BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Assessing the EU Working Party's Guidance on Harmonizing U.S. Discovery and EU Data Protection Requirements

By Alan Charles Raul, Edward R. McNicholas, John Casanova, Laurent Ruessmann, William Long and Julie Dwyer

The European Union's Article 29 Data Protection Working Party has taken an important first step toward reconciling EU data protection obligations with the information disclosure requirements of U.S. discovery rules. In a working document adopted Feb. 11 (the Guidelines),[1] the Article 29 Data Protection Working Party, comprising data protection representatives from each of the EU Member States, offers well-reasoned, pragmatic guidance for multinational companies faced with the need to comply with EU data protection requirements in the context of U.S. civil pre-trial discovery. While the Guidelines are not binding, they lay the groundwork for practicable solutions. Multinationals should review their discovery related policies and procedures in the light of the Guidelines and consider giving input to the Working Party to facilitate the development of even more specific practical guidance.

Alan Charles Raul and Edward R. McNicholas are partners in the Privacy, Data Security and Information Law Group of the Washington office of the international law firm of Sidley Austin LLP. McNicholas is a member of BNA's Privacy and Security Law Report Advisory Board. John Casanova is a partner and William Long is counsel in the Group and work from Sidley's London office. Laurent Ruessmann is a partner in the Group and works out of Sidley's Brussels office. Julie Dwyer is a former associate at Sidley and is now consultant to the firm. The views expressly herein are those of the author personally and do not necessarily reflect the views of any governmental or private entity, client, or association. This article is published for informational purpose only and is not legal advice. Readers should not act upon this article without seeking advice from professional advisers.

Balanced overall approach to U.S. discovery demands

Companies with operations in or ties to the United States are subject to pre-trial discovery rules that often require retention, processing, disclosure and transfers of personal information in connection with U.S. litigation. Recent amendments to the Federal Rules of Civil Procedure have emphasized that these requirements extend to electronically stored information. For multinationals with an EU presence, compliance with U.S. discovery demands poses challenges in light of EU ob-

[1] Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, 00339/09/EN, WP 158. A copy of the Guidelines is available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp158_en.pdf.

 ISSN 1538-3423

ligations to protect personal data. The Working Party's Guidelines acknowledge this problem, and offer several measures for facilitating multinationals' compliance with U.S. discovery obligations while ensuring protection for personal data consistent with the EU's Data Protection Directive.[2] Significantly, the Guidelines demonstrate that conflicts between the U.S. and EU systems are not intractable; to the contrary, the Working Party recognizes U.S. discovery goals as legitimate and draws upon mechanisms in both legal systems to achieve a balanced approach to cross-border compliance in the civil litigation context.

The Guidelines begin with the important acknowledgment that the Data Protection Directive does not prohibit data transfers for U.S. litigation purposes. The Working Party recognizes that parties involved in litigation have a legitimate interest in accessing information that is necessary to make or defend a claim, but it is necessary to balance the truth-seeking function of investigations with the rights of the individual whose personal data is sought. The Guidelines are intended to reconcile these two sets of legal obligations.

In doing so, the Working Party engages in a balancing analysis that is not dissimilar to that used in U.S. litigation when parties claim that discovery requests intrude into personal matters. The Working Party thus suggests an approach that is consistent with electronic discovery best practices in the United States.

Concrete steps to ensure compliance with EU data protection requirements

Under the EU Working Party's approach, companies should consider the Guidelines during each phase of data processing for litigation purposes: retention, disclosure, onward transfer, and secondary use. The Guidelines provide relatively detailed guidance for multinationals. Measures to help ensure compliance with EU data protection requirements throughout the discovery process include:

- Providing clear, advance notice of litigation-related data processing through privacy policies, as well as timely notification of affected individuals in the event of actual litigation;
- Informing data subjects of their rights under EU and U.S. law, including data access and correction rights;
- Considering the grounds for legitimate processing of personal data for litigation purposes, including whether to obtain consent or to rely on the processing being necessary for the purposes of a legitimate interest pursued by the data controller, for which a balance of interests test should be applied, taking into account the relevance of the personal data to the litigation and consequences for the data subject;
- Applying to U.S. courts for protective orders that clarify EU data protection requirements, require measures to minimize information collection and dissemination, and specify procedures for safeguarding information security and confidentiality;
- Devising litigation-specific technical and organizational information security measures and controls over third-party service providers;
- Affording corporate data protection officers an active oversight role in the litigation and discovery process;
- Establishing procedures for reviewing data and culling non-responsive documents in the EU, prior to any international data transfers, and for redacting or anonymizing personal data to the extent possible;
- Adopting restrictive data retention policies consistent with U.S. and relevant EU law;
- Ensuring that any litigation data transfers are justified under EU data protection provisions or pursuant to a recognized mechanism such as the Safe Harbor, model contracts or binding corporate rules; and
- Considering use of the Hague Convention, although it should be noted that not all Member States have signed the Hague Convention or have signed with reservations (and the use of the Convention is optional and less expeditious than other options under U.S. law).

Analysis and explanation of the guidelines

Data Retention

The EU's Data Protection Directive provides that personal data shall be kept only for the period of time necessary for the purposes for which the data have been collected. As the Guidelines explain, data controllers[3] may not retain personal data for an indefinite time period where there is merely a remote possibility of litigation. Where, however, the data are relevant to pending or imminent litigation, retention is permitted until the conclusion of the proceedings and any appeal and, indeed, is even required in order to avoid sanctions for spoliation of evidence. Since U.S. discovery rules require production only of existing information, data controllers located in the European Union may avoid running afoul of U.S. law by adopting a clear records management policy that provides for restrictive data retention periods in accordance with documented, local EU requirements.

Reasonable litigation holds, or the preemptive storage of personal data for use in potential future litigation, may be justified only under Articles 7(a), (c) and (f) of the Data Protection Directive.[4] These provisions permit data processing where the data subject has unambiguously given his consent, where it is necessary for compliance with a legal obligation to which the data controller is subject, or where necessary for the purposes of the legitimate interests pursued by a data controller or third party to whom the data are disclosed, except where such interests are overridden by concern for data subjects' fundamental rights and freedoms.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[3] A data controller is the entity which alone or jointly with others determines the purposes and means of the processing of personal data and which carries on processing in the context of its establishment in the European Union or where not established in the European Union makes use of equipment situated in the European Union for the purposes of processing personal data other than for the purpose of transit through the European Union. 95/46/EC, art. 2(d).

[4] Id. art. 7(a), 7(c), 7(f).

  PVLR ISSN 1538-3423

Legitimacy of Processing

Any processing of personal data, including that for litigation purposes as part of the pre-trial discovery procedure, must meet a requirement of legitimacy under the Data Protection Directive. Grounds for legitimate processing include the consent of data subjects, the processing is necessary to comply with a legal obligation to which the data controller is subject, and the processing is necessary for the purposes of the legitimate interest of the data controller or of third parties to whom the data are disclosed.[5]

Consent

The Working Party concludes that, in the discovery context, consent is typically unlikely to provide an appropriate ground for processing. In most cases, data subjects, such as customers and employees, do not have control over a company's decision to do business in or relating to the United States, and therefore they cannot be considered to have freely consented to the processing of data in relation to U.S. litigation.

Under the Working Party's view, it also may well prove difficult for companies in individual cases to produce clear evidence that data subjects have received proper notification and have provided valid consent to processing. Companies are certainly encouraged to provide notice when they are able to do so, but valid consent implies that the data subject must have a real opportunity to withhold consent without suffering any penalty, or to withdraw it subsequently if he changes his mind. The Working Party, however, does recognize that there may be situations where the individual is aware of, or even involved in, the litigation process and consent can properly be relied upon as a ground for processing.

In circumstances where valid consent is not possible, companies will need to rely upon the rationale that either they are acting in compliance with an EU legal obligation or that they or pursuing a legitimate interest, in order to process personal data in relation to U.S. legal proceedings.

Compliance with a Legal Obligation

As for the legal obligation rationale, the Working Party states that, in general, an obligation imposed by a foreign (i.e., U.S.) legal statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate.[6]

The Working Party, however, does note that the laws of some individual Member States may recognize or impose legal obligations to comply with an order of a court in another jurisdiction seeking discovery. That is, there may exist a requirement under a Member State's law to comply with the U.S. discovery request, and the Working Party would recognize the Member State's legal obligation as a valid basis for processing data in the European Union.

In those Member States where there is no such obligation, however, the situation remains complex. For example, some Member States have filed reservations under the Hague Convention in effect declaring that discovery of any information is not allowed in relation to foreign legal proceedings. In such States, the ''legitimate interest'' justification, referred to below, may still provide a ground for the processing of personal data for pre-trial disclosure, but the ''legal obligation'' justification would not be available.[7]

Pursuit of a Legitimate Interest

From the U.S. perspective, the significant advance in the international comity dialogue involves the Working Party's discussion of what interests it may consider to be legitimate interests. Under the Guidelines, compliance with pre-trial discovery requirements may be found to be necessary for the purposes of a legitimate interest pursued by a data controller or by the third party to whom the data are disclosed, provided that data subjects' fundamental rights and freedoms are protected. As the Working Party observes, the aim of discovery is to achieve ''fairness'' in the proceedings and reach a ''just outcome'' by providing the parties with access to relevant information.[8] Thus, the ''interests of justice would be served by not unnecessarily limiting the ability of an organisation to act to promote or defend a legal right.''[9] This key recognition that the goals of the discovery process are worthy and legitimate represents a significant step toward cross-border cooperation in discovery matters.

To balance data subjects' rights against the parties' need for access to information, the Working Party proposes a case-by-case inquiry that takes into account proportionality, the relevance of the personal data in question, and any consequences of the processing for the data subject. The Working Party also emphasizes that personal data must be protected by adequate safeguards and data controllers must preserve data subjects' right to object to processing under Article 14 of the Data Protection Directive.[10] The Working Party comments that as a first step data controllers should limit disclosure, where possible, to anonymized data or at least pseudonymized data with a filtering of irrelevant data, possibly by a trusted third party in the European Union, leaving a much more limited set of personal data to be disclosed as a second step.[11]

Where sensitive personal data, for example health data, is at issue, further grounds for processing are necessary which could include under Article 8 of the Directive obtaining the explicit consent of the data subject or where the processing is necessary for the establishment, exercise or defense of legal claims. Special requirements may also apply to confidential or privileged information. Certain types of information may be protected by additional laws such as the e-Privacy Direc-

[5] *See id.* art. 7.

[6] Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, 00339/09/EN, WP 158, at 9.

[7] Article 23 of the Hague Convention provides that a contracting state may at the time of signature, ratification or accession declare that it will not execute letters of request issued for the purposes of obtaining pre-trial discovery of documents. A number of Member States, including France, Germany, Spain and the Netherlands, have filed reservations under Article 23.

[8] Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, 00339/09/EN, WP 158, at 9.

[9] *Id.*

[10] 95/46/EC, art. 14.

[11] Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, 00339/09/EN, WP 158, at 10.

tive.[12] Data controllers should exercise caution in such circumstances to ensure compliance with all relevant legal obligations, but the Guidelines do not indicate that there is anything about these concerns that could not be addressed by a well-crafted protective order issued by the U.S. court.

Proportionality

Under the Data Protection Directive, personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes, and not used for incompatible purposes. The personal data must also be adequate, relevant, and not excessive in relation to the purposes for which the data are collected and further processed.[13] The Guidelines note that the U.S. system also values proportionality and balancing the rights of the different interests. Throughout the discovery process, courts consider and weigh the need for the parties to obtain information, the interests of individuals whose personal or confidential information is at issue, and the relevance of the information to the litigation. Drawing upon this common ground, the Working Party suggests a cooperative approach that relies on mechanisms in both the European Union and the United States to resolve concerns about proportionality.

When responding to a discovery request, data controllers in the European Union should undertake a filtering exercise that involves identifying relevant information, isolating personal data, and evaluating whether that data can be redacted or anonymized. Filtering should be carried out in the European Union, in the Member State in which the personal data are found, prior to any cross-border data transfers to a jurisdiction outside the European Union. It may be appropriate to engage an independent, trusted third party in the European Union to determine the relevance of any personal data to the litigation.

The Working Party strongly encourages litigating parties to actively involve data protection officers from the beginning of the discovery process. Data controllers should also approach U.S. courts to explain EU data protection requirements and to request protective orders specifically tailored to facilitating compliance with data protection obligations.

Notice to Data Subjects

Notice of data processing is a central component of fairness under the Data Protection Directive. In the pretrial discovery context, the Working Party recommends ''advance, general notice of the possibility of personal data being processed for litigation.''[14] Once processing actually occurs for litigation purposes, companies should give further notice concerning the recipients of the data, the purposes for processing, the types of data involved, and the nature of data subjects' rights.

Where individuals' personal data are collected from third parties rather than from data subjects directly, data controllers should provide notice of the processing as soon as reasonably practicable. The Guidelines allow for an important, though narrow, exception to this rule where there is a substantial risk that such notification would compromise the ability of the litigating party to investigate the case properly or gather the necessary evidence. The exception should be applied restrictively and on a case by case basis, but there is not necessarily a conflict between the Working Party's approach and prudent U.S. discovery management practices.

Data Access and Correction Rights

The Guidelines make it clear that data subjects' right to access and correct their personal data (where it is inaccurate, incomplete or outdated) under the Data Protection Directive should be respected throughout the litigation process. Prior to any transfers, EU data controllers should ensure protection for this right. The Working Party also suggests using protective orders to extend this obligation to parties that receive personal information, so that data subjects may verify that the data transferred is not excessive.

Data Security and Controls Over External Service Providers

Throughout the litigation process, data controllers must take all reasonable technical and organizational measures to protect data from accidental or unlawful destruction or accidental loss and unauthorized disclosure or access. These measures should, however, be appropriately tailored to the purposes of the litigation and to the requirements of data security regulations in force in relevant Member States. The obligation to protect data security and to observe strict confidentiality rules should also extend to the courts themselves, to law firms participating in the litigation, and to litigation support services as well as to any experts involved in collecting or reviewing the data.

Data controllers are responsible for ensuring that external service providers, for example expert witnesses, comply with data protection requirements, including those related to proportionality, lawfulness of processing, and data retention periods. The data controller must also periodically verify compliance by external providers with the provisions of the Directive. Where the service provider is acting as a data processor, then the data controller will also need to enter into a data processing agreement with the service provider under which the service provider agrees to act only on the instructions of the data controller and to implement appropriate technical and organizational measures.

From the U.S. perspective, numerous federal and state data security regimes (including, most recently, highly detailed Massachusetts regulations), require that data processors have comprehensive information security programs, process data only as directed, and confirm compliance with written privacy agreements. Accordingly, the U.S. and EU approaches to controls over external service providers appear to be harmonious—with the U.S. approach possibly being even more stringent.

Cross-Border Data Transfers

The Guidelines, however, do not in any way diminish requirements that companies seeking to transfer personal data from the European Union to the United States must rely on a specific compliance mechanism for doing so, such as the Safe Harbor scheme, model

[12] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[13] 95/46/EC, art. 6.

[14] Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, 00339/09/EN, WP 158, at 11.

  PVLR ISSN 1538-3423

contracts, or a set of approved binding corporate rules. The Guidelines clarify that these established means for international data transfers might also legitimize transfers for litigation purposes.

Where the transfer of personal data for litigation purposes is likely to be a single transfer of all relevant information, there would be a possible ground for the transfer under Article 26(1)(d) of the Data Protection Directive where the transfer is necessary or legally required for the ''establishment, exercise or defence of legal claims.''[15] Where a significant amount of data is to be transferred, however, the use of binding corporate rules or the Safe Harbor should be considered. According to the Working Party, Article 26(1)(d) cannot be used to justify the transfer of all employee files to a group's parent company on the grounds that legal proceedings might be brought one day in the U.S. courts, but surely few companies would rely upon such a slender rationale.[16]

Finally, the Working Party urges reliance on the Hague Convention, where possible, to facilitate litigation-related data transfers. The Working Party recognizes that compliance with a request under the Hague Convention would provide a formal basis for a transfer of personal data, although it also recognizes that not all Member States have signed the Hague Convention and some have signed with reservations. Moreover, from the U.S. perspective, the Hague Convention is merely optional and it is fraught with a level of technical and temporal complexity that normally makes it an option only of last resort.

Conclusion and guidance for multinationals

The Guidelines acknowledge that they are an initial consideration of the issues, and an invitation to public consultation between interested parties, courts, and others. While the Working Party ultimately calls for a more formal government accord, the Guidelines set out practical ways for multinational companies to attempt to reconcile the litigation processes in the U.S., and other countries outside the EU, with the data protection requirements of the EU's Data Protection Directive as implemented by Member States. It, however, should be noted that any conclusions of the Working Party will ultimately be subject to Member State data protection requirements and the approach taken by national data protection authorities.

Consistent with the Guidelines, multinationals should strive to provide notice to individuals whose information is or may be used in connection with U.S. litigation. To do so, companies should revise their privacy policies and other data protection documents and statements to provide clear, advance notice of the prospect that the company will be involved in U.S. or other foreign litigation, and of the fact that U.S. or other laws require the company to collect, retain, process, and transfer individuals' personal data. Company policies should inform data subjects of their rights under EU and U.S. law, including data access rights. Companies should also adopt specific procedures for providing notice to affected individuals in the event of actual litigation. This notice should include information on the data recipients, the methods and purposes for processing, and the categories of data involved.

Companies may also wish to advise their data subjects of their ability to seek relief from the U.S. courts if they consider their personal interests to be unduly burdened by a discovery order in light of the issues at stake. Moreover, data subjects should also be informed that they may seek to involve their national Data Protection Authority in the U.S. discovery process, and to request that the Member State's Data Protection Authority intervene in the U.S. litigation for purposes of asserting their legal interests. Indeed, in several circumstances, EU Member States (and other countries) have intervened in U.S. legal proceedings to assert that certain data is privileged or protected from disclosure by foreign law, and there is an established body of international comity law addressing such considerations.

Consideration should also be given to grounds for the legitimate processing of personal data for litigation purposes, including whether to obtain consent or to rely on the processing being necessary for the purposes of a legitimate interest pursued by the data controller, for which a balance of interests test should be applied taking into account the relevance of the personal data to the litigation and consequences for the data subject. Companies should also consider adopting data retention policies that are appropriately restrictive in light of U.S. state data disposal requirements and local EU law.

To promote compliance with EU data protection obligations, multinationals involved in U.S. litigation are often well-advised to apply to the court for a protective order that sets forth EU data protection requirements and requires procedures to narrow the scope of information disclosure, and to protect the security and confidentiality of any data exchanged between the parties. Companies should also:

- devise technical and organizational security measures and procedures specifically tailored to the litigation process and which are consistent with requirements in applicable Member States, and
- establish strict controls over third-party service providers, including entering into data processing agreements and having contractual rights to verify compliance.

Special attention should be paid to sensitive personal data or to confidential or privileged information, which may be subject to additional requirements. Corporate data protection officers should be charged with specific duties relevant to litigation and should take an active oversight role in the discovery process.

Multinationals must also establish procedures for conducting an initial review of documents in the European Union, and for culling non-responsive or unnecessary documents prior to any international data transfers. Personal data should be redacted or anonymized to the extent possible. Where suitable, companies should engage an independent, trusted third party in the European Union to evaluate the relevance of personal data to the litigation.

Finally, before exporting any data, companies should ensure that the transfer is justified either under specific EU provisions or pursuant to a mechanism such as the Safe Harbor or binding corporate rules.

[15] 95/46/EC, art. 26(1)(d).

[16] Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, 00339/09/EN, WP 158, at 13.