DATA AND DISCOVERY STRATEGIES CLIENT ALERT

JANUARY 2018

SHOOK HARDY & BACON

WHEN *AEROSPATIALE* MEETS THE GDPR: CAN U.S. LITIGANTS EXPECT LIMITS ON DISCOVERY OF EU PERSONAL DATA?

In less than four months, on May 25, 2018, the European Union's new data protection regulation becomes enforceable. As we previously outlined, the General Data Protection Regulation (GDPR) creates a uniform law for all organizations that operate in the EU (including those that only offer goods and services in the Union) and expands EU residents' rights to privacy and data protection. The GDPR will affect whether and how organizations can store and transfer personal data for purposes relating to potential or pending civil litigation in the United States. The implications of GDPR enforcement on organizations' U.S. litigation practices are significant given the breadth of affected data and the significant consequences for violations. Under the GDPR, "personal data" is broadly defined to include information from which an individual can be identified, directly or indirectly.2 And violations carry the risk of significant fines and citizen suits.

In this client alert, we examine whether the steeper consequences for violations under the GDPR—as compared to its 1990s predecessor, the Data Protection Directive—will change the analysis of U.S. federal courts considering limits on federal discovery obligations for personal data from the EU.

The GDPR's Effect on American Discovery

In the United States, an organization generally has a duty to preserve potentially discoverable information—including personal data—if litigation has begun or is anticipated. And typically, at least some of the preserved information will be produced to other parties in the litigation. Absent specific protection from the court, any such information is fair game for introduction into evidence at trial, at which point, it is generally considered a public record.

This analysis was prepared by Shook attorneys Ruth Anne French-Hodson and Jesse E. Weisshaar.[1]

Shook's Data and Discovery Strategies practice provides results that are creative, defensible and cost-effective. Discovery services include first-pass document review, privilege review, and production/logging, as well as preservation consultation, collections, and vendor selection and management. The group's focus also extends to records and information management – e.g., developing policies and procedures, and proposing strategies for defensible data disposition.

To learn more about Shook's Data and Discovery Strategies practice, please visit shb.com or contact:

Denise Talbert
dd 816.559.2057
dtalbert@shb.com

Mark Cowing
dd 816.559.2275
mcowing@shb.com

But the GDPR places limits on the ability of organizations to maintain, transfer or disclose personal data from the EU, especially for purposes—like litigation—that might be unforeseen when the data is collected.[3] To collect personal data, an organization must:

- Do so in a fair and transparent manner[4];
- Collect only data that is accurate, relevant and necessary for the purposes[5];
- Permit the data subject to exercise her right to access data, rectify errors, erase data and object.[6]

To justify both collection and transfer to the United States, an organization must also ensure that an enumerated ground for processing and transfer applies.[7] The European Commission has indicated that there is only one possible—and narrow—ground for collection and transfer of personal data for a civil legal action in a non-EU state[8]: they must be "necessary" for a legitimate interest pursued by the organization controlling the data.[9] These tasks can be justified only if such legitimate interest outweighs the interests and fundamental rights of the data subject(s).[10] In addition, organizations must ensure that individuals have access to their data, can correct errors, erase their data and object to its collection or transfer.[11] Further, to justify transfer of personal data to the United States, an organization must also show that the interest is not only legitimate but "compelling."[12] Additionally, any transfer pursuant to this provision must not be "repetitive," must "concern only a limited number of data subjects," and must ensure "suitable safeguards" to protect the personal data.[13] The European Commission has emphasized that the transfer exception is to be strictly interpreted, is the exception from the typical rules—not regular discovery practice—and requires notification to the supervisory authority and data subject(s).[14]

Applying these requirements is no easy feat when an organization is faced with, for example, a U.S. court order requiring the production of the custodial files—any number of which are likely to contain personal data—of an organization's EU employees. But organizations that fail to comply with the GDPR do so at their peril. For violations of the regulations related to transfer of personal data, a national supervisory authority may impose administrative fines up to €20 million (roughly 24.5 million U.S. dollars) or 4% of the organization's annual worldwide gross revenue, whichever is greater.[15] Independent analyses estimate that a violation of

the GDPR could result in fines that are 79 times higher than those available for similar violations under the EU's Data Protection Directive.[16]

Moreover, a non-compliant organization faces the risk of private enforcement. One of the major changes from the EU's Data Protection Directive to the GDPR is that EU residents are now allowed to sue to recover "material or non-material" damages resulting from data protection violations.[17] "This has the potential to subject U.S. companies to litigation in each of the 28 EU member states (where the same conduct may give rise to multiple proceedings in different forums as it impacts multiple member state residents), and where there are significant differences between and among member states' legal regimes."[18]

U.S. Consideration of Foreign Restrictions on Data Sharing

In the often-cited 1987 case of *Societie Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. S.D. Iowa*, the U.S. Supreme Court made clear that foreign statutes "do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute."[19] Instead, district courts determining whether to give effect to a foreign rule—such as those limits on the processing of personal data—are to apply "rules of comity," including weighing the interests of the respective nations.[20]

American courts have uniformly held that the United States has a substantial interest in efficient discovery under the Federal Rules.[21] U.S. courts have also recognized the interest that foreign nation-states have in data privacy.[22] But in considering what weight to give that interest, they have considered two indicators of how valued an interest is to a foreign country: (1) whether the foreign government has raised an objection to the specific discovery at issue,[23] and/or (2) whether the foreign government actually enforces the foreign rule for similar violations. As relates to the latter factor, federal courts have given considerable weight to whether the party resisting discovery is likely to face "hardship" as a result of its conflicting legal obligations.[24]

As part of the "hardship" analysis, federal courts have considered whether an organization faces "a real risk of prosecution" for complying with American discovery obligations.[25] Finding no or minimal hardship under the EU's Data Protection Directive, federal courts have cited the lack of evidence of actual prosecution or penalties from compliance with

U.S. discovery obligations based on the Directive's requirements.[26] In part because these courts found no real risk of enforcement, companies have generally been required to produce data from the EU in accordance with case-specific discovery protocols.[27] Indeed, we have not been able to identify any reported case where a party was permitted to fully withhold production of documents based on the EU's Data Protection Directive.[28]

Hardship Under the GDPR

Although the GDPR allows for the imposition of severe fines for violations, this, by itself, is unlikely to change the comity analysis of U.S. federal courts. As the cases applying *Aerospatiale* demonstrate, federal courts look not only at the possibility of fines but also to whether foreign rules are actually enforced. Because it is not clear at this stage how national regulators will enforce the GDPR, organizations operating in the EU and facing U.S. litigation are in a difficult spot.

Current signals of likelihood of enforcement under the GDPR are unclear. On the one hand, the British regulatory office has cautioned that it does not plan to approach enforcement under the revised regulatory scheme differently and noted that fines are not typically the best mechanism to ensure compliance.[29] On the other hand, the European Commission's recent filing of an amicus brief in a case pending before the U.S. Supreme Court implicating EU residents' data protection interests suggests that foreign authorities will be more active in defending the GDPR's enhanced rights in U.S. courts.[30] As the EC affirms, "There is [] no doubt that the European Union is actively regulating the issues at this case's heart, including how data stored in the European Union must be protected, and when such data may be transmitted abroad."[31] It may well be that the United Kingdom is an anomaly, and EU governments will prove willing to follow the EC's lead by explicitly objecting—via formal briefs, in-court appearances or letters to or on behalf of the parties—when discovery transfers would violate the GDPR and/or will prove more willing to impose the significant fines permitted under the GDPR than has been the practice under the Data Protection Directive.

But with or without such action by EU government actors, an organization has an entirely new argument as to likely "hardship" when U.S. discovery obligations conflict with requirements under the GDPR: the possibility of citizen suits. The likelihood, volume and results of such citizen suits are as unpredictable as each EU country's enforcement

discretion (if not more so). But U.S. courts may be more inclined to credit something with which they have direct familiarity. And the fact that such citizen suits are now available under the new regulatory regime may—by itself or in combination with the increased fines—prove sufficient evidence of how seriously the EU values data protection and privacy.

Conclusion

Organizations facing conflicting obligations regarding personal data under U.S. civil litigation requirements and EU data protection principles will be provided no immediate resolution to the conflict by the EU's enforcement of the GDPR come May. But such organizations will be armed with new ammunition to argue "hardship" under the *Aerospatiale* standard. And if the GDPR's threat of enforcement via fines imposed by national authorities or via citizen suits proves real, then American courts may be forced to place new limits on discovery that reaches personal data from the EU.

1. The authors would like to give special thanks to those at the firm who have taken the time to review and comment on the article. Camila Tobón, head of Shook's International Data Privacy Task Force, provided invaluable insight into the workings of the GDPR. We would like to especially thank our mentor, Mark Cowing, for his encouragement of our interest in the impact of foreign legal regimes on American discovery and his assistance in thinking through the real-world impacts for our clients.

2. Council of the European Union Interinstitutional File 5419/16, General Data Protection Regulation, ("GDPR"), Arts. 4(1), 9, 10, available at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf. Individuals who are identified or identifiable are called "data subjects" in the GDPR. GDPR, Arts. 4(1). Even stricter requirements are imposed for access to or use of "sensitive personal data," which include data on race, ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, mental or physical health, sex life, and prior criminal convictions or civil judgments. *Id*. at Art. 8.
3. In its December 2017 amicus submission to the U.S. Supreme Court in *U.S. v. Microsoft*, the European Commission made clear that collection and transfer for U.S. discovery obligations must comply with the GDPR and that "a foreign court order does not, as such, make a transfer lawful under the GDPR." Brief of the European Commission on behalf of the European Union as *Amicus Curiae* Supporting Neither Party at 8, 14, *U.S. v. Microsoft Corp.*, No. 17-2 (S. Ct. Dec. 13, 2017) (hereinafter, EC amicus brief).
4. GDPR, Article 5(1)(a), (b).
5. GDPR,Article 5(1)(c), (d), (f).
6. GDPR,Articles 15, 16, 17, 21.
7. GDPR,Article 6(1).
8. EC amicus brief at 10.
9. GDPR,Article 49(1); Article 6(1)(f).
10. GDPR,Article 6(1)(f).

11. GDPR,Articles 15-17, 21.

12. GDPR,Article 49(1). The GDPR does not provide any guidance on what might constitute a "compelling" legitimate interest. But the recent EC amicus brief noted that a legitimate interest that meets this requirement could be an interest "in not being subject to legal action in a non-EU state." EC amicus brief at 15. In that case, Microsoft faces a civil contempt finding for non-compliance with the U.S. government's warrant for electronic mail messages stored in Ireland. Brief of Petitioner at 7, *United States v. Microsoft Corp.*, No. 17-2 (S. Ct. Dec. 6, 2017).

13. GDPR,Article 49(1).

14. Because the EC has determined that the United States does not provide an adequate level of data protection, transfers can normally occur only through the consent of the data subject, EU-U.S. Privacy Shield framework by participating companies, binding corporate rules or model contracts. Article 45, 46; *see also* Press Release, European Commission, European Commission – Fact Sheet: EU-U.S. Privacy Shield: Frequently Asked Questions (July 12, 2016), available at http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm. If any of these are available, they are the preferred justification for transfer to avoid resort to the narrow exception described above.

15. GDPR, Article 83(5). The supervisory authority will have discretion to craft a fine based on multiple mitigating and aggravating factors including the nature and gravity of the infringement (including how many data subjects were affected); whether the infringement was negligent or intentional; if and when actions were taken to mitigate the damages; and if the entity cooperated with the authorities. Article 83(2). *See also* Matthew Oliver & Steven Llanes, *Answers to Critical Questions about Enforcement of the EU's New GDPR Privacy Law*, Corp. Counsel (May 24, 2017 at 12:00AM), http://www.corpcounsel.com/id=1202787291207/Answers-to-Critical-Questions-About-Enforcement-of-the-EUs-New-GDPR-Privacy-Law?slreturn=20170828172704 (indicating that "higher tier-violations" include "failing to obtain the necessary level of customer consent to process data, failing to permit data subjects to exercise their rights including as to data erasure and portability, and transferring personal data outside the EU without appropriate safeguards.").

16. Press Release, NCC Group, Last year's ICO fines would soar to £69 million post-GDPR (Apr. 28, 2017), available at https://www.nccgroup.trust/us/about-us/newsroom-and-events/press-releases/2017/april/last-years-ico-fines-would-soar-to-69-million-post-gdpr/.

17. GDPR, Article 82; *see also* Shook, Hardy & Bacon Data and Discovery Strategies Client Alert, Ruth Anne French-Hodson and Jesse Weisshaar, EU Data Protection Reforms on the Horizon – Impact on U.S. Discovery Obligations (May 2016), available at https://www.shb.com/results/insights/datadiscoveryalert/eu-data-protection-reforms-on-the-horizon.

18. Oliver & Llanes, *Answers to Critical Questions about Enforcement of the EU's New GDPR Privacy Law*, available at http://www.corpcounsel.com/id=1202787291207/Answers-to-Critical-Questions-About-Enforcement-of-the-EUs-New-GDPR-Privacy-Law?slreturn=20170828172704.

19. *Societie Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. S.D. Iowa*, 482 U.S. 522, 544 n.29 (1987).

20. *Aerospatiale*, 482 U.S. at 544 n.28. See also Restatement (Third) of Foreign Relations Law of the United States § 442 (requiring consideration of "the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located").

21. *St. Jude Medical S.C., Inc. v. Janssen-Counotte*, 104 F. Supp. 3d 1150, 1162 (D. Or. 2015) (compiling cases and noting the "substantial interest in vindicating the rights of American plaintiffs" and the "overriding interest in the just, speedy, and inexpensive determination of litigation in its courts" (internal quotations and alterations omitted)).

22. *Laydon v. Mizuho Bank, Ltd.*, 183 F. Supp. 3d 409, 423 (S.D.N.Y. 2016) (noting that "courts have repeatedly held that European nations bound by the EU [Data Protection] Directive have an interest in protecting the privacy rights of their citizens" (internal alteration and quotation omitted)); *In re Xarelto (Rivaroxaban) Prods. Liab. Litig.*, 2016 WL 3923873 (E.D. La. July 20, 2016) (finding that "Germany has a weighty national interest in protecting the personal data of German citizens in their capacity as employees").

23. *Laydon*, 183 F. Supp. 3d at 424 (in considering what weight to give the United Kingdom's interest in data privacy, the court looked "to whether the foreign government has raised an objection to the discovery sought").

24. *See, e.g., Linde v. Arab Bank PLC*, 706 F.3d 92, 110 (2d Cir. 2013) ("Cases from our Circuit counsel that, when deciding whether to impose sanctions, a district court should also examine the hardship of the party facing conflicting legal obligations . . . ."); *In re Auto. Refinishing Paint Antitrust Litig.*, 358 F.3d 288, 304 (3d Cir. 2004) (noting that the party resisting discovery had not "identified a single instance where a German national has been prosecuted, penalized, or sanctioned under German law for complying with discovery orders from a United States judicial or administrative proceeding pursuant to the Federal Rules").

25. *Linde*, 706 F.3d at 110.

26. *St. Jude Med. S.C., Inc. v. Janssen-Counotte*, 104 F. Supp. 3d 1150, 1164 n.9 (D. Or. 2015) (Germany); *Laydon v. Mizuho Bank, Ltd.*, 183 F. Supp. 3d 409, 425 (S.D.N.Y. 2016) (United Kingdom); *Devon Robotics v. DeViedma*, 2010 WL 3985877 (E.D. Pa. Oct. 7, 2010) (Italy); *In re Xarelto (Rivaroxaban) Prods. Liab. Litig.*, 2016 WL 3923873 (E.D. La. July 20, 2016) (Germany); *In re Activision Blizzard, Inc. Stockholder Litig.*, 86 A.3d 531 (Del. Ch. 2014) (France).

27. *Id.*

28. *St. Jude*, 104 F. Supp. 3d at 1168 (holding that there was no blanket protection to the personal data sought under the German Data Privacy statute but allowing individual challenges based on comity be made to the discovery special master and requiring all personal data be produced as attorneys' eyes only and, if necessary, filed under seal); *Laydon*, 183 F. Supp. 3d at 425 (denying motion for protective order based, in part, on the British Data Protection statute); *In re Xarelto*, 2016 WL 3923873 at *19-20 (requiring in camera review of personnel files before determining motion to compel and requesting that the defendant seek the consent of two employees for production of their personnel files given the importance of the data); Devon Robotics, 2010 WL 3985877 at *6 (denying motion for protective order based on Italian Data Protection code); *In re Activision Blizzard, Inc. Stockholder Litig.*, 86 A.3d at 550-551 (granting motion to compel and concluding that the discovery process could be modified to accommodate French interests in data protection).

29. Matt Burgess, *What is GDPR? WIRED explains what you need to know*, WIRED (JAN. 12, 2018), http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018. Despite the Brexit process, the United Kingdom plans to cover the same provisions and protections through a new Data Protection Bill. *Id.*

30. *See generally* EC amicus brief at 3 (stating its "significant interests" in the case including "ensuring that the Court proceeds based on a correct understanding of EU law").

31. *Id.* at 5-6.