DATA AND DISCOVERY STRATEGIES CLIENT ALERT

MAY 2016

SHOOK HARDY & BACON

EU DATA PROTECTION REFORMS ON THE HORIZON – IMPACT ON U.S. DISCOVERY OBLIGATIONS

With the adoption last month of the General Data Protection Regulation (GDPR), the European Union is set to impose landmark data protection measures. The GDPR builds on the EU's previous directive governing personal data by creating a uniform data protection law for all companies that operate in the EU; strengthening the rights of EU citizens; and imposing stronger penalties for violation of such rights. The GDPR will affect current practices—including those relating to data preservation and collection for U.S. litigation purposes—of all companies that operate or market in the EU. Affected companies will need to ensure they are in compliance when enforcement begins in mid-2018.

Regulatory Backdrop

Since the mid-1990s, when the European Commission adopted its "Data Protective Directive," Europe has taken an approach that advances two main objectives: (1) providing individuals with control of their "personal data" in certain circumstances; and (2) restricting the use and transfer of "personal data" collected by organizations or individuals.[1] But in the 20 years since the passage of the Directive, rapid technological advances have transformed the ways in which the global community shares and uses personal data. In response to the ubiquitous use and easy transfer of personal data, the European Commission in 2012 proposed revising the Directive.[2] Revision efforts culminated in April 2016 with final approval of the GDPR.[3]

Major Provisions in the GDPR

The major provisions of the GDPR revolve around two key goals: simplification of the regulatory environment for businesses and strengthened individual rights. The GDPR accomplishes the first of these goals in multiple ways:

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

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 Stategies 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

Patrick Oot
dd 202.639.5645
oot@shb.com

- **Uniform law:** Because the new data protection initiatives have been adopted as a regulation, they will be implemented as one uniform EU law rather than relying on the current system of nation-by-nation implementing legislation.
- **Uniform application:** Under the existing regime, companies established outside the EU are not subject to standards as strict as those to which EU companies are held. The GDPR will apply the same rules to all organizations operating in the EU, regardless of their origin.[4]
- **One-stop shop for regulation:** Under the existing regime, if a company has locations in multiple EU countries, it has to comply with country-specific rules and answer to national authorities in *each* location. The GDPR will allow a company to answer only to the national authority in the EU country where its headquarters is located.[5]
- **Streamlined international transfer of data:** The GDPR will streamline data transfer by simplifying the approval process for "binding corporate rules."[6] Binding corporate rules are used to ensure that intra-organizational transfers of personal data to non-EU countries—regardless of their data protection regimes—meet EU guidelines.[7] These binding rules must include "all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data."[8]
- **Streamlining red tape:** Companies will not have to produce impact assessments for all processing activities as they must under the current Directive.[9] But they will have to provide more information in notices to citizens about their data processing activities.

While the procedural and jurisdictional features of the GDPR are focused on uniformity and certainty, the substance of the GDPR expands citizens' rights. As with the existing Directive, the first principle guiding the GDPR is that protection of personal data is a fundamental right, and this principle is evidenced in an increased focus on individuals' rights to their data.[10] As asserted by Germany's Jan Philipp Albrecht, the Member of the European Parliament who championed the legislation, "Citizens will be able to decide for themselves which personal information they want to share."[11]

- **Strengthened right to be forgotten:** If an individual no longer wants her data "processed"—a defined term that includes merely storing or organizing[12]—and a company has no legitimate reason to keep the data, the company will be required to delete the data.[13]
- **Consent must be explicit:** When consent is required for processing or transferring data, individuals must receive clear and understandable information and provide "clear affirmative" consent.[14]
- **Special protection for children:** Additional protections will be provided for processing of personal data of children. For example, communications addressed to children must be in clear, plain language that *a child* could understand.[15] Additionally, a parent or guardian must give permission for processing personal data of a child under sixteen-years-old.[16]

Compliance Measures

The GDPR also includes provisions addressing the how and the why of compliance.

- **Guiding principles:** Two new principles should guide the development of data protection measures at every stage: (1) **Privacy by design:** Data protection safeguards should be part of product and process design from the very beginning of development, and (2) **Privacy by default:** The default for settings should be privacy protection.[17]
- **Data protection officers:** Companies must appoint an independent data protection officer if: (1) they systematically and regularly monitor EU citizens "on a large scale"; or (2) their core activities involve "large scale" processing of special categories of data[18] or data related to criminal convictions and offenses.[19] The data protection officer must have "expert knowledge of data protection law and practices" and will help monitor internal compliance.[20]
- **Stronger sanctions:** Depending on which provision is violated, the national supervisory authority may impose administrative fines up to €20 million or 4 percent of total annual worldwide gross revenue, whichever is greater, for GDPR violations.[21] The supervisory authority will have discretion to craft a fine based on multiple miti-

gating 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.[22]

- **Private right of action:** Any person who is damaged as a result of infringement of the GDPR will be able to bring suit in her national courts for compensation for the "material or non-material" damages suffered.[23] The GDPR requires joint and several liability if multiple entities are determined to bear responsibility.[24]

Global Impact of the GDPR

The changes resulting from the GDPR will be myriad, and companies around the world should be prepared for its impact. In particular, companies with global operations should be prepared for the EU's "longer arm" of data privacy protection, for a revision of processes for obtaining consent, and for how these and other aspects of the GDPR will affect discovery in U.S. litigation.

Application to All Companies That Market to EU Consumers

The GDPR will expand the reach of European data privacy laws from EU-based companies to all companies that market to EU citizens.[25] In this way, the GDPR serves a consumer protection role—safeguarding the rights of EU citizens—and is not just about setting regional norms of data privacy. With this expanded jurisdiction, companies outside the EU that market in the region will have the biggest adjustment to make with the implementation of the GDPR because the whole regime—and not just the new provisions—will be an added challenge of doing business in the EU. Such companies will need to consider how the express provisions of the GDPR affect its practices and policies, including those that relate to processing for U.S. litigation purposes.

Data Privacy Under GDRP vs. Discovery in U.S. Litigation

Companies that operate in the U.S. and the EU are likely already familiar with the competing demands on data in the two different regions. In the United States, federal and many state courts require potentially relevant information—including personal data—to be preserved if litigation has

begun or is foreseeable, and at least some of the preserved information may eventually be produced to other parties. But in the EU, both the existing Directive and the to-be-implemented GDPR place limits on the ability of companies to maintain or transfer personal data, especially for purposes—like litigation—that might be unforeseen when the data are collected. The EU's and the United States' competing demands on data are not alleviated under the GDPR;[26] companies will continue to face obstacles as they strive to meet their data preservation and collection obligations under U.S. law.

- **Litigation Holds**

To comply with U.S. preservation obligations in the face of pending or anticipated litigation, companies generally issue "litigation holds" to preserve relevant data. The European Commission has previously indicated that companies may justify the use of litigation holds (without data subject consent) as processing that is "necessary" for a "legitimate interest." But the company must employ a "rule of proportionality" to ensure that only the essential records are maintained. This requires a careful look at what would actually be "objectively relevant" to any foreseeable litigation to determine if anonymized or redacted versions of the data can be maintained instead of the full records.[27] To avoid retaining personal data longer than necessary, companies should also be prepared to promptly release a litigation hold once the matter that precipitated the hold is resolved.[28] The GDPR maintains the "legitimate interest" justification and accompanying "rule of proportionality" as an alternative to consent for the preservation of personal data.[29]

While the GDPR increases individuals' control over use of their personal data, their rights are subject to exceptions that allow for use and transfer of personal data for litigation purposes. Specifically, if personal data are required "for the establishment, exercise or defence of legal claims," the data are not subject to an individual's rights of erasure or objection under the GDPR.[30] The GDPR does not provide any guidance as to whether U.S. litigation discovery obligations satisfy the "defence of legal claims" justification. But previous guidance on similar language in the current Directive suggests that this provision may provide an appropriate ground to justify retention in accordance with a litigation hold (without data subject consent).[31]

- **Collection and Production**

Data collected for U.S. litigation purposes are often transferred to counsel and/or data vendors for review in advance of production, and at least some data will be produced to opposing parties and, perhaps, used with expert witnesses, as evidence in court filings and/or as exhibits at trial. Personal data that are transferred for such purposes will have to meet both the requirements for preservation discussed above and additional requirements for transfer. Because the EU has determined that the U.S. laws do not provide an adequate level of protection to personal data, transfer to the United States for litigation purposes must generally be justified under one of the following grounds: (1) the recipient is subscribed to the new EU-U.S. Privacy Shield framework[32] (which replaced the previously invalidated Safe Harbour framework); (2) the recipient has entered into a contractual agreement for transfer that includes a "standard contractual clause" approved by the European Commission[33]; (3) the recipient is subject to binding corporate rules.34 Transfer of personal data without one of these safeguards in place can be based on the "defence of legal claims" justification only if transfer is "occasional," involves a "single transfer of all relevant information," and does not involve the transfer of "a significant amount of data."[35] Thus, it is likely that in most U.S.-litigation-related circumstances, transfer must be supported by one of the three mechanisms outlined above.[36]

Regardless of the justifications for preserving and/or transferring personal data of EU citizens for litigation purposes, companies must employ the two guiding principles of the GDPR—privacy by design and privacy by default—to develop their policies for handling the U.S. discovery demands. Additionally, for companies that are required to appoint independent data protection officers, these independent officers will monitor and determine whether the internal policies and actual practices related to preservation, collection and transfer comply with the GDPR.

- **Explicit Consent**

A company obliged to preserve and/or transfer personal data of EU citizens for U.S. litigation purposes might alternatively justify such data processing based on consent from the data subjects. But under the GDPR such consent must be *explicit*. Passive consent—such as failing to untick a box—or implicit consent through silence will no longer be acceptable.[37]

Rather companies will need to ensure that the consent they receive is based on an affirmative statement or clear affirmative action. The GDPR explains that such consent "could include ticking a box . . . or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data."[38]

Conclusion

The newly adopted GDPR reinforces the EU's commitment to protection of individuals' personal data by providing EU citizens with increased rights and imposing stronger penalties for violation of such rights. In today's global economy, in which personal data plays an integral role, compliance with the GDPR is likely to require significant changes in the data processing policies of companies across the globe. Affected companies are advised to begin assessing the GDPR's impact on their practices—particularly those relating to preservation and cross-border transfer of data for U.S. litigation purposes—without delay to ensure they are in compliance with the GDPR when implementation begins in 2018.

---

1 Under the Directive, "personal data" include any information relating to an identified or identifiable person. Council Directive 95/46/EC, 1995 O.J. (L281/31) ("Directive text"), at Art. 2(a). 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. "Personal data" under the GDPR is similarly defined. Council of the European Union Interinstitutional File 5419/16, General Data Protection Regulation, ("GDPR text"), at Arts. 4(1), 9, 10, available at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

2 GDPR text, at Recitals 5-11.

3 Publication of the GDPR in its official form in the EU's "Official Journal" is expected to occur in May 2016 or shortly thereafter. Twenty days after publication, the GDPR will have legal force, but the GDPR's provisions will not become enforceable until after a two-year grace period (*i.e.*, likely in May or June 2018).

4 GDPR text, at Recital 22.

5 *Id.* at Recital 124.

6 *See generally id.* at Article 47. For more information on binding corporate rules, see European Commission, Overview on Binding Corporate rules (last updated Mar. 23, 2016), available at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm.

7 GDPR text, at Recital 107, 110; Article 47.

8 *Id.* at Recital 110.

9 *Id.* at Recital 89.

10 *Id.* at Recitals 1, 2.

11 European Parliament Press Release, *Data protection reform – Parliament approves new rules fit for the digital era* (Apr. 14, 2016), available at http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era.

12 Processing is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR text, at Article 4(2).

13 *Id.* at Recital 63; Article 17.

14 *Id.* at Recital 32; Article 4(11).

15 *Id.* at Recital 58.

16 *Id.* at Article 8(1).

17 *Id.* at Article 25.

18 The special categories are defined as "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." *Id.* at Article 9(1).

19 *Id.* at Article 37.

20 *Id.* at Recital 97; Article 38.

21 *Id.* at Article 83(4)-(5).

22 *Id.* at Article 83(2)

23 *Id.* at Article 82.

24 *Id.* at Article 82(4).

25 Any company that processes personal data in relation to an offering of goods or services in the EU is subject to the GDPR. *Id.* at Recital 23.

26 The GDPR expressly recognizes these competing demands and warns that "extraterritorial application" of the laws of "third countries . . . may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation." *Id.* at Recital 115.

27 Article 29 Data Protection Working Party, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation* ("Cross Border Discovery Working Document"), at 9-10 (Feb. 11, 2009), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf. The Sedona Conference has recommended that entities maintaining personal data of EU citizens should consult privacy counsel to help craft a litigation hold to avoid conflict under the data protection laws while ensuring that relevant material is identified quickly. The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, at 5-6 (Sept. 2015), available at https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Practical%20In-House%20Approaches%20for%20Cross-Border%20Discovery%20and%20Data%20Protection.

28 *Id.* at 16-17.

29 GDPR text, at Recital 47.

30 *Id.* at Article 17(3)(e), 21(1). *See also id.* at Article 18(2) (establishing "defence of legal claim" exception to an individual's "right to restriction of processing").

31 Cross Border Discovery Working Document, at 10.

32 GRPD text, at Article 46(2)(a). For more information about the Privacy Shield, *see* European Commission Press Release: *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield* (Feb. 29, 2016), available at http://europa.eu/rapid/press-release_IP-16-433_en.htm.

33 GDPR text, at Article 46(2)(c). For more information about standard contractual clauses, *see* European Commission, Model Contracts for the transfer of personal data to third countries (last updated Dec. 12, 2015), available at http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

34 GDPR text, at Article 46(2)(b).

35 *Id.* at Article 49(1)(e); Cross Border Discovery Working Document, at 13.

36 *See* Cross Border Discovery Working Document, at 13.

37 GDPR text, at Recital 32.

38 *Id.*