PRETRIAL PRACTICE & DISCOVERY

Section of Litigation

Summer 2018, Vol. 26 No. 3

Cross-Border E-Discovery Meets Data Privacy Protection in the European Union

By Mark Austrian and Christopher Loeffler – June 26, 2018

A company's obligation to produce extensive electronically stored information (ESI) in civil and criminal litigation and government investigations commenced in the United States transcends geographical borders. However, the European Union and European Economic Area (collectively, EU) severely restrict the transfer of broadly defined personal data (EU personal data) to the United States. This often conflicts with the company's obligations to produce ESI to opposing counsel in the United States. The U.S. Supreme Court ruled in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522, 543–44 (1987), that foreign data-protection laws cannot be used to limit the scope of U.S. discovery. Rather, courts would be required to weigh the needs of the requesting party and the impact of U.S. discovery in foreign countries. *See*David Kessler et al., *The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States*, 17 Sedona Conf. J. 595–611 (Nov. 2016).

On May 25, 2018, the EU's General Data Protection Regulation (GDPR) goes into effect, governing the search, preservation, collection, review, and processing of EU personal data in the EU and the forwarding (onward transfer) of such data out of the EU. These privacy restrictions apply to EU personal data of individuals located in the EU if the company that initially collected or processed the data has facilities in the EU, does business in the EU, or monitors the behavior of EU individuals. The GDPR provides for a data controller with responsibility and liability for ensuring and demonstrating that appropriate data-protection safeguards have been instituted, including with respect to an onward transfer of EU personal data to a third party. Violation of these regulations can result in significant fines (the greater of 4 percent of annual global revenue or €20 million).

This article focuses on the procedures that companies should consider before the onward transfer of EU personal data to their outside counsel, opposing counsel, or a governmental agency in the United States. A more complete and authoritative analysis of cross-border e-discovery is contained in publications by the Sedona Conference and the EU Article 29 Working Party (WP), which will become the European Data Protection Board under the GDPR. Pertinent Sedona Conference publications include *International Principles on Discovery, Disclosure & Data*

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

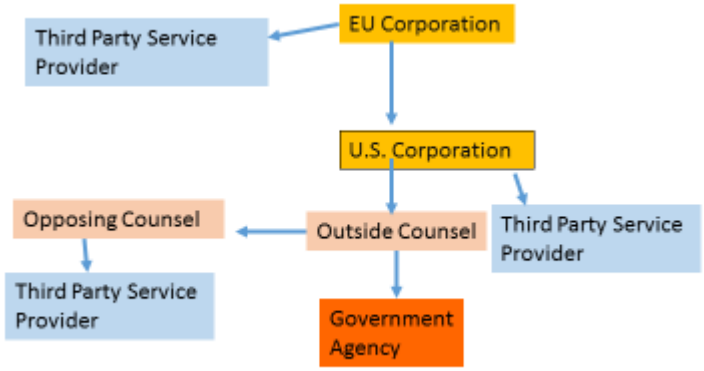
PRETRIAL PRACTICE & DISCOVERY

Summer 2018, Vol. 26 No. 3

Protection in Civil Litigation (transitional ed. Jan. 2017) (*International Litigation Principles*); and *Practical In-House Approaches for Cross-Border Discovery & Data Protection* (public cmt. ver. June 2017) (*GDPR Practical Approaches*). Pertinent WP publications include *Working Document 1/2009 on Pre-Trial Discovery for Cross-Border Civil Litigation*,0039/09/EN 158 (adopted Feb. 11, 2009) (WP 158); and 0018/EN 262 (adopted Feb. 8, 2018) (WP 262).

Overview of Onward Transfers

The parties that need to be considered in this onward transfer of EU personal data to the United States in litigation and investigatory proceedings are as follows:



The processing of EU personal data incorporates many of the procedures described by the Electronic Discovery Reference Model, which conceptualizes the e-discovery process from identification to presentation. However, EU processing is much broader than simply converting ESI from one format to another and requires that the data be processed fairly and transparently; collected only for specified, explicit, and legitimate purposes; limited to what is necessary in relation to the transfer's purpose; accurate and up-to-date; and kept no longer than necessary.

It is not surprising that there is great potential for the privacy restrictions of the GDPR and the comparatively expansive scope of discovery in the United States to conflict with each other. The Sedona Conference's *International Litigation Principles* envisions a three-stage approach to avoid or minimize conflicts between U.S. discovery obligations and the GDPR: (1) a stipulation or protective order to extend special protections to EU personal data, (2) phased discovery to

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

permit time to implement further data-protection processes, and (3) a legitimization plan to maximize compliance with the GDPR and U.S. discovery obligations.

Mechanisms for Onward Transfers

In addition to mutual legal-assistance treaties (e.g., the Hague Convention), the GDPR provides five mechanisms to assist with the onward transfer of ESI: transfers to a country that has been deemed adequate, consent of the data subject, the Privacy Shield (for transfers to the United States), binding corporate regulations (BCR), and standard contractual clauses (SCCs). For a comparison of these approaches, see Katia Bloom & K Royal, *Transferring Personal Data out of the European Union: Which Export Solution Best Fits Your Needs?* ACC Docket (June 2015).

EU personal data cannot be transferred outside of the EU unless a country has "adequate" data-protection laws. GDPR art. 45. There are exceptions or "derogations" in GDPR article 49, and WP 158 and 262 permit processing if necessary for the prosecution or defense of legal claims. However, the recently issued WP 262 only states, in section 5, that "data transfers for the purpose of formal pre-trial discovery in civil litigation *may* fall under this derogation" (emphasis added). Thus, individual member states must enact local laws permitting this transfer. Some member countries only apply this exception to trial proceedings and not pretrial proceedings. Others, such as France, have enacted blocking statutes preventing this transfer completely.

Consent of the data subject to U.S. discovery is often a difficult issue. Article 7 of the GDPR details the various conditions involved in the topic of consent.

The Privacy Shield, prepared by the U.S. Department of Commerce (DOC) in cooperation with the EU, is analogous to a safe harbor and consists of 23 Privacy Shield Principles and binding arbitration. For self-certification compliance with the DOC, the party must conduct a self-assessment, issue a commitment to cooperate with EU data-protection authorities, and provide public notice.

BCRs allow members of a corporate group committed to a binding and approved set of data-protection rules to transfer personal data within their organization (including from inside the EU to outside of it). *See Working Document Setting Up a Table with the Elements and Principles to Be Found in Binding Corporate Rules*, 17/EN WP 256 (adopted Nov. 29, 2017).

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Summer 2018, Vol. 26 No. 3

A written contract with SCCs must be in place for a transfer of EU personal data from an EU controller to a U.S. controller but is not required when the data is then transferred from the U.S. controller to a third party such as a service provider or law firm. The U.S. controller would be responsible for ensuring that in a third-party transfer, the proper confidentiality and security protections are in place, followed, and verified.

The goal of responding to U.S. discovery requests and processing EU personal data is to protect privacy by minimizing the amount of data that must be processed, transferred, and produced. Thus, where possible, companies should consider processing EU personal data in the jurisdiction where the data is located, using many of the same e-discovery filtering techniques as applied in the United States. *See GDPR Practical Approaches*, *supra*, at 17–19, 32–33. Additional privacy safeguards include producing data in a more anonymized, redacted, aggregated, or pseudonymized form with individual identifiers other than the data subject's name. *See* WP 152; *International Litigation Principles*, *supra*, at 14–15.

Onward Transfers to Outside Counsel

The U.S. controller will want to onward transfer EU personal data to its outside litigation counsel. Outside litigation counsel could receive the EU personal data by subjecting itself to the confidentiality and security requirements of the U.S. controller, entering into preapproved model contract clauses in either a separate service contract or an engagement letter with provisions contained in the SCC, or qualifying with the Privacy Shield.

Law firms and third-party service providers already have stated and publicly disclosed compliance with the Privacy Shield Principles, and the Federal Trade Commission has jurisdiction over their compliance.

Onward Transfers to Opposing Counsel

A significantly more difficult problem relates to the onward transfer of EU personal data to opposing counsel in civil and criminal litigation. The most effective solution to this problem is to negotiate limitations on the production of such data through a Federal Rule of Civil Procedure 26(f) conference and application of the limitations of e-discovery found in Federal Rule of Civil Procedure 26(b)(1) and related case law. If this fails, where there is a controller-to-controller contract, section II(b) of the SCC permits the U.S. controller, "the data importer," to transfer EU personal data to a third party, including an opposing counsel, as long as the U.S. controller implements and monitors the required confidentiality and privacy restrictions. *See* Commission

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Summer 2018, Vol. 26 No. 3

Decision 2004/915/EC of 27 December 2004, annex set II, § II(b). The outside law firm, presumably with the approval of the U.S. controller, could also agree to the onward transfer of EU personal data to opposing counsel, as long as opposing counsel agree to implement provisions protecting the confidentiality and security of the EU personal data. Because the U.S. controller retains liability for assuring these protections, opposing counsel will have to agree to some supervision by the U.S. controller. As a practical matter, opposing counsel will rarely agree to enter into such an agreement due to the required supervision of a U.S. controller or to go through the time and expense of qualifying for the Privacy Shield.

A more acceptable solution may be to enter into an agreed-upon protective order providing the basic privacy protections afforded by the GDPR. This procedure is not set out in the GDPR or in any of the WP's working papers. However, an appropriate protective order would signify to EU data-protection authorities that the requirements of the GDPR are respected and that these requirements will be enforced by the U.S. courts. *See International Litigation Principles*, *supra*, app. C. If the parties cannot agree, the court can enter its own protective order. The company may also find it beneficial to show good-faith compliance with the GDPR by documenting its processes in a legitimization plan. *Id.*app. D.

Onward Transfers for Government Investigations

The onward transfer of EU personal data is entirely different where such data must be produced for a U.S. government investigation. While a company can use the same techniques for limiting and transferring EU personal data to the United States as in civil litigation, there is, in general, no ongoing court supervision to balance the competing interests of the parties. Furthermore, the government believes that its interests in protecting the country's economies and the health, safety, and welfare of its citizens are fundamentally different than those of private parties in civil litigation. Thus, the U.S. government will not enter onward transfer restrictions as provided by the GDPR. *See generally*Sedona Conf., International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigation: Principles, Commentary & Best Practices (public cmt. ver. May 2017). The best guidance in this instance, as in many others, is for the U.S. company to adhere to the principles put forth by the Sedona Conference's *International Litigation Principles* and be prepared to develop a framework and protocol for disclosure of EU personal data, to confer with the government investigators to explain the conflicting requirements, and to negotiate a reasonable resolution.

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

PRETRIAL PRACTICE & DISCOVERY

Section of Litigation

Summer 2018, Vol. 26 No. 3

Conclusion

The takeaway from all of this is that U.S. counsel, for both the plaintiff and the defendant in civil litigation and in responding to government requests, must carefully evaluate GDPR requirements and coordinate their efforts with their clients as well as GDPR experts before the onward transfer of EU personal data to the United States.

Mark Austrian is a partner at Kelley Drye & Warren LLP in Washington, D.C., and is an adjunct professor at the American University Washington College of Law. Christopher Loeffler is a special counsel with the firm; he is also an information privacy professional for the United States and Europe, certified by the International Association of Privacy Professionals.

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.