



small_frog/Getty Images

Navigating Cross-Border Discovery in US Litigation

Because of technological innovations and expanding globalization, it is increasingly common for information sought by parties in a US litigation to be located abroad. At the same time, foreign data protection laws have become more prevalent and carry significant penalties for non-compliance. In this shifting landscape, parties and their counsel must carefully navigate the boundaries between domestic discovery obligations and foreign data processing and transfer restrictions.



SAMANTHA V. ETTARI

SENIOR COUNSEL
PERKINS COIE LLP

Samantha's extensive experience in privacy, data security, and data management issues includes legal, practical, and reputational risk counseling, often in the context of mergers, acquisitions, and technology-driven strategic and investment transactions. As senior counsel at the firm, she advises clients on both domestic and international privacy statutes and regulations, as well as cross-border transfers of data. Samantha is also a seasoned litigator and trial lawyer and has litigated diverse matters to final judgment, including contract and licensing disputes and false advertising and consumer fraud claims.

In today's global marketplace, US-based litigations often involve paper and electronic documents, communications, databases, and applications from other countries and jurisdictions. This cross-border discovery presents complex considerations and tasks for counsel throughout the course of a litigation, especially given the passage of the European Union's (EU's) General Data Protection Regulation (GDPR) and similar data protection laws worldwide.

This article highlights key issues to consider and steps to take for parties involved in cross-border discovery, including:

- Conducting an early case assessment that addresses cross-border data collection and production.
- Negotiating cross-border discovery protocols and confidentiality agreements.
- Compelling the production of cross-border discovery.

- Importing documents and data into the US for use in litigation.
- Returning or destroying documents and data at the conclusion of the litigation.



Search [Conflicts Between US Discovery and Non-US Data Protection Laws](#) for more on minimizing the conflicts that may arise between US discovery obligations and foreign data protection laws.

CONDUCTING AN EARLY CASE ASSESSMENT

Parties and potential litigants must be ready to address cross-border data collection and production at the outset of a matter. Key steps include:

- Identifying custodians with information relevant to the litigation.
- Reviewing relevant foreign regulations and company policies regarding cross-border data transfers.
- Determining whether to retain local counsel.
- Considering preservation and proportionality issues.
- Raising cross-border issues with opposing counsel and the court early on in the case.

IDENTIFY CUSTODIANS

As soon as possible, the parties should identify any custodians with information relevant to the claims and defenses raised or likely to be raised in the litigation, as well as any other relevant data sources. They should then determine:

- Where the custodians are located.
- In what countries the custodians officially reside.
- Where the data is located, stored, and backed up.

If any of these locations are outside the US, the parties must assess whether there are applicable foreign data protection laws that might govern the preservation, collection, export, and production of the data.

REVIEW RELEVANT REGULATIONS AND POLICIES

To avoid potentially significant penalties, parties and their counsel must consider the application of several types of foreign laws before conducting cross-border discovery in a case, including:

- Data protection regulations (DPRs), which govern the collection, use, and disclosure of personal information.
- Blocking statutes, which prohibit the application of foreign law, and often:
 - bar the cross-border transfer of certain categories of information (such as financial or economic data); and
 - prohibit the taking of evidence (such as civil depositions) within the country.
- Bank secrecy acts, which generally prohibit banking institutions and their officers and employees from disclosing financial records and other customer data to third parties.

These types of laws heavily regulate the transfer of certain data types and information outside a given country, and therefore may apply to data intended for use in a US litigation. Because violators of these statutes and regulations may be subject to civil and even criminal penalties, it is critical that parties confronting the potential preservation or export of international data relevant to a US-based litigation show that they take the foreign laws — and the interests of residents protected by those laws — seriously (see *The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)* (Sedona International Principles), Principle 1 (Jan. 2017)). Parties can demonstrate their compliance efforts through their conduct, internal documentation, and communications with local data protection authorities (DPAs).

Additionally, the parties should review their organizations' policies on data retention, international data transfers, and acceptable use, as well as employment agreements, which may include provisions on extraterritorial data transfers (such as whether data is stored outside the country). These policies may provide additional support or guidance on data processing and transfers to the US arising from litigation.

RETAIN LOCAL COUNSEL

It is usually necessary for parties to employ local data protection or data privacy counsel to help them effectively and lawfully navigate a country's DPRs (see *New York State Bar Ass'n (NYSBA), Guidelines for Obtaining Cross-Border Evidence (NYSBA Cross-Border Guidelines)*, Guideline 8 (Sept. 2018)). Additionally, many DPRs require organizations to have a data privacy officer, who may serve as a good resource for insight on foreign DPRs.

These local experts should be equipped to advise and assist a party in:

- Determining whether applicable DPRs protect relevant data.
- Establishing and documenting whether a lawful basis under the applicable DPR allows for a cross-border data transfer for use in US litigation.
- Drafting any necessary data transfer agreements or notifications.
- Preparing the data for transfer in the appropriate form, if minimization and de-identification (such as pseudonymization or anonymization) are required before exporting the data (see below *Data Transfer Methods*).
- Understanding whether a foreign jurisdiction may recognize and apply the attorney-client privilege and work product protection to the information sought.
- Coordinating with local DPAs, where necessary.
- Preparing submissions to the US court to explain the collection, review, export, and production limitations imposed by the applicable DPRs.

CONSIDER PRESERVATION AND PROPORTIONALITY ISSUES

One of the first steps in a contemplated litigation is to preserve potentially relevant documents and data (for more information, search [Reasonable Anticipation of Litigation Under FRCP 37\(e\): Triggers and Limits](#) on Practical Law). Under some foreign DPRs, including the GDPR, the act of preserving documents is considered “processing” and triggers rights and obligations under those laws (see GDPR, Article 4(2)). This means parties may face DPR requirements even before a complaint is filed. Parties should consider whether the foreign DPA discourages or prohibits pre-litigation processing of data, and whether the applicable DPR has any statutory exceptions that allow for the processing of data (see, for example, Article 29 Data Protection Working Party, Working Document 1/2009 on pretrial discovery for cross border civil litigation, at 7-8 (Feb. 11, 2009)).

To help minimize the impact and risks of violating foreign DPRs, parties should:

- Prioritize determining whether grounds exist, or there is a statutory exception, under the foreign DPR that authorizes the processing and cross-border transfer of information, such as when necessary for legitimate interests or to defend against legal claims (see below *Importing Data into the US*).
- Consider limiting the scope of preservation to only information that is strictly relevant to the claims and defenses and proportionate to the needs of the case. However, these concerns must be balanced with the potentially broader preservation requirements imposed by US statutory and common law.



Search [Conflicts Between US Discovery and Non-US Data Protection Laws](#) for more on determining whether a statutory exception allows for the collection, processing, and cross-border transfer of personal information.

Search [Cross-Border Legal Holds: Challenges and Best Practices](#) for more on implementing a US-style legal hold to preserve data located abroad.

The Federal Rules of Civil Procedure (FRCP), as well as many US state and local courts and arbitral tribunals, impose a proportionality limit on the discoverability and production of documents and data, meaning that the scope of discovery cannot go beyond what is proportional to the needs of the case (FRCP 26(b)). Given the additional costs and risks beyond traditional domestic discovery associated with cross-border discovery, proportionality may require litigants to narrow the scope of cross-border discovery more than they would for domestic discovery.

Before discovery formally commences or during initial discovery negotiations, the parties should consider whether:

- US residents or US-based custodians can provide similar or identical documents and data, obviating the need for cross-border discovery.

- The relevant documents or data are located on US-based servers or systems (and therefore may have already been “transferred” to the US).
- Overseas custodians can be limited to only those who are critical information sources (for example, obtaining a supervisor’s communications or data may eliminate the need for the collection, review, and production of information from the supervisor’s direct reports).

RAISE CROSS-BORDER ISSUES EARLY IN THE CASE

As early as possible in litigation, a party should educate its adversary and the court or tribunal about the restrictions on cross-border discovery presented by the applicable DPRs. The parties should address these issues when conferring under FRCP 26(f) and with the court during pretrial conferences to address discovery issues. The party seeking overseas information should be prepared to explain potential workarounds, solutions, and necessary documentation. Cooperation between the parties on cross-border issues is imperative at these pretrial conferences (see NYSBA Cross-Border Guidelines, Guidelines 3, 4).

NEGOTIATING CROSS-BORDER DISCOVERY ISSUES

Once litigation has commenced, there may be opportunities to negotiate various aspects of how the parties should handle cross-border discovery, including timing and scope. For example, parties may:

- Negotiate a tiered or phased discovery schedule that calls for the production of US-based information first.
- Seek a scheduling order that contemplates additional time to comply with DPR requirements before transferring data, including complying with DPA requests and documentation requirements in the local jurisdiction.
- Limit the production of information about or from overseas data subjects to only critical custodians.
- Limit the scope of the information produced.
- Use analytical and artificial intelligence tools, including technology assisted review, search terms, deduplication, threading, and date restrictions to cull data sets (for more information, search [E-Discovery: Processing Electronically Stored Information](#) on Practical Law).
- Conduct some or all of the review in the foreign country before transferring data.
- Seek a pretrial order or discovery protocol that provides rules and guidelines for:
 - transferring, storing, and reviewing produced documents and data;
 - sharing with the adversary upon production the rights and obligations required of data controllers or processors under the applicable foreign DPRs so the adversary does not violate any DPRs (see below *Documentation Requirements*);
 - redacting irrelevant data subject information;



Search [Protective Order for Documents Protected by Non-US Data Protection Laws](#) for a sample protective order, with explanatory notes and drafting tips.

- using de-identification techniques on data that allow for the data's use in litigation, such as redactions with corresponding and separately maintained legends (see below *Data Transfer Methods*); and
- performing anonymization of data where possible before transferring data (see below *Data Transfer Methods*).
- Enter into a stipulated confidentiality agreement or seek a protective order that provides:
 - descriptions of the relevant DPRs, including key sensitivities, limitations, rights, and obligations regarding the cross-border transfer of data;
 - confidentiality designations compliant with the DPRs;
 - limitations on the individuals or entities that can access the data;
 - standards for securing the data and notification requirements in the event of a breach;
 - procedures for using protected information in public filings and open court, including protocols for redactions, data de-identification, and filing under seal; and
 - procedures for the disposition, destruction, or return of data or information to the data controller at the close of the litigation (see, for example, GDPR, Article 17).

(See *Grupo Petrotekemex, S.A. de C.V. v. Polymetrix AG*, 2019 WL 2241862, at *7 (D. Minn. May 24, 2019) (compelling discovery, despite a Swiss blocking statute, because the information sought was critically important to the litigation, the existing protective order allowed “confidential” or “attorneys’ eyes only” designations, and non-responsive information could be redacted); *In re Commodity Exch., Inc., Gold Futures & Options Trading Litig.*, 2019 WL 1988525, at *7 (S.D.N.Y. May 6, 2019) (granting limited document production and partial redactions and pseudonymization, in compliance with multiple blocking and bank secrecy statutes); *Finjan, Inc. v. Zscaler, Inc.*, 2019 WL 618554, at *3 (N.D. Cal. Feb. 14, 2019) (holding that the GDPR did not preclude the court from compelling discovery of an EU resident’s unredacted emails, subject to an existing protective order that allowed a “highly confidential” designation and narrow search terms); see also Sedona International Principles, Principles 3, 4, 5; New York City Bar, *Cross-Border E-Discovery: Navigating Foreign Data Privacy Laws and Blocking Statutes in U.S. Litigation* (Cross-Border E-Discovery Guidelines), p. 12 (July 2018).)

However, counsel should keep in mind that any agreements on the timing or scope of cross-border discovery may ultimately be irrelevant or unenforceable when foreign DPRs apply to the collection or production of data. This is because parties may be required to first obtain a court order ruling on the application of a foreign DPR if a party opposes production because of the DPR, or resort to often slow diplomatic channels, such as requesting evidence pursuant to an international treaty or through letters rogatory, to obtain the desired cross-border discovery (see below *Limitations of Diplomatic Channels*).

COMPELLING CROSS-BORDER DISCOVERY

A party may refuse to produce requested cross-border discovery based on concerns that voluntary production might violate applicable DPRs and subject the party to potential DPA sanctions. In these cases, opposing counsel may seek court intervention to compel production.

In the recent past, courts tended to give little deference to foreign DPRs during discovery disputes. Courts often viewed foreign DPRs as being relatively toothless or rarely enforced and therefore not a legitimate bar to the transfer of information for use in a US-based litigation. As a result, parties were compelled to produce cross-border discovery pursuant to routine practice under the FRCP or local discovery procedures. However, with the increasing and well-publicized enforcement of the GDPR and other DPRs, US courts may begin showing greater deference to foreign privacy laws and an increased reluctance to compel production of cross-border discovery under US civil discovery rules.

Parties on the losing end of a motion to compel cross-border discovery may need to seek the desired evidence through diplomatic channels, such as the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Evidence Convention). Many DPRs have carve-outs or exceptions for the transfer of documents through diplomatic channels. For example, the GDPR specifically references the mutual legal assistance treaty (MLAT) process, which is a diplomatic channel used by law enforcement agencies to seek evidence or information abroad.

Using diplomatic channels may aid parties in complying with foreign DPRs because the process typically involves discrete evidence gathering by local government representatives, with oversight by local courts. These representatives and courts are well-versed in local privacy laws, limitations on discovery in local courts, and the data minimization and anonymization goals of the local DPR. This heightened control over the discovery process and overseas evidence gathering helps alleviate concerns that the DPRs address.

At the outset of a litigation involving cross-border discovery, parties and their counsel should understand:

- The factors US courts consider in determining whether parties should proceed under the FRCP or through diplomatic channels.
- The limitations of using diplomatic channels.
- Strategies to avoid using diplomatic channels.

INTERNATIONAL COMITY ANALYSIS

In analyzing whether the application of foreign DPRs excuses a party’s noncompliance with discovery requests, courts

may conduct an international comity analysis and weigh the following factors:

- The importance of the documents or other information requested relative to the litigation.
- The degree of specificity of the request.
- Whether the information originated in the US.
- Whether there are alternative means to securing the information.
- The extent to which noncompliance with the request would undermine important US interests.
- The hardship of compliance on the party or witness from whom discovery is sought.
- The good faith of the party resisting discovery.

(See, for example, *Finjan, Inc.*, 2019 WL 618554, at *1 (conducting a comity analysis and holding that the GDPR did not preclude the court from ordering the defendant to produce the requested emails); see also Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c); *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for the S. Dist. of Iowa*, 482 U.S. 522, 544 n.28 (1987) (endorsing the balancing test in the Restatement); *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1475-78 (9th Cir. 1992); *Phoenix Process Equip. Co. v. Capital Equip. & Trading Corp.*, 2019 WL 1261352, at *13-14 (W.D. Ky. Mar. 19, 2019).)

LIMITATIONS OF DIPLOMATIC CHANNELS

Using diplomatic channels for cross-border discovery can be frustratingly slow, particularly where the channels require the party seeking discovery to go through both US and foreign courts, and because foreign courts may not prioritize requests from abroad.

Additionally, diplomatic channels may limit the discovery that a party can obtain in a way that US laws might not. This includes possible restrictions on:

- **The scope of discovery.** Foreign authorities may restrict discovery to only information that is limited, specific, detailed, narrow, and intended only for use at trial (see, for example, New York City Bar, Cross-Border E-Discovery Guidelines, p. 6-7).
- **Pretrial witness testimony.** This evidence is not typically collected abroad in the same manner as in the US (that is, via deposition). Rather, pretrial testimony may require court permission, attendance by consular representatives, or written questions only. Some countries do not allow any pretrial testimony to be taken at all and the litigant may be restricted to requesting data and documents only. (See NYSBA Cross-Border Guidelines, Guideline 6.)
- **Enforcement of discovery requests.** Some jurisdictions that are signatories to evidence treaties like the Hague Evidence Convention (which is the most widely adopted treaty used to secure discovery through diplomatic channels) do not recognize pretrial discovery.



Search [International Litigation: Requesting Discovery Abroad for US Proceedings](#) and [International Litigation: Requesting Evidence Abroad by Letter of Request or Letter Rogatory](#) for more on the procedures for and limitations on obtaining cross-border discovery through the Hague Evidence Convention and letters rogatory.

STRATEGIES TO AVOID DIPLOMATIC CHANNELS

Because using diplomatic channels can severely delay litigation and may result in obtaining a much narrower scope of evidence than desired, a party seeking cross-border discovery should consider taking steps that may encourage a court to grant a motion to compel cross-border discovery and allow the parties to avoid involvement in diplomatic channels altogether. These strategies include:

- Serving narrowly tailored discovery requests.
- Cooperating in efforts to limit overseas custodians and data sources, and adopting redaction and de-identification protocols where possible.
- Documenting that no other party or US-based custodian has the information sought.
- Demonstrating the urgency of discovery or that deadlines would be missed or delayed by using diplomatic channels.
- Establishing that the relevant DPRs are not routinely enforced or that confidentiality agreements and protective orders can satisfy DPR requirements.

IMPORTING DATA INTO THE US

Although the applications and parameters of foreign DPRs are still evolving, many DPRs provide mechanisms for importing protected data into the US for specific and defined purposes. The pretrial discovery conducted in a case must qualify under one of the DPR's permissible purposes or exceptions before the protected data can be transferred to the US. For example, under the GDPR, a data controller may be able to establish that the data transfer advances a "legitimate interest" or is necessary to establish, exercise, or defend legal claims (see GDPR, Article 49).

Once justification for the transfer is identified, often with the aid of local counsel (see above *Retain Local Counsel*), parties typically must fulfill documentation requirements and follow certain methods of data transfer to ensure compliance with the DPR exceptions.

DOCUMENTATION REQUIREMENTS


Assuming the cross-border data transfer qualifies under the relevant DPR, certain documents may need to be executed by one or more of the following as proof of compliance with the DPR:

- A US-based affiliate, parent, or subsidiary.
- A data custodian (referred to as a controller).
- US litigation counsel (also often considered a controller).
- An e-discovery vendor (referred to as a processor).

For example, to legitimize the cross-border data transfer, a DPR may require:

- **Binding corporate rules (BCRs) or company data transfer policies.** These rules typically govern the transfer of data within an organization or to affiliates, partners, or subsidiaries. (See, for example, GDPR, Articles 46(2), 47.)
- **Standard contractual clauses (SCCs) with data protection provisions.** Local DPRs may require these agreements transferring the privacy and other obligations of the foreign data controller (for example, a custodian) to another data controller (for example, US counsel) or a data processor (for example, a US-based e-discovery vendor). (See, for example, GDPR, Article 46(3).) These agreements typically:
 - include required clauses or language from the relevant DPRs about, among other things, the purposes and justifications for the data transfer and the data security measures that will be employed;
 - identify the controllers and processors and define their rights, obligations, and potential liabilities upon transfer of the protected data;
 - describe the data or categories of data to be transferred (keeping in mind that the data should be defined to contemplate evolving claims and defenses); and
 - identify any potential data recipients, such as the court, regulators, and adversaries, and describe how the data can remain protected while in the recipients' possession through court-ordered protective orders or party stipulations (see above *Negotiating Cross-Border Discovery Issues*).
- **Data protection impact assessments.** These assessments and accompanying documentation may be required where a litigant seeks to export data that contains special categories of protected, personal information. (See, for example, GDPR, Article 35.)
- **Notices.** Parties may need to notify the data subjects and the supervising DPA when data is transferred for a US litigation. (See, for example, GDPR, Article 49(1).)

Given the relative infancy of DPRs, some justifications for the data transfer may be controversial and challenged by a DPA or the individuals whose personal information is contained or referenced in the transferred data. Local data protection counsel should assist in documenting and defending the applicable justifications for the transfer in anticipation of these challenges. Documenting the reasons for the data transfer is also important to demonstrate the litigant's deference to local DPRs and its good faith compliance efforts (see Sedona International Principles, Principles 1, 5).

 Search [Cross-Border Discovery Under the GDPR](#) for more on the GDPR requirements that impact US proceedings and best practices for navigating cross-border discovery.

DATA TRANSFER METHODS

Once litigants satisfy the justification and documentation hurdles to transfer data to the US, they must prepare the data

for transfer in a way that complies with the applicable DPRs. Some techniques to protect data include:


- **Data minimization.** Parties should arrange to transfer only data that is absolutely necessary for the justified purpose. This may be accomplished by isolating and minimizing the number of custodians, using search terms and date ranges to limit the data exported, and conducting an in-country review so that no irrelevant, non-responsive data is transferred inadvertently. (See, for example, GDPR, Article 5(1)(c).)
- **Pseudonymization.** This technique involves de-identifying personal data before export so that it can no longer be attributed to the custodian or to the referenced data subject without separate, additional information, such as a legend or key. (See, for example, GDPR, Articles 4(5), 5(1)(e).)
- **Anonymization.** This process strips from personal data any information that can identify the data subject.

To satisfy DPR security requirements, protected data should be transferred over a secure network or by using safe portable devices, with encryption and password protection (see, for example, GDPR, Article 5(1)(f)). Likewise, the data should be stored on receipt in the US in a manner that is compliant with best-practice security standards or applicable DPR requirements.

Using an e-discovery vendor with a robust understanding of the applicable DPRs and certifications and security measures that meet their requirements can aid in a compliant data transfer. When retaining an e-discovery vendor, a party should consider whether cross-border discovery is likely and whether the vendor:

- Has operations or has operated in the relevant countries.
- Has software solutions for the de-identification (pseudonymization or anonymization) of the data, if necessary.
- Can transfer and store the data in a manner compliant with the applicable DPRs.

(See New York City Bar, *Cross-Border E-Discovery Guidelines*, p. 12-13.)

 Search [Considerations When Selecting an E-Discovery Vendor Checklist](#) for more on choosing an appropriate e-discovery vendor to meet the needs of a case.

RETURNING OR DESTROYING DATA

DPRs stress data minimization and expect controllers and processors to retain only data that is necessary for their operations or to satisfy legal or regulatory obligations. Many DPRs also condition the processing or transfer of data on its timely return or destruction. (See GDPR, Article 17.) As a result, parties should include provisions for the return or destruction of data collected from abroad in applicable protective orders or discovery protocols, and should promptly return or destroy documents and data once they are no longer necessary for US litigation.