

The Intersection of European Data Privacy and Domestic Discovery

BY RYAN P. NEWELL, ESQUIRE

In 2016, the European Union (“EU”) adopted the General Data Protection Regulation (the “GDPR”), which replaced its Data Protection Directive that was adopted in 1995. Described as “the toughest privacy and security law in the world,” it purports to “impose[] obligations onto organizations anywhere, so long as they target or collect data related to people in the EU.”¹ For domestic litigators, one might assume that the GDPR’s purported extraterritorial jurisdiction would be of no consequence when litigating in the United States. Indeed, the GDPR’s broad assertion of jurisdiction is arguably contrary to domestic principles and common law regarding permissible discovery. So while it is less than clear how the GDPR will or could be enforced in connection with potential violations in U.S. litigation, litigators would be wise to, at a minimum, be aware of its reach and potential consequences for violations.

The Broad Reach of the GDPR

Article 3 of the GDPR sets forth its territorial scope, the extreme breadth of which cannot be ignored:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

In other words, the GDPR’s protections are triggered when (1) organizations in possession of the data are in the EU (even if the data is not) or (2) organizations outside the EU offer

goods or services to people in the EU (or if the organizations are monitored by the EU). (There is a third smaller category concerning discovery from groups such as embassies.) In today’s global and virtual economy, a broad interpretation of the GDPR could raise implications for many domestic lawsuits.

If the GDPR applies, in order to process the data governed by the GDPR, one of the provisions of Article 6 must be satisfied. First, you can obtain consent from the person to whom the data belongs. Consent, however, is not easily obtained under the GDPR. It must be “freely given, specific, informed, and unambiguous”² and requests for consent must be in “clear and plain language.”³ Further complicating matters, consent can be withdrawn.⁴ It can be withdrawn on the eve of a discovery deadline, a deposition, or even trial. This poses a potential nightmare for litigators looking to rely on critical discovery that is subject to the GDPR. Moreover, in the employee-employer relationship, the GDPR makes it very difficult for employees to fully consent as there is a presumption that the employer holds significant leverage over the employee that would eviscerate the employee’s ability to freely give consent.⁵

In addition to consent, the additional bases for data processing under Article 6 include:

- i. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- ii. processing is necessary for compliance with a legal obligation to which the controller is subject;
- iii. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- iv. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- v. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.


Assuming Article 6 can be satisfied, the GDPR further provides requirements for how the data can be processed and provides robust protections to the person to whom the data belongs. While this article does not permit a deep dive into all of the GDPR’s nuances, it is worth noting the severe sanctions that the GDPR suggests can be imposed.⁶ There are two levels of potential fines that can result from GDPR sanctions. The “lesser” sanctions can be as much as €10 million or 2 percent of an organization’s annual revenue from the prior year, whichever is higher. The more severe sanctions can be as much as twice the lesser sanctions.

Effect of Blocking Statutes on U.S. Courts

Given the intricacies that must be adhered to and the magnitude of the penalties for lack of compliance, one might assume that the GDPR provides an adequate basis for resisting discovery requests directed at discovery protected by the GDPR. While Delaware courts have yet to resolve whether the GDPR as a “blocking statute” is an adequate basis for resisting discovery from the EU, other U.S. courts have been reluctant to preclude discovery on these grounds.⁷ For example, this past year, the District Court of South Carolina held that, it “is well settled 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.”⁸

Indeed, some courts have acknowledged the conflict posed by the GDPR’s protections and the mandates of domestic discovery. The Northern District of California has held that the GDPR “do[es] 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.”⁹ Similarly, the Eastern District of Pennsylvania has concluded that “[t]he United States ‘has a substantial interest in fully and fairly adjudicating matters before its courts — an interest only

realized if parties have access to relevant discovery — and in vindicating the rights of American plaintiffs.’ The interest of the United States in adjudicating this matter is substantial and requires production of relevant discovery.” The court in that matter acknowledged the interest of the foreign country, but ultimately concluded that the protective order in that matter afforded adequate protections to the data subject to the GDPR.¹⁰

While it remains to be seen whether the EU will successfully enforce the provisions of the GDPR when implicated by discovery in the U.S.,¹¹ litigators should consult the provisions of the GDPR and consult with practitioners licensed in the appropriate jurisdiction. And as has been suggested in prior articles in this publication, the best course is always to plan as early as possible in a transparent matter with the other parties and the court.¹² 

Notes:

1. For information on the GDPR, please visit <https://gdpr.eu/what-is-gdpr/>.
2. Article 4(11).
3. Article 7(2).
4. Article 7(3).
5. See <https://gdpr-info.eu/issues/consent/>.
6. See <https://gdpr.eu/fines/>.
7. *But cf. In re Activision Blizzard, Inc.*, 86 A.3d 531 (Del. Ch. 2014) (granting motion to compel and requiring use of two-tier confidentiality order notwithstanding French blocking statute).
8. *Rollins Ranches, LLC v. Watson*, No. 0:18-3278-SAL-SVH (D.S.C. May 22, 2020) (citing *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa*, 482 U.S. 522, 544 n.29 (1987)).
9. *Finjan, Inc. v. Zscaler, Inc.*, 2019 WL 618554, at *1, *3 (N.D. Cal. Feb. 14, 2019) (“the Court concludes that the GDPR does not preclude the Court from ordering Defendant to produce the requested e-mails in an unredacted form, subject to the existing protective order.”).
10. *Giorgi Global Holdings, Inc. v. Smulski*, 2020 WL 2571177, at *2 (E.D. Pa. May 21, 2020).
11. *In re Mercedes-Benz Emissions Litig.*, 2020 WL 487288, at *8 (D. N.J. Jan. 30, 2020) (not permitting personal data to be redacted; “Defendants failed to produce evidence that producing the information at issue here would lead to an enforcement action against Daimler by an EU data protection supervisory authority for breach of the GDPR. Indeed, whether an EU authority aggressively polices this type of data production in the context of pre-trial discovery in U.S. litigation remains to be seen.”).
12. See *A Low-Tech Solution to High-Tech Discovery*, *DSBA Bar Journal* (Oct. 1, 2019) (addressing use of discovery plans) available at www.dsba.org.

Ryan P. Newell is a partner at Young Conaway Stargatt & Taylor, LLP. He can be reached at rnewell@ycst.com.

CLE at HOME

DSBA CLE ONLINE

View an online CLE seminar
ANYTIME, ANYWHERE.

View the full online CLE catalog at www.dsba.org/cle.

