AMERICAN BANKRUPTCY INSTITUTE
JOURNAL
The Essential Resource for Today's Busy Insolvency Professional

News at 11

By Camisha L. Simmons[1]

Privacy Law Compliance in Bankruptcy: The EU's New GDPR

Coordinating Editor Camisha L. Simmons
Simmons Legal PLLC
Dallas

Camisha Simmons is the founder and managing member of Simmons Legal PLLC in Houston.

In 2016, the European Union (EU) enacted the General Data Protection Regulation (GDPR),[2] a sweeping privacy law granting individuals within the EU enhanced privacy protections. GDPR took effect on May 25, 2018. Its mandates and scope of enforcement, including the imposition of severe monetary penalties, were written to apply beyond the geographical boundaries of the EU member countries. Its broad application extends to any company that controls and processes the personal data of individuals in the EU or engages in the profiling of those individuals.

Noteworthily, the EU's new privacy framework has quickly influenced U.S. Congress members to encourage U.S. companies to apply the GDPR privacy protections to the personal data of U.S. citizens.[3] The law possibly also influenced California's recent passage of a sweeping privacy law, which is like GDPR in various respects.[4]

While the new California privacy law does not become effective until 2020, GDPR is currently in effect, though it is uncertain how and to what extent U.S. courts will apply GDPR. Nonetheless, practitioners should be ready to address GDPR issues as they arise. Failure to do so may prove costly. This article provides a general overview of GDPR, discusses its uncertain application and enforcement in the U.S., and highlights areas of the privacy law in which U.S. bankruptcy practitioners should be prepared to navigate.

General Overview of GDPR

Who and What Does GDPR Protect?

GDPR protects the "personal data" of natural persons in countries of the EU, irrespective of their legal status.[5] Individuals physically located in the member countries of the EU, therefore, currently receive protection under GDPR.[6]

It is the EU's position that individuals have a fundamental right to the protection of their personal data and "should have control of their own personal data."[7] This protection extends broadly to, among other personal information of individuals in the EU, genetic data, biometric data, health data, location data and "any information relating to an identified or identifiable natural person ('data subject')."[8]

Who Must Comply with GDPR?

GDPR specifically governs the conduct of data handlers that are "controllers" and "processors" of personal data.[9] A controller is any entity that "alone or jointly with others determines the purposes and means of processing of personal data," while the processor is the entity that "processes personal data on behalf of the controller."[10] "Processing" is considered "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means."[11]

All companies "established" in the EU engaged in data-processing activities must comply with GDPR, irrespective of where the processing takes

1 This article represents the views of the author, and such views should not necessarily be imputed to Simmons Legal PLLC or its respective affiliates and clients.
2 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, reprinted in *Official Journal of European Union*, OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018, *available at* gdpr-info.eu (unless otherwise specified, all links in this article were last visited on Aug. 23, 2018).
3 *See* S. Res. 523, 115th Congress (2018) (referred to the Committee on Commerce, Science and Transportation), *available at* congress.gov/bill/115th-congress/senate-resolution/523/text.
4 *See* Marc Vartabedian, "California Passes Sweeping Data-Privacy Bill," *Wall Street Journal*, June 28, 2018, *available at* wsj.com/articles/california-rushes-to-tighten-data-privacy-restrictions-1530190800 (subscription required to view article).
5 *See* GDPR, Art. 1. *See also* GDPR, Recital (14), *Official Journal of European Union*, OJ L 119, 04.05.2016, p. 3, *available at* eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (includes full text and recitals).
6 *See* European Union Countries, *available at* europa.eu/european-union/about-eu/countries_en (listing current members of EU).
7 *Id.* Art. 1; Recital (7).
8 *Id.* Art. 4 (1) (13), (14), (15).
9 *Id.* Arts. 3, 4 (2), (7), (8).
10 *Id.* Art. 4 (7), (8).
11 *Id.* Art. 4 (2).

place.[12] A company is "established" in the EU if the company exercises a real and effective activity through stable arrangements in the EU.[13]

In addition, GDPR, as written, broadly governs companies not established in the EU if the companies' processing activities relate to the offering of goods or services to individuals located in the EU, and/or the company tracks the behavior of individuals in the EU to (among other things) analyze or predict personal preferences, behaviors and attitudes.[14]

Enforcement and Penalties

Independent public authorities ("supervisory authorities") established by each EU member country are granted authority to monitor controllers and processors, investigate GDPR violations, and impose administrative fines for violations of GDPR.[15] The supervisory authority could fine a noncomplying company up to €20 million or up to 4 percent of the total worldwide annual turnover (gross global revenue) "of the preceding financial year, whichever is higher."[16]

Key GDPR Privacy Protections

Companies may only process the personal data of individuals located in the EU if the individual consents to the processing or another legitimate basis is demonstrated by the controller. Legitimate bases for the processing include, but are not limited to, situations where the processing is necessary for the performance of a contract to which the individual is a party or to comply with a legal obligation.[17] Consent to processing can be withdrawn by the individual at any time and should be freely given, informed, clear and unambiguous.[18] "Silence, pre-ticked boxes or inactivity" do not constitute consent.[19] Further, when the processing has multiple purposes, consent should be given for all of them.[20]

In addition to the expansive consent and legitimate basis for processing requirement, GDPR affords individuals in the EU with additional protections.[21] Controllers and processors of personal data must be transparent with respect to processing activities.[22] Therefore, individuals (with few exceptions) have unfettered access to their data. Individuals have the right to request that controllers disclose, among other specifics, the purpose of the processing of their data and the recipients of their data.[23] Personal data "collected for specified, explicit and legitimate purposes [must] not [be] further processed in a manner that is incompatible with those purposes."[24]

At any time, the individual may request that the controller correct inaccurate information, object to the processing of the data and any automated decisions related to the processing, and request erasure of the data.[25] Although an individual has the right to request erasure of the data, known as the "right to be forgotten," a controller is authorized to continue processing the data if it is necessary to comply with a legal obligation imposed by EU law or an EU member's law for the "establishment, exercise or defence of legal claims," or if it has overriding legitimate grounds.[26]

In addition, controllers must conduct data-protection impact assessments and appoint data-protection officers in certain instances, maintain records of all processing activities under their responsibility, and notify supervisory authorities of data breaches within 72 hours of the breach.[27] Where the data breach will result in high risk to individuals' rights and freedoms, the breach must be reported to those persons without undue delay.[28]

Considerations for Bankruptcy Practitioners

Will U.S. Courts Apply and Enforce GDPR?

GDPR has yet to be tested in U.S. courts, therefore, it is not certain whether and how U.S. courts will apply and enforce GDPR. Bankruptcy courts possibly may look to existing case law addressing several laws and principles, including 28 U.S.C. § 959(b), § 1509(e) of the Bankruptcy Code, the Hague Convention, common law and international principles of comity. Section 959(b) provides that trustees and debtors in possession must "manage and operate the property in his possession ... according to the requirements of the valid laws of the State in which such property is situated." Likewise, § 1509(e) requires a foreign representative in a chapter 15 proceeding to comply with the law of the place where the property (in this case, personal data) is located.[29] However, these sections do not specifically reference their applicability to the application of foreign law in U.S. bankruptcies.

Thus, courts may need to go beyond these sections to determine enforceability of GDPR in the U.S. One example in which foreign law is applicable in U.S. bankruptcy proceedings is where a foreign defendant in an adversary proceeding must be served. In such an instance, Rule FRBP 7004(a) requires compliance with both U.S. and foreign law.[30] Similarly, bankruptcy courts could conclude that DIPs or trustees in possession of an EU individual's personal data must also comply with both U.S. and EU privacy law.

Principles of international comity will likely determine enforceability of GDPR in the U.S.[31] Recognizing and enforcing GDPR under comity principles is within a court's discretion, and, as the U.S. Supreme Court has noted, comity "is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of

12 *Id.* Art. 3.
13 *Id.* Recital (22).
14 *Id.* Arts. 51-59.
15 *Id.* Arts. 51-59.
16 *Id.* Art. 83 (5), (6).
17 *Id.* Art. 6.6 (providing legal bases for processing).
18 *Id.* Art. 7; Recital (32).
19 *Id.*
20 *Id.*
21 *Id.* Arts. 12-22.
22 *Id.* Art. 12.
23 *Id.* Art. 15.
24 *Id.* Art. 5 (1)(b).
25 *Id.* Arts. 16-22.
26 *Id.* Art. 6 (1)(f), (3)(a), (b); Art. 17(1)(c); Art. 21(1); Recitals 40, 41, 47, 54.
27 *Id.* Arts. 24, 30, 33-35, 37-39.
28 *Id.* Art. 34.
29 *See* 11 U.S.C. § 1509(e) (providing that "a foreign representative is subject to applicable nonbankruptcy law"). *See also* H.R. Rep. No. 109-31, pt. 1, at 110 (2005), *reprinted in* 2005 U.S.C.C.A.N. 88, 110 ("Subsection (e) makes activities in the United States by a foreign representative subject to applicable United States law, just as 28 U.S.C. section 959 does for a domestic trustee in bankruptcy.").
30 *See* Fed. R. Bankr. P. 7004(a). *See also Kravitz v. Deacons (In re Advance Watch Co.)*, 587 B.R. 598, 602-03 (Bankr. S.D.N.Y. 2018).
31 *See, e.g.*, Samantha Cutler, "The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information," *Bos. Coll. L. Rev.*, 1513, 1525-29 (2018). *See also Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for Southern Dist. of Iowa*, 482 U.S. 522 (1987) (providing balancing test to determine whether foreign law should apply to discovery requests).

other persons who are under the protection of its laws."[32] The Restatement of Foreign Relations Law's reasonableness analysis might also guide courts in determining whether the extraterritorial reach of GDPR is permissible in the U.S.[33]

Navigating the Discovery of Personal Data of Individuals in the EU

If GDPR is enforced in U.S. bankruptcy courts, parties could face compliance challenges when conducting discovery in litigation. Control over one's own personal data paramount under GDPR. Therefore, in anticipation of litigation, parties should carefully consider what bases under Article 6 of the GDPR will establish the parties' right to place a litigation hold on and process the data of someone in the EU. If informed and voluntary consent is the legitimate basis for the hold and processing, litigants should provide detailed litigation hold notices to persons in the EU. Further, even if consent has been obtained, the individual could withdraw consent at any time.

In discovery planning, this "right to be forgotten" should be taken into consideration, even though GDPR provides that overriding legitimate or legal grounds and the "establishment, exercise or defense of legal claims" provide an exception to the right to erasure.[34] Parties should play it safe given that these exceptions have yet to be tested in U.S. courts.

Lastly, firms should also ensure that agreements with vendors assisting with discovery include provisions that address GDPR compliance obligations.

Potential Roadblocks in Asset Sales

The sale of assets in bankruptcy is a valuable tool available to debtors to monetize assets to create liquidity in order to satisfy creditor claims. Unfortunately, GDPR compliance might thwart or slow down a sale of valuable personal data of a company's customers and other individuals. The "right to be forgotten" restrictions on transfers, and the limitations on a company's use of data outside of the original purpose provided to the individual, might make it difficult to effectuate a sale of the personal data. EU parties-in-interest could object at any time to a company's proposed sale of individuals' personal data. To ensure GDPR compliance, a court could require that a debtor provide notice to individuals in the EU informing them of their right to opt in or out of a sale of their personal data.

For asset sales made outside the ordinary course of business, § 363(b)(1)(B) requires that the court order the appointment of a disinterested privacy ombudsman upon the findings by the court — among other facts, that the debtor's prepetition privacy policy prohibited the transfer of consumers' personal data[35] to nonaffiliate third parties, and the proposed sale is not consistent with the terms of the privacy policy.[36]

Where a debtor seeks to sell the personal data collected from someone in the EU, the sale of the data could be inconsistent with a GDPR-compliant privacy policy because the sale of the data might exceed the scope of the original purpose disclosed to the individual for the processing of his/her data by the company.

If § 363(b)(1)(B) applies, the court will not approve a sale of personal data unless the sale is consistent with the debtor's pre-petition privacy policy, or, after appointment of the ombudsman and notice and a hearing, the court finds, among other things, that the sale complies with the Bankruptcy Code and does not violate applicable law, including nonbankruptcy privacy law.[37]

EU supervisory authorities might possibly intervene in the bankruptcy sale proceedings in order to safeguard the privacy rights of EU subjects. U.S. federal and state regulators have previously intervened in bankruptcy sales to protect the privacy of personal data of U.S. consumers.[38] Accordingly, EU supervisory authorities' intervention in a U.S. bankruptcy is not a remote possibility. Any delay in the sale process resulting from enforcement of GDPR, including an ombudsman's compliance investigation, could dissuade prospective purchasers or lead to a lower sale price in those cases where the sellable assets are "melting ice cubes." abi

Reprinted with permission from the ABI Journal, Vol. XXXVII, No. 10, October 2018.

32 *See In re Platinum Partners Value Arbitrage Fund LP*, 583 B.R. 803, 809-10 (Bankr. S.D.N.Y. 2018) (quoting *Hilton v. Guyot*, 159 U.S. 113, 163-64 (1895)).

33 *See Restatement (Third) of Foreign Relations Law* §§ 402, 403, 421 (1987).

34 *See* GDPR Arts. 17; 49.

35 Personally identifiable information (PII) is defined in the Bankruptcy Code and includes a consumer's name, physical address, email address, phone number, Social Security number, credit card number, and birth certificate. *See* 11 U.S.C. § 101(41A). PII also includes "any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically." *Id.*

36 *See* § 363(b)(1)(B).

37 *Id.*

38 *See, e.g.*, Kenneth M. Misken and Camisha L. Simmons, "Government Addresses Privacy Concerns in Bankruptcy Sales," XXXI *ABI Journal* 10, 28, 70-71, November 2012, *available at* abi.org/abi-journal.