Ballard Spahr LLP

The Legal Intelligencer

European Union Discovery Presents Compliance Headaches for US Litigants

February 05, 2018
By Philip N. Yannella

Discovery of personal data held in the European Union (EU) has been an issue that has bedeviled U.S. litigants for some time. On the one hand, the U.S. Supreme Court has held that discovery of foreign documents is not barred by foreign privacy law. On the other hand, EU privacy regulators have threatened enforcement actions against U.S. companies that don't take proper steps to protect EU personal data in discovery. The result is that U.S. lawyers and litigants are often caught in a Catch 22 with regard to foreign discovery, forced to choose between sanctions by a U.S. court for failure to conduct discovery or sanctions from an EU regulator for conducting such discovery.

Many had hoped that the EU's new data privacy law, the General Data Protection Regulation (GDPR) would ease the burden of conducting discovery in the EU. Unfortunately, while the GDPR makes it easier in some ways to conduct foreign discovery, it imposes new record-keeping requirements on U.S. litigants. Moreover, fines under the GDPR can be as high as 20 million euro, or 4 percent of worldwide turnover, greatly increasing the compliance risk for U.S. litigants.

CONDUCTING DISCOVERY UNDER CURRENT LAW

Under current European data privacy law, U.S. companies cannot process the personal data of any EU residents except under certain limited conditions. "Personal data" is defined very broadly to mean any information about unidentified or identifiable persons, which would include email addresses, street addresses, phone numbers, and even in some cases IP addresses. "Processing" is also broadly defined and covers all aspects of discovery. Current law, however, provides a number of exceptions to the general prohibition on processing of personal data. The one most relevant for U.S. discovery is the "legitimate interests" exception, permitting discovery of E.U. personal data where necessary for the legitimate interests pursued by the controller, including defense or prosecution of litigation in the United States.

Current E.U. privacy law also prohibits the transfer data from the E.U. to the United States—which is not considered to be a nation that has an adequate level of protection—except under certain limited conditions. Data can be transferred to the United States if necessary or legally required for the exercise or defense of legal claims.

RELEVANT CHANGES UNDER THE GDPR

In some ways, the GDPR does not differ greatly from current law. The definition of personal data and processing remain broad under the GDPR, as does the general prohibition against the processing and transfer of personal data to the United States. Like current law, the GDPR provides several bases—including some new ones—that would allow for discovery of EU personal data and transfer to the United States. It also imposes new record-keeping requirements on U.S. litigants as

well as potentially massive fines—up to 20 mm euros, or 4 percent of worldwide turnover—for violations of the regulation. Here are the key provisions of the GDPR relevant to U.S. discovery:

LEGITIMATE INTERESTS

The GDPR provides a "legitimate interests" exception that allows processing where "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." The language of this exception is very similar to current law and likely would cover most U.S. litigation.

CONSENT

Consent continues to be a valid basis under the GDPR both for processing personal data and for transferring the data to the United States. Changes under the GDPR, however, make the use of consent considerably more challenging in the employer-employee context (which is how consent is typically obtained in U.S. civil matters) because of a presumption that employee consent is inherently coercive. Valid consent in the employment context requires written declaration that the employee may decline consent without fear of retaliation as well as verification that the data transfer cannot subject the employee to any legal harm. Consent must also be revocable by the employee at any point, which could present challenges in U.S. litigation where documents containing the personal data may already have been produced to the other side, and potentially disseminated to others, at the time consent is revoked.

ESTABLISHMENT, EXERCISE OF DEFENSE OF LEGAL CLAIMS

The "defense of legal claims" derogation under current law permits the transfer of EU personal data to the United States for litigation and remains in force under the GDPR. In some ways, this mechanism will be easier to employ under the GDPR than current law, which allows member states to implement national legislation that narrowly limits the legal claims exception and has led to a patchwork of differing requirements across EU. Because the GDPR does not need to be implemented by separate national legislation, the 'defense of legal claims' derogation will be applied in a more uniform fashion across the EU, which in theory should lower compliance risks for U.S. litigants.

PUBLIC INTEREST

The GDPR introduces a 'public interest' derogation that may allow for the transfers of personal data to the United States for law enforcement purposes. This derogation, however, would likely not apply to discovery in U.S. civil matters. The public interest exception is also not unlimited. The public interest must be recognized by either the EU or member states laws. Examples include money laundering or anti-trust proceedings, financial supervisory investigations or for the purpose of public health.

LIMITED TRANSFER OF INDIVIDUAL DATA IN CASE OF COMPELLING LEGITIMATE INTEREST

This provision—new under the GDPR—may also permit the transfer of personal data to the United States for discovery purposes if the following criteria are met: the one-time transfer of data affects only a limited number of data subjects; is necessary for compelling legitimate interests to the data transferring entity; these interests are not outweighed by the interests or rights and freedoms of data subjects, and the transferring entity has assessed all circumstances surrounding the data transfer and has provided suitable safeguards. An open question is whether defense or prosecution of litigation will be deemed a compelling legitimate interest by regulators. Under current law it is considered a legitimate interest.

DATA MINIMIZATION AND OTHER SAFEGUARDS

If transfer of data to the United States for discovery purposes is permissible under the GDPR, litigants must continue to implement safeguards, such as use of search terms and data restrictions, to limit the amount of data that is collected and transferred to the United States. This obligations flows, in part, from the GDPR's data minimization standard, which requires that companies process the minimum amount of personal data necessary for the purposes for which the data is being processed. Where data is processed without valid consent, the GDPR also requires that U.S litigants consider other mechanisms, such as encryption of pseudonymization, to protect the rights of EU citizens and prevent "further processing." One way to achieve these goals could be though use of a protective order that limits the parties' ability to access and disseminate EU personal data in litigation.

ACCOUNTABILITY

The GDPR has a new "accountability" requirement that requires that data controllers document the steps they have taken to comply with the GDPR. This is a new requirement for many U.S. companies who may not be accustomed to rigorously documenting the procedures they have implemented to safeguard the rights and freedoms of EU residents whose personal data is collected and processed for U.S. discovery purposes.

FINES

The most controversial aspects of the GDPR are the new administrative fines and the potential for extra-territorial application of the Regulation. The GDPR permits fines of up to 20 million euros, or 4 percent of worldwide turnover, for failing to abide by the GDPR's provisions governing processing of personal data, data access rights,or the transfer of data to the United States. Importantly, the sorts of errors that give rise to these heightened fines are implicated by discovery for EU residents for U.S litigation: e.g., improper basis for processing the data, improper consents and lack of safeguards for limiting access to EU personal data. Whether and how EU regulators enforce the GDPR against U.S. litigants that conduct EU discovery is the great unknown. Historically, EU regulators have not fined many U.S. companies for conducting discovery in E.U., but all bets are off once the GDPR becomes operative.

FINAL TAKEAWAYS

Discovery of EU nationals for U.S. litigation continues to be permissible under the GDPR, but limitations on the use of consent and the new accountability provisions will require careful compliance by U.S. litigants, particularly in light of the potentially onerous fines available under the GDPR. Other discovery best practices, such as use of search terms and a protective order to limit the amount of data collected and further use of the data, as well as safeguards like encryption and redaction to limit access to personal data will, in certain circumstances, continue to be necessary under the GDPR.

Philip Yannella is practice leader of Ballard Spahr's e-discovery and data management group. He concentrates his practice on complex litigation and investigations involving digital evidence, particularly data breaches, class actions and theft of trade secrets.