to be a single transfer of relevant information, there is an argument that the data processing is necessary or legally required for the establishment, exercise, or defense of legal claims (in which case there would arguably be less need for Safe Harbor adherence, data transfer contracts or Binding Corporate Rules). However, this argument may not be effective for transferring all employee files to a group's parent company on the grounds of the possibility that legal proceedings may be brought one day in U.S. courts.

- Compliance with a request made under the Hague Convention (on the Taking of Evidence Abroad in Civil or Commercial Matters) would also provide a formal basis for transferring personal data. Where it is possible for The Hague Convention to be used, this approach should be considered first as a method for transferring personal data for litigation purposes, before considering other transfer options.

Conclusion

The guidelines provide useful insight into how the European data protection authorities (through their representatives in the Article 29 Working Party) perceive the privacy compliance issues resulting from discovery obligations imposed by U.S. Federal Rules of Civil Procedure. These guidelines are a useful first official dialogue in this thorny cross-border issue. Unfortunately, the guidelines apply to U.S. civil litigation issues only, and it is unclear whether additional guidance (dealing with U.S. criminal and regulatory investigations) can be expected in the near future.

Moreover, some of the compliance solutions proposed by the guidelines (*e.g.*, the use of protective orders, and allowing continual ability to access and modify personal data) may not be practical in all cases. It is noteworthy that the Working Party appears to have defined a new role for privacy and litigation experts in Europe by suggesting that litigation parties could require the services of a "trusted third party" in order to decide on the relevance of data in accordance with U.S. Federal Rules of Civil Procedure.

***

About the Privacy Update

Hogan & Hartson frequently publishes the *Privacy Update* to track privacy developments at the FTC, FCC, and U.S. Congress, as well as in the EU. If you have questions or would like more information about this development, please contact one of the lawyers listed below or any Hogan & Hartson attorney with whom you regularly work.

WIM NAUWELAERTS
wnauwelaerts@hhlaw.com
+32.2.505.0959
Brussels

WINSTON J. MAXWELL
wjmaxwell@hhlaw.com
+33.1.55.73.23.20
Paris

LYNDA K. MARSHALL
lkmarshall@hhlaw.com
+1.202.637.5838
Washington, D.C.

HANNO TIMNER
htimner@hhlaw.com
+49.30.726.115.235
Berlin