Legal Insights

Wolters Kluwer

September 24, 2018

Discovery under the GDPR

By Cynthia J. Cole and Neil Coulson*, Baker Botts LLP

This is part of a continuing series of articles by Cynthia J. Cole and Neil Coulson on the legal developments and implications of the General Data Protection Regulation on U.S. companies. Here, we describe the landscape of discovery pre and post GDPR.

This document does not attempt to describe the full scope of the GDPR's discovery requirements or how companies can comply with the GDPR's numerous other requirements. This document is not intended to constitute legal advice and should not be relied on as such.

Introduction

For many years, litigants in the United States found themselves bound to the preservation and discovery obligations of the Federal Rules of Civil Procedure, even where those obligations came into conflict with foreign laws protecting personal data. However, within the European Union, violation of these laws rarely resulted in penalties, leaving U.S. parties free to pursue discovery without much fear of reprisals by E.U. authorities. This landscape is set to change, though, as the General Data Protection Regulation came into effect on May 25, 2018. Under the GDPR, the European Union has committed to much greater protections for personal data and has created significant penalties for any firms in violation of these protections (up to €20 million or 4% of worldwide revenue).

There are two discovery situations relevant under the GDPR. The first is where one party to litigation in the United States is located in the European Union and is subject to the general discovery obligations of U.S. courts. In this case, the party, whether it be an E.U.-based firm, or possibly a U.S. subsidiary which requires data from its parent, likely already has guidelines in place to comply with the security provisions of the GDPR, which can help to ease any necessary cross border transfers.

The second situation occurs when a party to litigation in the United States must request discovery of some information from a non-party that is located in the European Union. In such a case, while the non-party entity from whom discovery is requested may have appropriate security safeguards in place, parties to the U.S. litigation will not necessarily have adequate security measures in place to justify cross border transfer. In addition, parties must be careful when requesting data from the European Union to avoid subpoenas which are considered overly burdensome, which could result in sanctions by the court.

---

* Baker Botts partner **Neil Coulson** is the Department Chair — Intellectual Property in London and Moscow. **Cynthia J. Cole,** CIPP/E, is Special Counsel in Palo Alto in Baker Botts' corporate, technology and privacy practice groups.

Generally speaking though, regardless of which situation a party finds itself in, it must understand how to best balance its requirements under the GDPR as well as its obligations to U.S. courts. The steep penalties which can be imposed under the GDPR require firms to reassess their discovery strategies and determine whether the risk of penalties under the GDPR outweighs the harms of not complying with U.S. court-ordered discovery.[1] While there has been little time to see how the European Union will react to GDPR violations, in a recent case before the U.S. Supreme Court, the European Commission has given some guidance regarding how it will likely react to U.S. discovery and there are some best practices that firms should follow to ensure they bear the least risk when performing discovery in the European Union.[2]

I. The State of Discovery (Pre-GDPR)

For decades, courts in the United States have mandated that parties comply with normal discovery procedures and orders, even where materials are located in other countries. This rule dates back, at least, to the Supreme Court's decision in *Aérospatiale*, where the Court held that, before issuing such a discovery order, courts must exercise "special vigilance" to protect parties from the dangers of "unnecessary, or unduly burdensome, discovery." Once a court makes such an order, after considering the problem with "due respect," the parties must comply, without regard to violations of foreign statutes that may result from performance.

Although the Court does not delineate exactly how such an analysis would take place, it does draw five factors to consider from the Restatement (Third) of Foreign Relations Law: the importance of the documents to the litigation; the specificity of the request; the origin of the information (i.e. within the United States or not); the availability of alternative means of obtaining the information; and the extent to which noncompliance would undermine important interests of the United States or compliance would undermine importance interests of the nation where the information is located.

Taken together, even where U.S. courts respect the European Union's interest in protecting personal data, it is rare that such interests outweigh a party's discovery interest.[3] However, there are also alternative methods to discover information stored in foreign jurisdictions.

In the 1960s, the United States spearheaded an effort to allow for more efficient transmission of evidence from one nation to another, resulting in adoption of the Hague Evidence Convention.[4] This convention allows states, under Article 1, to send a request to "Central Authorities" within each member nation to "obtain evidence, or to perform some other judicial act." While this method can overcome a litigant's concerns regarding violation of a foreign law, it does come at a cost. Letters of

1 Fed. R. Civ. P. 37(b).

2 Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, United States v. Microsoft Corp., 584 U.S. — (2018) (No. 17-2) [hereinafter EU Amicus Brief].

3 *See, e.g.*, Perrigo Co. v. United States, 294 F. Supp. 3d 740 (W.D. Mich. 2018); Salt River Project Improvement & Power Dist. v. Trench France SAS, 303 F. Supp. 3d 1004 (D. Ariz. 2018). *But see* Laydon v. Mizuho Bankm 183 F. Supp. 3d 409 (S.D.N.Y. 2016) (refusing to compel discovery after comity analysis of UK law).

4 Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, July 27, 1970, 23 U.S.T 2555 [hereinafter Hague Evidence Convention].

Request under the Hague Convention can sometimes take up to six months or more to receive a response. In addition, Article 23 allows for contracting nations to put in place a reservation declaring that they will not execute letters of discovery intended for pre-trial discovery. Such reservations have been made by several major jurisdictions, including Germany, France, and the United Kingdom.

II. Discovery Under the GDPR

With passage of the GDPR, the European Union has recommitted to serious protection of the personal data of its citizens. While the actual effect of the GDPR on U.S. discovery efforts has yet to be seen, the European Union has given some guidance on how it will likely react to discovery requests in the future and how U.S. parties can avoid the steep penalties that accompany violation of the GDPR. And while the EU Amicus Brief appears in the *United States v. Microsoft* case, which was declared moot before the Supreme Court by passage of the CLOUD Act by Congress, the brief still contains insight into how European authorities will likely react to future discovery requests.

As a preliminary matter, all "processing," which includes storage and use, regardless of where it occurs, must meet the criteria of Article 6 of the GDPR. In the case of cross-border discovery, the most relevant ground for processing would likely be "necessary for the purposes of the legitimate interests pursued by the controller." The European Union acknowledges that this provision can justify cross-border processing, but also points out that the controller's interest must be carefully balanced with the fundamental rights of the person whose personal data is being requested. In addition, any processing of data also grants the subject of that data certain rights, which must then be followed by any processors who receive the personal data (see the GDPR arts. 15, 16, 17, 21, 30, 32, 33, 34).

It is important to note, though, that the GDPR only protects the personal data of natural persons. Under its provisions, legal persons, while they must comply with the GDPR, do not obtain any data protection. In reality, this distinction is less important than it sounds, since almost any data related to a legal person (such as a corporation) is likely to also include personal data which can identify or otherwise be linked to a natural person bringing it under the GDPR's protection. Even so, this distinction may provide an avenue for discovery, since, limited though the data may be, it remains unprotected by the strict provisions (and penalties) of the GDPR.

Only once this preliminary matter is resolved can the actual transfer of personal data to a non-EU state be justified. The EU Amicus Brief lists several potential avenues by which a U.S. party could conceivable seek discovery under the GDPR, under either of the situations that were outlined above.

Article 46

Without requiring specific authorization by the European Commission (as is the case with transfers under Article 45, for which the United States does not qualify), transfers can also be justified by showing that the personal data will be protected by "appropriate safeguards." These safeguards include: binding corporate rules (generally irrelevant in a litigation context); an approved code of conduct (also generally irrelevant in a litigation context); and an "an approved certification mechanism."

Between the United States and the European Union, the Privacy Shield framework exists as an "approved certification mechanism" for data transfers. Under this framework, individual companies, including several eDiscovery companies, can "self-certify" that they will maintain proper data protection requirements when transferring data between the European Union and the United States. While this method has been very popular among U.S. companies, the ease of transfer it affords may soon come to an end, as the European Commission has decided to suspend the program unless the United States is fully compliant by September 1, 2018. While the resolution to suspend the program is unbinding, it shows that the European Union will be less likely to tolerate data transfers to the United States when companies cannot guarantee the protection of personal data in such a transfer.[5]

Article 48

Under this article, the GDPR reaffirms that simply because a foreign court has ordered transfer or disclosure of personal data, such actions are not automatically legal within the European Union. Such court ordered discovery must instead be based on an international agreement in order to be enforceable. This means that letters of request under the Hague Evidence Convention or a "mutual assistance treaty" (MLAT) can overcome GDPR restrictions. In fact, the European Union considers MLATs to be the "preferred option for transfers" of personal information. However, since most MLATs relate only to criminal investigations, they are not very useful in civil proceedings. Additionally, the United States does not have MLATs with most Member States of the European Union.

The Hague Evidence Convention is also not ideal for U.S. parties. As discussed before, Letters of Request under the Hague Evidence Convention have their disadvantages, since they are both time-consuming and very restricted in terms of what they can actually discover, and so provide little practice use to U.S. parties seeking pre-trial discovery.

Article 49

This article allows for transfer of personal data to third countries or international organizations in specific situations. There are four specific situations in which a discovery request under this article might be permissible without violating the GDPR.

First, explicit consent of a data subject to the transfer can justify transfer. While this method is the most straightforward, it is also the least likely to be achieved. A party cannot be ordered to consent to the transfer, and so getting the informed consent of the opposing party during litigation will probably be very difficult. Second, transfer can be justified where it is "necessary for important reasons of public interest." While this is most likely, or at least more easily, applicable to criminal cases,[6] nothing in the GDPR itself prevents this justification from being used in civil cases as well, although such interests would have to be very important to outweigh the data subject's right in such a case.

---

5 The full text of the resolution is available at: http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2018-0305&language=EN

6 EU Amicus Brief at 15.

Third, transfers can be justified where it is "necessary for the establishment, exercise or defence of legal claims." While at first glance this provision seems directly applicable to discovery, in practice, European governments generally do not view pre-trial discovery as falling within the scope of this allowance, since such activities are "a precursor of the trial itself."[7] That being said, the determination that legal claims must be a part of the trial itself was a determination made by individual Member States, not the European Union as a whole. The GDPR itself contains no such restriction and so may allow for discovery under this provision. That doesn't mean, however, that the European Union will not, in the future, pass legislation which restricts the definition of "legal claims" again, so parties must remain aware of future developments within the Union.

Finally, the GDPR leaves open a broad possibility of one-time transfer for "the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subjects." The "legitimate interest" could be "the interest of the controller in not being subject to legal action in a non-EU state," according to the EU Amicus Brief. This transfer must also: (1) concern a limited number of data subjects; (2) be assessed in light of all circumstances of the data transfer; and (3) ensure that suitable safeguards are in place to protect the personal data.

III. Best Practices

While companies face much steeper fines in the European Union for GDPR violations, there is no reason to suspect that U.S. courts will abandon their practice of ordering discovery of materials in the European Union. So, until further guidance is given or trends on either side can be assessed, it is important for companies to maintain the safest procedures when complying with U.S. discovery orders. Ultimately the decision to comply with a discovery order will require an analysis based on the specific needs and facts of a particular case.

Source

Considering the risks that are inherent in discovery (for U.S. litigators at least) in the European Union, parties should do as much as they can to avoid the conflict of law if possible, at least until further guidance is provided. Even where alternative methods (such as Letters of Request under the Hague Evidence Convention) may be more time consuming, the monetary benefits of both avoiding fines and avoiding having to craft lengthy legal justifications may make it worthwhile in the long run. This means making a determination of the importance of each piece of evidence to the trial (and whether a party needs it at all in order to succeed) and determining whether or not the information is available from another source, preferably one subject to the authority of a U.S. court and which doesn't invoke a conflict of laws issue.

Minimization

Whether complying with a discovery order or requesting discovery from another party (or even a non-party), it is important for companies to attempt to access and transfer only the minimum

7 David J. 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. 575, 581 (2016).

amount of data that they need. This will ensure that companies comply with both the GDPR and the discovery request to the best of their ability.

This means that all discovery requests pertaining the information within the European Union should be very specifically targeted, indicating the specific information that is requested, ensuring that the information is limited in scope and doesn't affect a large number of data subjects, and implementing appropriate safeguards for any data that is acquired. Ideally, such a request should also indicate why the evidence will be important at the trial and guaranteeing that it will only be used for that purpose and promptly deleted once its purpose is completed.

Such steps should be easy to undertake if a company is already compliant with the GDPR generally. However, if companies rely on the E.U.-U.S. Privacy Shield to demonstrate appropriate safeguards, then it is important to consider implementing more secure policies since, as explained above, the European Union has indicated that it will end the Privacy Shield framework due to noncompliance by the United States.

Deidentification

While the GDPR's provisions are very exacting, they only apply to the processing of personal data. This means that any information that can be used to directly or indirectly identify a particular individual will be covered by the GDPR, as will any such data that U.S. litigants seek to discover. In order to get around this, though, in certain circumstances it may be possible to "deidentify" data such that it is no longer subject to the same level of protection under the GDPR.

This can be done by two processes. First, pseudonymization, defined in Article 4, is the process by which personal data is deidentified in a way that it cannot be associated with a particular data subject without the use of additional information, usually held by the controller or processor but kept separate. Second, the process of anonymization, similar to pseudonymization, deidentifies personal data. However, unlike pseudonymization, the data cannot afterwards be associated with a particular individual, even with the use of additional data. Often, anonymized data takes the form of aggregated data which measures trends over large (but deidentified) data sets.

Within the context of discovery, this can be useful. As discussed earlier, the GDPR does not apply to the data of legal persons, but it can be difficult to collect the data of legal persons without incidentally collecting personal data as well. With pseudonymization, this data can be collected, with personal data redacted, so that parties can comply with a discovery request without implicating the GDPR.

Also, under the GDPR, pseudonymization is recommended as a security measure which should be put into place by data processors, meaning that, by default, pseudonymized data should be held separately from the data needed to associate it with a data subject. This simplifies the discovery process since a company's default security regime should allow for discovery of pseudonymized data on its own. Of course, this means that any party collecting that data must be careful that they do not already possess further information that can be used to reidentify a data subject.[8]

8 For example, they must ensure that data collected via other discovery (even of data within only the United States) cannot be combined with the discovered pseudonymized data in order to identify a particular individual.

Deidentified data, though, is only useful where personal data itself is not being discovered by the parties. If a discovery request requires personal data, then pseudonymization and anonymization will provide little to no benefit, since any personal data which can identify a particular individual is subject to the rigors of the GDPR.

Supervisory Authorities

Under the GDPR, various "Supervisory Authorities" are established throughout the European Union in order to implement, monitor, and enforce the GDPR's provisions. Considering their important role in E.U. data protection, it will be important for companies to understand which Supervisory Authority they will be dealing with when conducting discovery in the European Union. Not only will their prior conduct serve as a guide to parties conducting discovery abroad, but consultation during discovery will also help ensure that a company is doing everything in its power to minimize the risk of data breaches and ensure that it is compliant with the GDPR.

In the future, larger Supervisory Authorities, which repeatedly deal with parties fulfilling U.S. discovery requests, will likely develop guidelines to aid parties in conforming to both their obligations under E.U. and U.S. law. Alternatively, the European Data Protection Board, which ensures consistent application of the GDPR throughout the European Union, may provide cross border discovery guidelines.[9]

In addition, since the Supervisory Authorities are responsible for imposing fines under Article 83, being transparent with regard to discovery compliance can help reduce both the likelihood that a fine will be imposed and the amount of any fine. While there can be no guarantee, until further guidance is issued, that complying with a U.S. discovery order will not result in a fine, communicating with the Supervisory Authorities and ensuring that they are properly informed regarding the situation can only benefit parties who operate in the European Union.

Conclusion

Despite the significant risk of fines now possible under the GDPR, it is unlikely that U.S. courts will discontinue their practice of requiring compliance with cross-border discovery requests in the European Union. As a result, until both sides clarify, either through practice or published guidelines, how they will handle discovery under the GDPR, parties must do their best to balance their obligations under U.S. court rules and the GDPR.

The above practices, in combination with the justifications currently available under the GDPR, provide the safest path in going forward with discovery in the European Union. This might require resorting to slower methods of discovery (such as a Letter of Request under the Hague Evidence Convention) or even abandoning less promising pieces of evidence altogether, but until parties know how the European Union will react under the GDPR, it is best to take all possible steps to avoid the serious fines that can now be imposed.

---

9 As the Article 29 Working Party, the EDPB's predecessor, did.