

New York Law Journal

The European Union's GDPR and the Enforcement of US Court Discovery Orders

In their International Litigation column, Lawrence W. Newman and David Zaslowky discuss how US courts address the tension between the expansive scope of US discovery and the restrictive framework that EU countries have for processing the personal data of individuals under the GDPR.

By **Lawrence W. Newman and David Zaslowky** | November 19, 2025



The General Data Protection Regulation (GDPR) is the European Union's (EU) flagship privacy law, which was enacted in May of 2018, to regulate the processing of personal data of individuals within the EU. It applies to entities based in the EU and those outside the bloc that handle EU residents' data. With fines reaching up to €20 million or 4% of global annual turnover, the GDPR is a legal instrument with global implications.

For US litigators, the GDPR's extraterritorial reach has presented a challenge, particularly in federal district courts, where discovery and enforcement orders have frequently intersected with EU data protection provisions regarding the safeguarding of the privacy of EU individual persons. The result has been discovery disputes in which courts have had to accommodate the expansive scope of US discovery within the restrictive framework for individual persons under the GDPR.

The tension between US discovery obligations and foreign data protection laws is not new. In *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, 482 U.S. 522 (1987), the Supreme Court dealt with the extent to which a federal district court must employ the procedures under the Hague Evidence Convention with respect to discovery from a French adversary that is subject to US personal jurisdiction.

In its opinion, the court referred to a comity analysis “suggested” by the Restatement of Foreign Relations Law of the United States (which subsequently became Section 442), which listed factors that it said are “relevant to any comity analysis.”

These factors, which have since become known as the “Aerospatiale factors,” are referred to by courts when they engage in a comity analysis in which they weigh the interests of the US legal system against those of the foreign jurisdiction: (1) the importance to the investigation or litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the US; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the US or compliance with the request would undermine important interests of the state where the information is located. To these, there have been added two factors that courts have also considered: (6) the hardship of compliance on the party or witness from whom discovery is sought; and (7) the good faith of the party resisting discovery.

This balancing test became the cornerstone of judicial reasoning in cases where foreign so-called blocking statutes prohibiting the transfer of economic evidence were raised in opposition to US discovery requests. Since the GDPR came into force in May of 2018 US courts have applied these factors where the requested discovery involves personal data.

For example, in *In re Hansainvest Hanseatische Investment-GmbH*, 364 F. Supp. 243 (S.D.N.Y. 2018), the petitioner sought discovery under 28 U.S.C. § 1782 of banking and transactional records located in the EU for use in a contemplated proceeding in Germany. The respondents objected, citing potential liability under the GDPR.

The court granted the application but imposed conditions: the petitioner was required to indemnify the respondents against any potential breaches of European data privacy laws. This approach created a pathway for production while allocating risk in a manner that respected both US discovery norms and European privacy concerns.

In *In re Mercedes-Benz. Emissions Litigation*, Civ. No. 16-cv881 (SRC) D. N.J., Nov. 7, 2019, a Special Master appointed by the district court prohibited the Mercedes defendants from redacting “the names, positions, titles or professional contact information” of certain employees of any defendant (p. 9). The defendants argued that compliance would violate the GDPR and expose them to penalties.

The district court affirmed the Special Master’s ruling, which held that a Discovery Confidentiality Order was sufficient to mitigate the risk. This ruling reflects what has become the widespread practice in courts faced with such issues that GDPR concerns be addressed through procedural safeguards rather than outright denials of discovery.

In *Finjan, Inc. v. Zscaler, Inc.*, Case No. 17-cv-06946-JST (KAW) (N.D. Cal.), Feb. 14, 2019, the defendant argued that the GDPR barred the production of emails from an EU-resident custodian. The court rejected this argument after applying the *Aerospatiale* factors, all of which it found favored disclosure.

In a more recent case, *United States v. Eaton Corporation*, Case No. 24-3732 (Aug. 8, 2025), the Sixth Circuit Court of Appeals upheld a district court order permitting disclosure to the Internal Revenue Service of the evaluations of certain employees in Eaton’s affiliate in Ireland.

The case originated two years earlier with an IRS summons in a 26 U.S.C. §482 transfer pricing audit arising out of Eaton’s sale of intellectual property to its Irish affiliate. The district court applied the *Aerospatiale* factors, especially the fourth factor (alternative means to obtain the information) and the fifth factor (the national interests of the United States in tax collection), which it determined outweighed Ireland’s minimal interests in shielding the personal evaluations, particularly since there was to be no disclosure of sensitive information of the employees.

The Enforcement Question: US Orders and EU Response

If a US district court issues an order compelling the production of EU-based data, what happens when the producing party must execute that order within the EU?

In such a scenario, the GDPR's Article 48 may theoretically become involved. It provides that court judgments or decisions from non-EU countries requiring the transfer of personal data are not, in and of themselves, a valid basis for such transfers. Instead, the transfer must be grounded in EU law, typically through mechanisms like Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or explicit consent.

This provision effectively acts as a blocking statute, preventing the direct enforcement of US court orders in the EU without additional legal justification. The European Data Protection Board (EDPB) has emphasized that compliance with foreign legal orders must be assessed under EU law and that data controllers must ensure that any transfer is lawful under the GDPR.

The reality is, however, that, according to available case reports and commentaries, there has never been any known EU enforcement action that penalized EU persons for complying with US court orders to produce evidence protected under the GDPR. US courts have relied on this fact as a bulwark against the argument by EU parties that they will suffer severe consequences if forced to produce documents in US litigation.

In the *Finjan* case, for example, the US district court emphasized that the party resisting discovery on the basis of the GDPR had failed to provide information on "the likelihood of enforcement" against that party.

Likewise, in *Mercedes-Benz*, the Special Master noted that the defendants "have not pointed to any prior enforcement activities by the EU focused on violations of the GDPR in the litigation context" (p. 9).

As a further example, in a state court case, the Eighth District Court of Appeals of Ohio rejected the argument that the GDPR was a bar to enforcement because the defendant resisting discovery had failed to show that compliance with the US court order would lead to "hardship or an enforcement action from an EU data protection supervisory authority for breach of the GDPR." *Phillips v. Vesuvius USA Corp*, 2020 Ohio-3285, 2020 WL 311-8892 (Ohio Ct. App, 8th Dist, June 11, 2020).

These cases have their antecedents in blocking-statute litigation a few years earlier, where US courts were confronted with non-US resistance to discovery orders on the grounds that compliance would result in penalties in countries with blocking statutes.

A Sedona Conference study of cases citing the *Aerospatiale* case in response to blocking statutes revealed many cases in which the courts specifically noted that they had been presented with no evidence that actual harm would occur as a result of disclosure. See Kenneth J. Withers, Recent U.S. Court Decisions Citing [*Aerospatiale*] and Restatement (Third) of Foreign Relations Law of the United States §442 (1987), 2015.

Likewise with respect to the GDPR, the effectiveness of resistance to US discovery requests has significantly depended on the reality of whether compliance with US discovery orders will realistically result in penalties. The burden has been on EU defendants to make such a showing; we have found no readily apparent written indication of US courts having been shown evidence of realistic risks that GDPR penalties would actually be imposed.

It appears likely that the courts issuing discovery orders affecting overseas defendants have increasingly taken into consideration GDPR privacy issues through protective orders and measures such as anonymization of individuals' identities, redacting discovery requests and other limiting measures and, more generally, responding more favorably to specifically tailored requests.

In recent years, there have been fewer reported cases involving GDPR-related discovery disputes compared to the number of disputes reported shortly after the GDPR went into effect in May of 2018.

This change may be attributable to courts' receptivity to such modifications of discovery requests and perhaps also to awareness of the evident lack of EU penalty imposition for compliance with US discovery orders. Consistent with this perception is a reduced level of discussion in practitioner-related publications concerning GDPR penalty enforcement of US discovery orders.

Nevertheless, the GDPR continues to exist and practitioners need to be mindful that circumstances may arise where a US court may determine that sufficient protection of individual privacy interests cannot be afforded through a court order modifying or imposing conditions on discovery requests.

Lawrence W. Newman is of counsel and David Zaslowsky is a partner in the New York office of Baker McKenzie. They can be reached at lawrence.newman@bakermckenzie.com and david.zaslowsky@bakermckenzie.com, respectively. The authors express their appreciation to Anai's Itani from the London office and Alexis E. Marin from the New York office for their contributions to this article