GT GreenbergTraurig

Is a Company Permitted To Transfer PI From Europe to the US for a Discovery Request?

The EDPB has stated that the transfer must be "occasional," and expressly recognizes that data transfers for the purpose of formal pre-trial discovery procedures in civil litigation may fall under this derogation.

By Diane D. Reynolds, Jena M. Valdetero and David A. Zetoony | November 8, 2022 | New Jersey Law Journal

The Federal Rules of Civil Procedure, as well as state procedural rules, permit parties to a lawsuit to conduct discovery, in search of information and documents that may be relevant to the litigation. Parties can issue requests for documents, information (called interrogatories), and admissions of fact to other parties to the lawsuit; parties may use subpoenas to issue requests to third parties. When discovery issued in a U.S. civil proceeding seeks personal information regarding Europeans, or personal information that is held by an entity that is established in Europe, three main privacy questions arise:

• Whether under the GDPR there is a lawful basis to process personal information in the context of the discovery request?;

• Whether the country in which the personal data resides has legislation that specifically prohibits the transfer of information to the United States for purposes of civil discovery?; or

• Assuming that the processing has a lawful basis and is not outright prohibited, whether the GDPR permits the transfer of such information to the United States.

The following describes the legal considerations that underpin each issue.

Lawful Basis of Processing Personal Information

In order to process personal information under the GDPR, a controller must rely upon one of six lawful purposes of processing: consent, performance of a contract with the data subject, compliance with a legal obligation, necessity to protect the vital interests of a person, necessity to perform a task in the public interest (e.g., on behalf of a member-state government agency), or necessity to promote the legitimate interest of the controller so long as that interest is not overridden by the fundamental rights or freedoms of individuals.

The Article 29 Working Party (the predecessor to the European Data Protection Board (EDPB)) initially took the position that only three of the above lawful purposes could plausibly be relied upon in the context of complying with a foreign (e.g., United States) pretrial discovery request: the consent of the data subject, the controls need to comply with law, and the legitimate interest of the controller. It then analyzed each of these lawful purposes to explain if, and when, they could be used to justify compliance with a foreign litigation discovery request.

The Working Party concluded that in most cases consent is "unlikely" to provide a good basis for processing in the context of United States pretrial discovery processes, as U.S. courts and litigants often do not solicit individual data subjects' consent prior to the disclosure of personal information. It also expressed concern that the standards for soliciting, and obtaining, consent in countries like the United States may not match the standards imposed by European privacy laws.

The Working Party also concluded that in most cases a need to comply with law was unlikely to provide a valid basis for processing as the lawful basis had to be related to a European member state's law (not a U.S. law). As a result, for this lawful basis of processing to apply there would need to be an obligation within a European member state "to comply with an order of a court in another jurisdiction seeking such discovery."

The Working Party ultimately found that the only lawful purpose available in most pre-trial discovery situations was the legitimate interest of the controller. That interest would presumably be to further the "interests of justice" by "acting to promote or defend a legal right."

The Working Party cautioned, however, that before relying upon "legitimate interest" to process personal data controllers should engage in a balancing test that takes into account "issues of proportionality, the relevance of the personal data to the litigation and the consequences to the data subject" to make a conclusion as to whether the legitimate interest of the controller outweighed any impairment of data subjects' rights. In addition to conducting a balancing test, the Working Party suggested that data subjects should be given a right to object to the processing (if an objection was raised it would require the controller to re-examine the balancing test), and a party that provides data in connection with litigation should attempt to "restrict disclosure if possible, to anonymized or at least pseudonymized data." Specifically, the Working Party recommended that:

After filtering ("culling") the irrelevant data—possibly by a trusted third party in the European Union—a much more limited set of personal data may be disclosed as a second step. In addition to identifying a lawful basis of processing, controllers were also advised by the Working Party to consider whether other European privacy-related rights had been met such as whether notice had been given to data subjects that their information might be processed in litigation, and whether obligations had been imposed on the recipient of information (e.g., the adverse litigant or the party propounding discovery) will generally themselves be a controller of the produced personal data, the producing party should advise the recipient of their obligations to provide data subjects with access rights and correction rights, and to utilize appropriate data security to protect the information from disclosure.

Blocking Statutes

Some European Union (EU) member states consider the scope of U.S. civil discovery to be overly broad and burdensome. In reaction they have enacted what are referred to as "blocking statutes"—legislation that prohibits companies from providing documents or information in relation to civil litigation in foreign jurisdictions. For example, France enacted a blocking statute known as Law No. 68-678 of July 26, 1968, which states that "it is prohibited for any person to request, search for or communicate, in writing, orally or any other form, documents or information of an economic, commercial, industrial, financial or technical nature for purposes of establishing evidence in view of foreign judicial or administrative procedures or in the context of such procedures." Most blocking statutes contain an exception that permits the party propounding discovery to submit a "letter of request" under The Hague Evidence Convention. A letter of request refers to a document issued by a court in one country (e.g., the United States) in which the court requests that the courts in a second country (e.g., France) functionally domesticate the document request.

Cross-Border Transfer Mechanism

The GDPR permits a company to transfer personal data outside of the European Economic Area (EEA) if one of the following conditions has been met: the recipient entity is within a country that has been recognized by the European Commission as ensuring an adequate level of protection, the transferring and the recipient entity have put in place a European Commission-approved mechanism (a "safeguard") that imposes many of the substantive provisions found within the GDPR, or the transfer is subject to a derogation described in Article 49 of the GDPR.

The United States is not recognized by the European Union as having an adequate level of protection. As a result, a controller in Europe must either utilize a safeguard or transfer the information based upon an Article 49 derogation.

If a safeguard is utilized, the most common safeguard is the European Commission-approved Standard Contractual Clauses (SCCs). The SCCs are comprised of four different "modules," which are intended to be used to account for the following types of transfers:

Module Exporter	Importer Module 1	Controller Controller
Module 2	Controller Processor Module 3	Processor Processor
Module 4	Processor Controller	

Because a party to a lawsuit receiving personal data in discovery is likely determining the "purposes and means of processing" such information (e.g., to utilize in devising their litigation strategy), the recipient generally will be a data controller as well. Accordingly, Module 1 for controller-to-controller transfers would be appropriate. Getting a party to agree to sign SCCs may be challenging and may require assistance from the court. Transferring controllers should be prepared to educate all parties and the court on the obligations imposed by the SCCs.

The Article 49 derogations refer to a list of exceptions wherein a transfer mechanism is not needed. The Article 29 Working Party recognized that the derogations may be appropriate if there "is likely to be a single transfer of all relevant information" and "it is necessary or legally required for the establishment, exercise or defense of legal claims" in the foreign country (i.e., the United States). The EDPB emphasized the need for personal data to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, noting the need for a layered approach to the question of whether the personal data should be transferred. As a first step, there should be a careful assessment of whether anonymized data would be sufficient in the particular case. If this is not the case, then transfer of pseudonymized data could be considered. If it is necessary to send personal data to a third country, its relevance to the matter should be assessed before the transfer—so only a set of personal data that is necessary is transferred and disclosed.

The EDPB has stated that the transfer must be "occasional," and expressly recognizes that data transfers for the purpose of formal pre-trial discovery procedures in civil litigation may fall under this derogation. While the derogation can also cover actions by the data exporter to institute procedures in a third country, for example, commencing litigation, it cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future.

About the Author:

Diane D. Reynolds *is a shareholder in Greenberg Traurig's New Jersey Office. She practices in the areas of corporate and data, privacy and cybersecurity law.* **Jena M. Valdetero** *and* **David A. Zetoony** *are co-chairs of the firm's U.S. data, privacy and cybersecurity practice. Valdetero is based in the firm's Chicago office and Zetooney is based in the Denver office.*