



# DIGITAL DISCOVERY & E-EVIDENCE



**VOL. 9, NO. 3**

**REPORT**

**MARCH 1, 2009**

Reproduced with permission from Digital Discovery & e-Evidence, 9 DDEE 73, 03/01/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

**SPECIAL REPORT**

A long-awaited Opinion from the European Union’s Article 29 Data Protection Working Party provides recommendations and observations regarding several aspects of the interplay between U.S. discovery and EU data protection including preservation, legitimate grounds for processing personal data in litigation, transparency, and the rights of data subjects in litigation. Drinker Biddle & Reath’s David J. Kessler and Peter Blenkinsop provide summary and analysis of the Opinion.

## **European Union Working Party Issues Opinion Regarding Guidelines for Addressing Conflict Between EU Data Protection Regulations and U.S. Discovery Obligations**

BY DAVID J. KESSLER AND PETER BLENKINSOP

**O**n February 17, the European Union’s Article 29 Data Protection Working Party made public its adoption six days earlier of Working Document 1/2009 on Pre-Trial Discovery For Cross Border Civil Litigation (WP 158) (the “Opinion”). The Working Party is an advisory board created under the EU Data Protection Directive (the “Directive”) and composed of Data Protection Authorities (DPAs) from each member state.

The Opinion is an outgrowth of concerns raised by DPAs to the Working Party in April 2007 and by CNIL (the French DPA), which issued a statement identifying four areas where data processing and transfers could give rise to problems under “French or European Law,” particularly regarding privacy: litigation hold/litigation freeze, pre-trial discovery, information injunctions by public U.S. authorities, and the creation of a new of-

fense called “information destruction.”<sup>1</sup> As a result of these concerns, the Working Party announced last February that it was making “pre-trial discovery” a high priority for 2008.

Citing *Societe Nationale Industrielle Aerospatiale et al. v. United States District Court for the Southern District of Iowa*, 482 U.S. 522, 544 n. 28 (1987) and the Sedona Conference’s® *Framework For Analysis of Cross Border Discovery Conflicts*, the Working Party recognizes the very real tension between a company’s need

<sup>1</sup> The Opinion only addresses the potential conflict between U.S. obligations to preserve information and pre-trial discovery requests and the EU data protection directive. The Working Party specifically did not address the two other issues raised by CNIL: (1) document production in U.S. criminal and regulatory investigations and (2) criminal offices in the U.S. related to data destruction. (Opinion, p. 3.)

to make or defend claims in litigation—which includes, at least in the United States, its obligations to produce relevant and responsive data held in the EU—and its obligation to protect and secure the personal data of third parties in the EU—namely a company’s employees and customers.

The Opinion is meant to provide guidance to data controllers (i.e. companies) that are trying to reconcile their obligations to produce data in litigation (mostly within the United States) that is subject to EU laws regarding the processing and transfer of personal data.

**First Steps.** In the end, the Working Party describes the Opinion as “an initial consideration of the issue of the transfer of personal data for use in cross border civil litigation” and as “an invitation to public consultation with interested parties, courts in other jurisdictions and others.” (Opinion, p. 14.) In addition, the Working Party acknowledges that “resolving the issues of pre-trial discovery is beyond the scope of an Opinion by the Working Party and that these matters can only be resolved on a governmental basis, perhaps with the introduction of further global agreements along the lines of the Hague Convention.” (Opinion, p. 2.)

## The EU Data Protection Directive

The Directive is an omnibus privacy regulation that restricts how businesses may use and disclose personal data—which includes not only information relating to an identified person, but also identifiable information. As a matter of course, the term “personal data” is read very broadly.

Under the Directive, personal data may not be “processed”—another broadly read term that includes collection, transfer, use, disclosure, destruction, preservation—unless necessary for one of several enumerated purposes. Among the several purposes detailed in the Directive, three have looked promising for legitimizing the processing of personal data for litigation:

- (1) consent of the data subject,
- (2) that compliance with pre-trial discovery is necessary for compliance with a legal obligation, or
- (3) if the data furthers the purposes of a legitimate interest pursued by the data controller or by the third party to whom the data is disclosed under Article 7(f) of the Directive.

The Opinion addresses each of these purposes.

**Balancing Competing Interests.** In prior decisions, DPAs have found that the Directive’s reference to a “legal obligation” is only applicable to an obligation imposed by community or member state law (and, thus, obligations imposed by the United States would be irrelevant). Moreover, they have indicated that in determining whether a data controller or third party recipient has an overriding interest in processing data, a balancing of interests test must be conducted that takes into account the rights and interests of the data subject.

These rights and interests include, inter alia: the interest in transparency, including being provided with notice of the identity of the controller, the purposes of the processing, and recipients of the data; the right to access personal data about oneself and have inaccurate or incomplete data amended or deleted; and the interest in having personal data about oneself safeguarded

from loss, misuse, unauthorized access, and other security risks.

## Record Retention and Preservation

The Opinion addresses conduct occurring even before the start of litigation, providing guidance on information management and pre-litigation preservation.

**Record Management Policies and Schedules Are Appropriate and Recommended.** Acknowledging that companies operating in the EU have no legal grounds to store personal data for an unlimited period of time because of litigation and that U.S. obligations only require the production of existing data, the Opinion encourages companies to adopt and implement information management systems that destroy obsolete data. In fact, the Working Party notes that “even in the United States there has recently been a tendency to adopt restrictive retention policies to reduce the likelihood of discovery requests.” (Opinion, p. 8.) With U.S. discovery obligations spilling into the EU, it makes sense that best practices to limit discovery costs would follow.

**Preservation of Personal Data Is a Legitimate Interest for Pending or Reasonably Anticipated Litigation.** The Opinion is explicit: “If on the other hand the personal data is relevant and to be used in a specific or imminent litigation process, it *should* be retained until the conclusion of the proceedings . . . There may be a requirement for ‘litigation hold’ or pre-emptive retention of information, including personal data. In effect, this is the suspension of the company’s retention and destruction policies for documents which may be relevant to the legal claim that has been filed at court or where it is ‘reasonably anticipated.’ ” (Opinion, p. 8 (emphasis supplied).)

**Preservation for Potential, Future Litigation Not Legitimate.** The Opinion is equally explicit the other way: “The mere or unsubstantiated possibility that an action may be brought before the U.S. courts is not sufficient” reason to preserve personal data held in the EU (Opinion, p. 8.)

## Legitimacy of Processing for Purposes of Litigation

One of the thorniest questions for companies attempting to resolve conflicts between U.S. discovery obligations and EU data protection requirements is whether processing data for U.S. litigation is a legitimate purpose under the Directive. The Working Party, after analyzing three potentially promising grounds for processing personal data in U.S. litigations, finds only one ground that may be proper and only if it is not overridden by the interests of the data subject.

**Generally, Consent Is Not a Legitimate Basis for Processing Personal Data.** The Working Party concludes that “it is unlikely that in most cases consent would provide a good basis for processing.” (Opinion, p. 8.) However, the document recognizes that where consent can be freely given (i.e., without risk of penalty for withholding consent and with the opportunity to withdraw consent at a later time), it may properly be relied upon as a ground for processing.

**Generally, Compliance With a Legal Obligation Is Also Not a Legitimate Basis for Processing Personal Data.** The Opinion finds that obligations imposed by foreign statutes or regulations may not qualify as legal obligations under the Directive.

**Processing Necessary for the Purpose of a Legitimate Interest Is a Legitimate Basis Only When Not Overridden by Interests of the Data Subject's Fundamental Rights and Freedoms.** To balance these two interests, the Working Party recommends that companies weigh issues of proportionality, the relevance of the personal data at issue, and the consequences of the data subject (all of which can also be considered by U.S. courts in either their standard comity analysis or under its new “not reasonably accessible” analysis under Fed. R. Civ. P. 26(b)(2)(B)).

To assist companies in balancing these interests, the Working Party makes several additional recommendations:

- Where possible, companies should limit disclosure of personal data to anonymised or pseudonymised data.
- The best practice is to perform as much culling and review as reasonably possible in the country the data was originally stored (which could potentially mean that companies collecting data from multiple locations would need to process and cull it in multiple locations before consolidating it).
- Companies should be particularly wary of producing sensitive personal data and other special categories of information such as privileged communications.
- At each stage of discovery, from identification and preservation through production and presentation, companies should involve their data protection officers.

## Transparency and Rights of Access, Rectification, and Erasure

**Companies Should Provide General and Specific Notices That Personal Data May Be Processed in Litigation.** To comply with the principle of transparency, the document indicates that general notice of the possibility of personal data being processed for litigation should be provided. (For example, in contracts for employment, European companies may wish to alert their employees regarding the risk of the need to transfer their personal data to the U.S. for legal purposes.)

The Opinion also indicates that where personal data is actually processed for litigation purposes, specific notice should be given of the identity of any recipients, the purposes of the processing, the categories of data concerned, the existence of rights concerning access, rectification and erasure, and where the processing is based on Art. 7(f), of the right to object on compelling legitimate grounds to the processing.

**Notice May Be Delayed if There is a ‘Substantial Risk’ of Interference With the Company's Ability to Investigate or Preserve Evidence.** Referencing its Opinion on internal whistleblowing schemes, the Working Party states that an exception to the notice rule is necessary where notification of one or more data subjects might undermine the ability of the company to preserve evidence. The Opinion stresses, however, that this exception must be applied narrowly on a case-by-case basis.

**Rights of the Data Subject Persist During the Litigation and There Is No General Waiver of the Rights to Access or Amend.** The Opinion is clear that data subjects’ rights under Article 12 of the Directive do not end when litigation begins. Based on this conclusion, the Working Party makes several recommendations and observations, including:

- These obligations should be imposed on parties receiving the data (i.e., opposing parties), possibly through protective orders.
- These rights may be restricted under Article 13 on a case-by-case basis, for example where it is necessary to protect the rights and freedoms of others.
- A data subject’s right to amend or delete (even for corrective purposes) can conflict with a company’s obligation to preserve data and could be seen as altering evidence in litigation.

## Data Security

**Companies Must Provide Reasonable Security for Data Within Their Possession and at Their Law Firms and Other Providers.** The Opinion states that “requirements are to be imposed not just on the data controller but such measures as [are] appropriate should also be provided by the law firms who are dealing with the litigation together with any litigation support services and all other experts who are involved with the collection or review of the information.” (Opinion, p. 12.)

**Vendors Will Need to Comply With the Directive if They Handle Personal Data Originating From the EU.** “In particular they must abide by strict confidentiality obligations and communicate the information processed only to specific persons. They must also comply with the retention periods by which the data controller is bound.” (Opinion, p. 13.)

**The Working Party Believes U.S. Courts May Need to Implement Similar Security Measures.** The Working Party concludes that court services in relevant jurisdictions would need to be employed as “personal data relevant to the case would be held by the courts for the purposes of determining the outcome of the case.” (Opinion, p. 13.)

## Implications

The Working Party’s conclusions regarding the interplay between U.S. regulation and EU data protection regulations are not surprising and do not mark a major shift in policy. However, the Working Party’s guidance provides a better-lit path for companies, their lawyers, and their privacy officers to follow in an area that is still more in shadow than not.

The Opinion provides helpful direction regarding record retention (an unexpected aid to companies trying to implement such policies in the EU), preservation (a help to companies who were worried that even preserving data in pending litigations was running afoul of the directive), and understanding the rights of data subjects in litigation when their data lands on U.S. soil (the Working Party is clear that it believes that these rights continue on).

One interesting possible ramification of the Opinion is its conclusion that requesting parties who obtain personal data that is held in Europe must have the ability

to allow data subjects to at least review their data. This added burden may induce certain requesting parties to limit or, at least, more thoughtfully consider the scope of their requests so as not to incur unnecessarily the cost of sophisticated review tools that allow EU citizens access to specific documents and data.

As the Working Party remarks, this is only the beginning of the conversation, and more work needs to be done on both sides of the Atlantic to address cross-border discovery, but it appears to be a good start to the dialogue. Now its up to litigators, multi-national companies, interested groups like the Sedona Conference®, and the U.S. courts to continue the discussion.

*David J. Kessler is a partner at Drinker Biddle & Reath in its Intellectual Property and Commercial Litigation groups. David was one of the founders of the firm's E-Discovery and Data Management Team and as national e-discovery counsel represents his clients regarding both strategic and tactical e-discovery issues as well as information management choices. David is also a member of both Working Group 1 and Working Group 6 of the Sedona Conference®.*

*Peter Blenkinsop is an associate in the Washington, D.C. office of Drinker Biddle & Reath LLP., where he focuses on privacy and data security law.*